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

Table des matières

ANALYSES (1/2)

APPLICATION DU DROIT INTERNATIONAL AU CYBERESPACE : UNE ANALYSE DE LA TERMINOLOGIE CHINOISE

Dans l'esprit du profane, la Chine est un adversaire économique et politique redoutable ne respectant ni règle ni norme communément reconnue, que ce soit dans le monde réel ou dans le cyberespace. Pourtant, lorsqu'il s'agit de régir le cyberespace, le gouvernement chinois prône bel et bien l'application du droit international à travers les principes de la Charte des Nations Unies, et soutient l'élaboration de normes universelles et consensuelles capables de contraindre l'action des États dans le cyberespace – Chine comprise. La Chine a d'ailleurs pris part aux discussions du Groupe gouvernemental d'experts (GGE) à l'origine de l'applicabilité du droit international au cyberespace (rapport de Juin 2013).

Il ne s'agit dorénavant plus de savoir si la Chine se positionne pour ou contre l'applicabilité du droit international dans le cyberespace, mais bien de savoir quelles sont, pour la Chine, les conditions de l'application du droit international dans le cyberespace.

Une approche classique arrime la conception chinoise de l'applicabilité du droit international au cyberespace à la poursuite des intérêts économiques et financiers de la Chine. Si cette approche n'est pas erronée, elle omet néanmoins une dimension non négligeable de la construction du discours chinois sur la scène internationale : la dimension nationaliste.

Trois notions en particulier sont développées dans le corps de l'article, chacune constituant une pierre angulaire des éléments de langage chinois que ce soit dans les messages à destination d'une audience nationale ou internationale. Analyser ces éléments de langage révèle les dynamiques qui peuvent sous-tendre la stratégie chinoise dans les négociations sur l'application du droit international au cyberespace.

1. Fondement des éléments de langage chinois : la « protection de la souveraineté chinoise » (维护国家主权)

Le concept de souveraineté renvoie à la qualité spécifique à un État qui détient le « pouvoir suprême impliquant l'exclusivité de la compétence sur le territoire national (souveraineté interne) » et sur le plan international la compétence pour négocier avec d'autres États[1].

Pour la Chine, le concept de « souveraineté » est indissociable de la mémoire de l'ingérence de puissances étrangères dans les affaires intérieures (politique, commerciale etc.) et de leur intrusion sur le territoire chinois. Le concept a servi de fondement à l'édification de la légitimité du Parti Communiste Chinois (PCC) qui repose sur l'unification du territoire et de la nation et la rupture avec ce que l'histoire officielle appelle le « siècle des humiliations » (百年国耻).

La souveraineté de la Chine est, de fait, liée à un processus de réappropriation de son honneur notamment sur la scène internationale. Enjoindre, dans les instances internationales, les États à respecter le droit international, constitue un rappel constant du droit de parole que la Chine a acquis sur la scène diplomatique.

[1] https://cnrtl.fr/definition/souverainet%C3%A9

Elsa Kania montre que brandir le « droit de parole » (发言权) a pu être pour l'État chinois un moyen au service de la quête de pouvoir, économique ou militaire[2]. De même, dans le contexte de l'élaboration du cadre légal dans le cyberespace, les représentants chinois usent du concept de souveraineté non seulement pour rappeler qu'ils ont le droit – et le pouvoir – de prendre part à ces négociations, mais aussi pour faire de la protection de la souveraineté (chinoise) une condition non négociable à l'application du droit international au cyberespace récusant par la même tout doit de regard de la communauté internationale sur la gestion de ce qu'ils considèrent comme leur cyberespace national.

Il s'ensuit que les normes de comportement des États dans le cyberespace proposées par la Chine évoquent le respect de la souveraineté des États, et notamment le Code de conduite pour la sécurité de l'information soumis à l'Organisation des Nations unies (ONU) par l'Organisation de coopération de Shanghai (OCS) en janvier 2015. L'actuel président chinois, XI Jinping, a poursuivi l'introduction de ce concept dans les éléments de langage sur le cyberespace, et a confirmé la conception chinoise d'un cyberespace en tant que projection d'un territoire fini, semblable au territoire national, où l'autorité de l'État doit s'appliquer dans les mêmes conditions.

En ce sens, les quatre articles de la Stratégie nationale de cybersécurité[3] chinoise et les articles 1, 2 et 3 de la Stratégie pour la coopération internationale dans le cyberespace[4] de la Chine font référence à la souveraineté nationale[5]. Ces exemples illustrent, de surcroît, la continuité entre le discours destiné à la scène nationale et le discours déployé à l'échelle internationale.

En mer de Chine méridionale, l'État chinois s'est servi du concept de souveraineté pour légitimer et étendre sa présence militaire[6]. Or, la transposition du concept de souveraineté au cyberespace donne aux États une justification suffisante pour riposter, non seulement dans le cyberespace mais également dans le monde physique, et la Chine n'est pas le seul État défendre cette approche[7]. Transposé au cyberespace, l'emploi de la conception chinoise de la souveraineté pourrait, à terme, justifier des contrôles dans les infrastructures ou sur les flux d'autres pays.

2. La « stabilité » (稳定), clef de voûte des représentations politiques chinoises

En matière de cybersécurité et de cyberdéfense, il est attendu des normes internationales applicables au cyberespace qu'elles soient en mesure de préserver la *stabilité* du cyberespace.

La tradition classique chinoise porte une attention particulière à cette notion. En effet, les auteurs classiques considèrent qu'un bon gouvernement est un gouvernement stable, autrement dit, capable de se maintenir et

[2] https://www.ccpwatch.org/single-post/2018/11/27/The-Right-to-Speak-Discourse-and-Chinese-Power
[3] **国家网**络安全战略 (2016).
[4] 网络空间国际合作战略 (2017).
[5] Art 2: conveys the idea that sovereignty is a fundamental principle of international cooperation on cyberspace;
And according to Art 3: ensuring sovereignty through international cooperation on cyberspace is China's main objective.
[6] « 维护南海领土主权和海洋权益 » : protéger la souveraineté des territoires en mer de Chine méridionale et les droits et intérêts dérivé des mers et océans.
[7] Le ministère des Armées français a, dans un document de septembre 2019, publié un document sur l'application du droit international aux opérations dans le cyberespace dans lequel il assimile cyberattaque et agression armée.

capable de maintenir la stabilité de la société. La stabilité, conçue ici comme un contexte idéal d'émergence de la prospérité économique et politique, explique est donc pour la Chine une exigence répétée.

La notion de *stabilité* a été, comme celle de *souveraineté*, développée dans la Stratégie nationale de cybersécurité et dans la Stratégie pour la coopération internationale dans le cyberespace. Elle est de plus commentée dans le document « la Défense chinoise de la nouvelle ère » publié en juillet 2019. Enfin, le président chinois, XI Jinping, l'emploie dans ses discours sur le cyberespace, qu'ils soient de portée, internationale ou non[8].

La *stabilité* est par conséquent un élément de langage chargé de signification et ancré dans le discours politique sur la scène politique nationale, et que l'État chinois entend introduire et (faire) appliquer dans le cyberespace.

Assurer la stabilité du cyberespace a été invoqué pour mettre en place une surveillance des flux de données et d'informations dans le cyberespace par la Chine. Dans l'esprit des dirigeants chinois, la promesse de stabilité s'apparenterait davantage à une obligation de se conformer aux lignes du Parti. En effet, dans le monde physique, assurer la stabilité est l'objectif affiché de toutes les mesures instaurées par le gouvernement chinois dans la région autonome du Xinjiang depuis 2017. Ces mesures prévoyaient « d'assurer la stabilité de la région »[9] ; de préserver la « stabilité de son développement »[10] et « une société stable »[11].

3. « Gouverner le cyberespace selon la loi » (依法管理) : rassurer et assujettir

La concrétisation des vocables juridique et politique apparaît plus clairement encore avec l'expression (lexicalisée en chinois) de « gouvernement selon la loi ». Cette expression, qui fut d'abord un slogan des manifestations de Tian'anmen en 1989 en faveur d'une justice fiable, est délicate à aborder. En 1989, il s'agissait de réclamer le respect et l'application du droit par l'État chinois, en d'autres termes de réclamer un cadre légal clair. L'État chinois, dès avant XI Jinping, s'est réapproprié l'expression de « gouvernement selon loi » pour apparaître, sur la scène nationale, comme un État juste et moderne en rupture avec les pratiques de la période maoïste.

XI Jinping fait du gouvernement par la loi un élément important de son programme de réforme de la société et notamment en matière de lutte contre la corruption et contre les comportements considérés comme immoraux, anormaux ou obscènes. Gouverner selon la loi s'est donc traduit – entre autres – par une entreprise de *moralisation* de la société, et ce jusque dans le cyberespace. De ce point de vue, l'expression « selon la loi » est ainsi mentionnée 19 fois dans la Loi nationale sur la cybersécurité. Rogier Creemers a par ailleurs montré comment la surveillance du cyberespace national a pu servir l'œuvre de *moralisation* de la population chinoise[12]. Le cadre légal conçu pour circonscrire cette entreprise permet, entre autres, de cibler les

---

[8] Par exemple, lors de la *World Internet Conference (***第二届世界互**联网大会) à Wuzhen en décembre 2015, de la Conférence nationale de travail sur la cybersécurité et l'informatisation (**全国网**络安全和信息化工作会议) d'avril 2018.

[9] « **保**证新疆稳定 » (Quotidien du Peuple).

[10] « 发展稳定 » (Quotidien du Peuple).

[11] « 稳定社会 » (Quotidien du Peuple).

[12] Dans cette optique, Rogier Creemers a notamment montré comment les systèmes de crédit social ont participé à la moralisation de la société.
Rogier Creemers, « The Pivot in Chinese Cybergovernance », *China Perspectives*, 2015/4 | 2015, 5-13 ; China's "Social Credit System: An Evolving Practice of Control", Mai 2018.

informations et les acteurs en ligne qui sont perçus dans la loi comme des menaces pour la stabilité de l'État. En définitive, sous couvert de moralisation de la société, l'Etat chinois met en place l'éviction légale ou censure des avis et des informations non conformes, accréditant ainsi le discours réflexif de l'État sur son attachement au gouvernement selon et par la loi.

Du point de vue des relations internationales, parler de « gouvernance selon la loi » dans un contexte d'élaboration de normes régulant et limitant l'action des États dans le cyberespace suppose que la Chine s'engage à respecter le droit international dans le cyberespace.

Néanmoins, et au moyen d'un certain flou, la loi nationale chinoise sur le cyberespace confère à l'exécutif une marge de manœuvre non négligeable pour interpréter les lois et les mettre en pratique. Par exemple, l'Article 1 al.9 et l'Article 5 al.49 de la loi sur la cybersécurité obligent les fournisseurs internet à se soumettre au contrôle de l'État, mais la nature et le degré de ce contrôle ne sont jamais précisés. Il en va de même de l'Article 6 al. 75, qui autorise le gouvernement chinois à rechercher les structures, organisations ou individus étrangers responsables d'une cyberattaque sur des systèmes d'information chinois d'importance vitale et de prendre « toute mesure de sanction nécessaire ». Il semble, en définitive, que le « gouvernement selon la loi » se confond étrangement avec le gouvernement selon la volonté de l'État à un instant T.

Conclusion

Il apparaît que les corpus légaux internationaux acceptés par la Chine, tel que la Charte des Nations unies, sont ceux conformes à ces notions. Le concept de « souveraineté », la notion de « stabilité » et l'expression « gouvernement selon la loi » figurent tous dans le Code de conduite pour la sécurité de l'information soumis par les membres de l'OCS au Nations unies et font ainsi partie des éléments de langage mis en avant par la Chine pour modeler les normes internationales dans le cyberespace.

Cette terminologie choisie par la Chine pour élaborer le cadre légal international est conforme à des exigences de politique intérieure et est constituée à partir de notions et de concepts issus de préoccupations plus spécifiquement nationales. Leur introduction dans les normes internationales s'inscrit dans une volonté de validation de ses approches par la communauté internationale.

En effet, leur introduction dans les normes internationales appliquées au cyberespace augmenterait évidemment la crédibilité de la Chine sur la scène internationale, et plus encore contribuerait à asseoir la légitimité du parti communiste chinois. Il est par conséquent dans l'intérêt de l'Etat chinois – indissociable du parti communiste – de proposer des valeurs et des concepts cohérents et dans la continuité des politiques nationales.

Il ne s'agit pas d'exclure ces termes des corpus légaux internationaux, mais de bien connaître leur charge implicite et la manière dont ils peuvent se concrétiser.

ANALYSES (2/2)

LES CAPACITÉS SATELLITAIRES AU DÉFI DE LA MENACE CYBER

Les satellites fournissent des services essentiels à l'accomplissement des missions des armées. Celles-ci ont vu leurs besoins dans ce domaine – et donc leur dépendance à ces services – augmenter avec les années. Originellement, les armées se reposaient uniquement sur les données et informations fournies par leurs propres satellites. Mais avec l'accroissement de leurs besoins, notamment en bande passante, et avec la montée en performance des satellites commerciaux, elles ont commencé à intégrer leurs capacités dans la conduite de leurs opérations… au risque de faire de ces satellites civils des cibles militaires.

Comme le rappellent les auteurs du livre blanc « Defending Spacecraft in the Cyber Domain » du think tank américain Center for Space Policy and Strategy[13], la question de la vulnérabilité des satellites aux cyberattaques a longtemps été occultée pour les raisons suivantes, qu'ils partagent avec les systèmes industriels :

- Les satellites utilisent des composants logiciels et matériels spécifiques, qui ne sont donc pas vulnérables aux mêmes malwares que l'informatique commune ;
- Les satellites communiquent directement avec des stations au sol, sans interconnexion à l'Internet commercial ;
- La chaîne logistique de développement, production et lancement de satellites, notamment militaires, est censée être fermée et hors d'atteinte d'adversaires potentiels ;
- L'accès physique par des acteurs malveillants aux satellites eux-mêmes paraît peu probable.

Le retour d'expérience des systèmes industriels classiques démontre que ces éléments ne sont pas satisfaisants : la chaîne logistique, souvent internationalisée, n'est jamais complètement sûre, et des malwares spécifiques aux composants satellitaires peuvent être développés. Rappelons à ce sujet que le secteur de l'aérospatial est particulièrement visé par les campagnes de cyberespionnage[14] et que les informations dérobées peuvent mener à la découverte de vulnérabilités au sein des écosystèmes satellites concernés. Enfin, si l'accès physique aux satellites reste difficile, les stations au sol restent un vecteur d'attaque crédible.

À quelles cybermenaces sont exposées les constellations satellitaires et quelles en seraient les conséquences pour les capacités opérationnelles des armées ?

1. Typologie des menaces cyber et de de guerre électronique

Quatre principaux types de menaces cyber et électroniques affectent les liaisons satellitaires :

- Le déni de service, par brouillage des signaux ou envoi de paquets illégitimes : l'attaquant produit un signal d'interférence destiné à surcharger le signal légitime ou le système récepteur (satellites ou dispositifs au sol), de façon à interrompre la communication. Dans le cas d'un brouillage classique

[13] https://aerospace.org/paper/defending-spacecraft-cyber-domain

[14] "CrowdStrike Intelligence Report: PUTTER PANDA"; CrowdStrike., accessible à https://cdn0.vox-cdn.com/assets/4589853/crowdstrike-intelligence-report-putter-panda.original.pdf

relevant des dispositifs de guerre électronique, l'attaquant est cependant facilement localisable puisqu'il le brouilleur doit émettre très fortement pour surcharger le signal légitime, et s'expose à des représailles cinétiques en cas de conflit ouvert ;

- L'interception : Il s'agit de l'écoute illégitime d'un signal, soit à des fins de renseignement, soit en tant que première étape d'une compromission des systèmes. Avec l'avènement de la radio logicielle ou SDR (*Software Defined Radio*), il est devenu relativement aisé et peu coûteux de capturer un signal satellite. En revanche il reste difficile, dans le cas où les informations ainsi transmises sont chiffrées, de casser le chiffrement pour pouvoir exploiter les informations captées ;
- L'usurpation : l'attaquant parvient à envoyer un signal perçu comme légitime par sa cible, afin de l'induire en erreur ou en tant qu'étape constitutive d'une compromission du système On peut citer le cas classique de l'usurpation de signaux GPS. Contrairement au brouillage, la cible ne réalise pas qu'elle est victime d'une attaque et peut ainsi penser qu'elle se situe en un lieu différent, voire à un instant temporel différent puisque les signaux GPS servent également à maintenir la synchronisation temporelle. Certains considèrent que c'est ce type d'attaque qui a été utilisé par l'armée iranienne en 2011 pour capturer un drone américain, et dans la série de collisions ayant impliqué des navires américains en Asie du Sud-Est en 2017[15] ;
- La compromission partielle ou complète des systèmes du satellite ou des stations au sol et de leurs réseaux. La compromission peut viser la prise de contrôle cinétique du satellite, l'interception des données y transitant, ou encore le simple déni de service. L'impact d'une attaque, notamment sur une station au sol a le potentiel de compromettre le service de l'ensemble de la constellation correspondante. La compromission d'une station au sol suivra les étapes classiques de la *kill-chain* cyber, d'autant que celles-ci sont aujourd'hui principalement constituées d'informatique classique, et pourra donc impliquer les méthodes et techniques habituelles : *spearphishing* visant le personnel des stations au sol, emploi de vers type stuxnet pour passer les *air-gap*, accès physique aux consoles de contrôle (menace interne ou intrusion), etc.

2. Usages militaires et impacts potentiels de cyberattaques sur les systèmes satellitaires

Les satellites permettent aux armées de renforcer leurs capacités de :

- Position, navigation et timing (PNT) : perception de la situation géographique dans les différents domaines de l'action militaire (terre, air, mer, espace), recueil d'informations pour le ciblage de précision, synchronisation dans le temps des opérations, géolocalisation et navigation (notamment maritime) ;
- Intelligence, surveillance et reconnaissance : imagerie, évaluation de la menace, perception de situation, informations de ciblage, SIGINT ;
- Défense anti-missile ;
- Communications ;
- Suivi des données et des conditions météorologiques.

Le tableau suivant présente les principaux impacts potentiels de la perte de ces capacités tant pour les activités civiles stratégiques que militaires :

15 https://web.archive.org/web/20190107235625/https://www.japantimes.co.jp/news/2017/08/23/asia-pacific/experts-doubt-human-error-four-times-row-others-call-gps-hack-unlikely/

Capacité concernée	Impacts potentiels de la perte de capacité ou de la manipulation des données
Position, navigation et timing (PNT)	• Impacts sur l'espace aérien civil ; • Impacts sur les transactions financières, les horloges internes dans le secteur financier utilisant le système GPS ; • Impacts sur le fonctionnement d'appareils et de missiles liés à la perte du signal temps ; • Perturbation des données de navigation des équipements provoquant une possibilité de voir des unités ou des armes, notamment des missiles, détournées par l'adversaire. S'agissant des conséquences pour les satellites eux-mêmes : • Perte de contrôle ou destruction des satellites, soit du fait de l'incapacité à détecter des objets dans l'espace, soit par modification de l'orbite du satellite, ce qui peut également entraîner un risque de destruction en chaîne (syndrome de Kessler[16]) et des dégâts au sol par rentrée non contrôlée dans l'atmosphère ; • Perte temporaire ou permanente des fonctionnalités du satellite permanent, par exemple en grillant ses cellules solaires.
Intelligence, surveillance et reconnaissance (ISR)	• Compromission de la prise de décision à tous les niveaux de commandement résultant d'une diminution de la perception de situation (terre, mer, air, espace) ; • Capacité de ciblage défaillante.
Défense anti-missile	• Perte des capacités de protection contre les attaques de missiles balistiques ; • Détection erronée, ou une mauvaise attribution de l'origine d'une attaque de missile balistique pouvant mener à une escalade non intentionnelle.
Communications	• Blocage ou altération de la transmission d'informations perturbant la prise de décision (pouvant également provoquer des escalades non intentionnelles) ; • Blocage de la transmission des ordres le long de la chaîne de commandement ; • Réduction de la bande passante disponible, forçant un mode dégradé et une diminution des capacités opérationnelles.
Suivi des données et des conditions météorologiques	• Incapacité à programmer et mener à bien les opérations terrestres, maritimes ou aériennes ; • Pertes matérielles ou humaines du fait d'une conduite d'une opération dans des conditions météorologiques non prévues. • Pour le secteur civil, des risques sur l'agriculture qui utilise des données satellitaires pour piloter les besoins en eau et en pesticide.

Tableau modifié de l'étude « *Cybersecurity of NATO's Space-based Strategic Assets* »
Dr. Beyza Unal, Chatham House International Security Department[17].

[16] Le syndrome de Kessler, du nom du consultant à la Nasa ayant envisagé le scénario en 1978, veut que plus le nombre de débris en orbite augmente, plus le risque de collision avec d'autres objets en orbite augmente provoquant une réaction en chaîne rendant les orbites impraticables.

[17] Le syndrome de Kessler, du nom du consultant à la Nasa ayant envisagé le scénario en 1978, veut que plus le nombre de débris en orbite augmente, plus le risque de collision avec d'autres objets en orbite augmente provoquant une réaction en chaîne rendant les orbites impraticables.

3. La disruption des capacités satellitaires adverses : un enjeu pour les armées

La disruption des capacités satellitaires adverses est perçue à travers le monde comme un enjeu majeur dans des conflits modernes.

Les doctrines militaires chinoises[18] et russes considèrent par exemple les capacités anti-spatiales comme des moyens de réduire l'efficacité militaire de leurs adversaires, et développent à cette fin des armes antisatellites cinétiques (armes à énergie dirigée, missiles antisatellite). La Chine et la Russie possèdent d'ailleurs leurs propres systèmes de géolocalisation alternative au GPS, BDS et GLONASS respectivement. Ainsi, leurs armées ne sont pas tributaires des systèmes GPS et Galileo dont la disruption constituerait un avantage certain en cas de conflit, malgré des dommages collatéraux potentiels sur leur propre secteur civil, qui peut intégrer une certaine proportion de systèmes dépendant de ces constellations, notamment l'aviation civile et les systèmes financiers. L'Iran et la Corée du Nord revendiquent la même vision de l'importance de la disruption des capacités satellitaires de leurs adversaires[19] , bien que ne possédant pas des mêmes capacités d'armement cinétique antisatellite.

Pour autant, même si plusieurs nations ont réalisé des tests d'armes cinétiques, notamment la Chine, les États-Unis, l'Inde et la Russie, l'utilisation de ce type d'armement est finalement peu souhaitable même pour les États qui en ont la capacité. En effet, tous ces États bénéficient de capacités satellitaires et y ont investi lourdement, et toute destruction de satellite risquerait donc de compromettre le bon fonctionnement de l'ensemble de l'écosystème, notamment du fait du syndrome de Kessler cité précédemment.

En revanche, une action plus ciblée dans le cyberespace pourrait permettre une action de disruption efficace sans nécessairement risquer la prolifération de débris orbitaux. Nous savons que la majorité des pays cités précédemment ont mené des campagnes d'espionnage visant le secteur de l'aérospatial et possèdent ou développent des capacités offensives cyber significatives. Si sur le plan cinétique, la défense des constellations satellitaires semble hors d'atteinte et le développement de capacités de dissuasion reste la seule protection envisageable, sur le terrain cyber en revanche, de réelles mesures de protection peuvent et doivent être prises pour d'assurer la pérennité des capacités et des missions.

Cela signifie que s'agissant de l'utilisation des capacités satellitaires commerciales pour les propres besoins, les armées ne peuvent pas se contenter de protéger uniquement les canaux qui leurs sont réservés, mais ont également le besoin de s'assurer de la cybersécurité de l'ensemble de l'écosystème sous-jacent. Cela implique d'être proactif dans l'assurance qu'une prise en compte des besoins de cybersécurité existe chez les prestataires. Des besoins qui ne se limitent pas aux seules spécifications des systèmes satellitaires : surveillance efficiente des systèmes et réseaux, sensibilisation du personnel, audits réguliers et *threat hunting* dans les stations au sol mais aussi dans l'ensemble de la chaîne logistique que l'on sait particulièrement ciblée depuis des années par les campagnes étatiques de cyberespionnage. Du côté des satellites eux-mêmes, et notamment des smallsats qui se multiplient, il est urgent de systématiser les architectures intégrant des racines

[18] Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2018; Office of the Secretary of Defense; 16 May 2018.
Statement for the Record: Worldwide Threat Assessment of the US Intelligence Community; Office of the Director of National Intelligence; 13 Feb 2018, accessible à https://www.dni.gov/files/documents/Newsroom/Testimonies/2018-ATA---Unclassified-SSCI.pdf

[19] https://www.dia.mil/Portals/27/Documents/News/Military%20Power%20Publications/Space_Threat_V14_020119_sm.pdf

de confiance (Root of Trust)[20], d'embarquer des fonctions de surveillance de la mémoire (dont l'analyse par des solutions de détection de menace peut être réalisée au sol), de chiffrement des canaux de contrôle et autres mesures de cyberprotection appropriées.

FOCUS INNOVATION

Flare Systems : une nouvelle approche de la *Cyber Threat Intelligence* (CTI)

Présentation

Flare Systems est une jeune entreprise canadienne fondée en 2017 à Montréal. Elle a été co-créée par Mathieu Lavoie, son *Chief Executive Officer* (CEO), anciennement chef d'équipe de pentesters dans le secteur bancaire, Israël Hallé, *Chief Technical Officer* (CTO), auparavant analyse de *malware* chez Google, et David Décary-Hétu, *Chief Research Officer* (CRO) et docteur en criminologie.

La création de la société est le fruit d'un constat : « *Beaucoup de sociétés de cybersécurité promettent beaucoup mais livrent peu. Protéger toutes les compagnies de toutes les menaces est pratiquement impossible, mais protéger efficacement un secteur ciblé l'est* »[21].

Ainsi, Flare Systems s'est donnée pour ambition de protéger les institutions bancaires contre toutes les menaces cyber potentielles, causées tant par des actes malveillants que des erreurs humaines.

A l'automne 2019[22], elle a levé 1,1 million de dollars CAD qui lui permettent de s'attaquer à de nouveaux marchés (américain et européen) et d'accélérer le développement de ses solutions technologiques – élément essentiel à l'heure où les acteurs malveillants collaborent de plus en plus et adaptent constamment leurs méthodes.

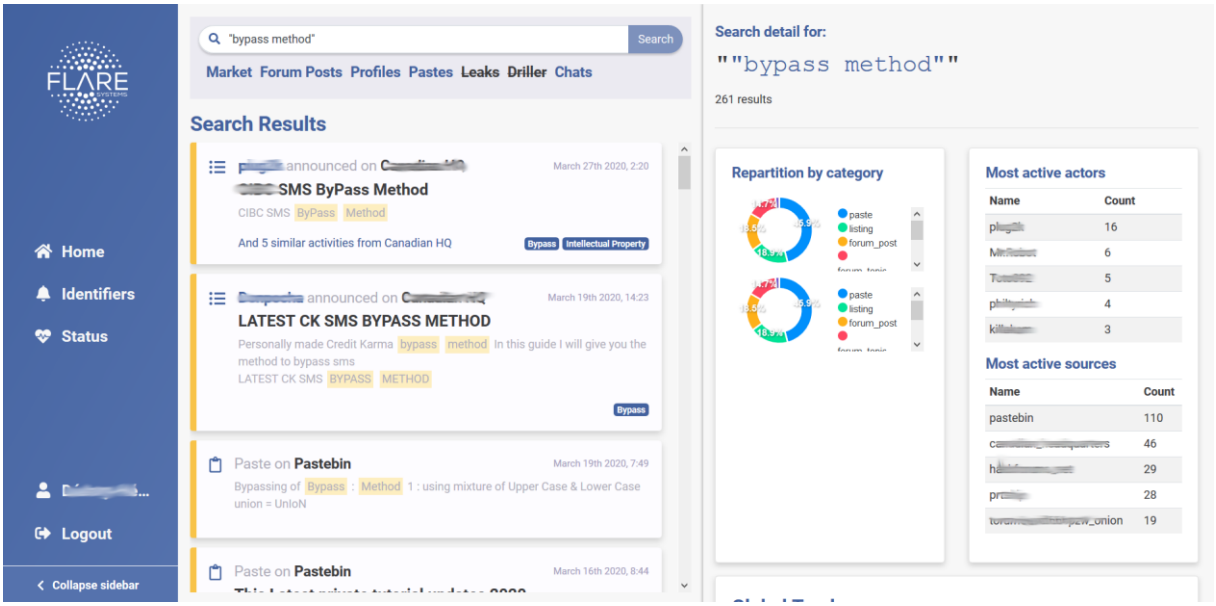
[20] https://uefi.org/sites/default/files/resources/UEFI%20RoT%20white%20paper_Final%208%208%2016%20(003).pdf
[21] Issu de l'entretien avec David Décary-Hétu, mars 2020
[22] https://www.luge.vc/fr/lentreprise-de-cybersecurite-et-de-fintech-flare-systems-recoit-un-financement-de-1-million-de-luge-capital/

La solution

À travers une série de produits rassemblés sous l'appellation Firework, Flare Systems collecte de manière autonome et quotidienne un important volume d'informations sur les différentes couches du Web (sur le darkweb principalement, mais aussi de plus en plus sur le clearweb) et pré-analyse les éléments recueillis pour générer des alertes sur les menaces qui pourraient peser sur ses clients.

La solution repose sur une série de briques technologiques telles que le *Machine Learning* et l'Intelligence artificielle (IA) qui lui permettent de catégoriser les flux d'information, vérifier la fiabilité des publications et la crédibilité des comptes, et ce dans le but de donner du sens au contenu collecté. Sur les marchés illicites (cryptomarchés notamment), Flare Systems peut ainsi se mettre dans la position d'un acheteur potentiel de numéro de carte de crédit mis en vente sur le darkweb afin de récupérer des éléments clés sur l'origine du produit, le vendeur, le trafic, etc.

De plus, la société propose un outil qui se veut à la fois proactif – en surveillant en temps réel les menaces qui pèsent sur les entreprises et les institutions et en donnant à ses clients la possibilité de bloquer un compte s'il se rend compte que ses identifiants ont fuité sur Internet – et simple d'intégration, puisqu'il ne nécessite pas de partage préalable de données par le client (telles que les noms de leurs clients ou leurs informations personnelles). Il n'y a donc pas de problématique de protection des données sensibles.



Interface du logiciel Firework pour la détection de fraude bancaire

L'innovation

Flare Systems se distingue de ses concurrents en ce qu'elle ne se contente pas de collecter l'information, mais la nettoie afin de ne proposer à ses clients que les éléments les plus pertinents et leur présenter les principales menaces pesant sur eux. La structuration de l'information est donc primordiale : la solution permet ainsi d'extraire l'intégralité des données dans chacune des pages web analysées, permettant des recherches pointues et *in fine* une analyse plus fine.

Par ailleurs, elle se concentre sur la surveillance de deux groupes d'individus : les attaquants, mais aussi les employés. D'une part parce que le second groupe est lui-même surveillé par le premier qui tente de détecter les incidents de sécurité pour mieux les exploiter, et d'autre part car la fuite d'informations confidentielles dans une entreprise est souvent le résultat de négligence involontaire de ses employés. Phénomène qui s'est même accru du fait de la crise sanitaire actuelle et de l'utilisation massive des outils de travail à distance qu'elle a induite. A l'heure du *credential stuffing*[23], une entreprise peut ainsi contrôler son empreinte technologique et savoir si certains de ses employés ou clients ont utilisé des mots de passe qui ont fuité sur Internet et si lesdits mots de passe ont été réutilisés dans les systèmes de l'entreprise.

De plus, au-delà d'un nouveau mode de surveillance, la société propose une autre approche de la transparence, en permettant à ses clients de comprendre comment, quand et d'où viennent les résultats qui leurs sont transmis (transparence des modes de surveillance de Flare Systems). Via l'interface, il est ainsi possible d'avoir accès aux sources qui alimentent le système, de mesurer le niveau de vulnérabilité ou encore de connaître la fréquence d'analyse.

Enfin, si la société répond aux besoins des institutions financières, ses solutions ont également un intérêt pour d'autres secteurs industriels, dans un contexte où les pirates et acteurs malveillants agissent en réseaux sans frontière et s'attaquent bien souvent aux mêmes cibles – dans la finance aujourd'hui, mais sans doute dans d'autres secteurs demain, la défense entre autres.

ACTUALITÉ

Audition du Commandant de la cyberdéfense à l'Assemblée nationale

Commandant de la cyberdéfense, le général de division aérienne Didier Tisseyre a été reçu le 6 mars par la Commission de la défense nationale et des forces armées de l'Assemblée nationale. Portant sur le thème « Cyber, nouvel espace de conflictualité », son audition s'est articulée autour d'une présentation des enjeux, acteurs et priorités stratégiques de la cyberdéfense française. Elle intervient dans un contexte de diversification des cybermenaces et de montée en puissance de la cyberdéfense, priorité nationale depuis le *Livre blanc sur la défense et la sécurité nationale de 2013*, qui s'est concrétisée avec l'inauguration en octobre 2019 du premier bâtiment entièrement dédié à la conduite des cyber-opérations du ministère des Armées (Rennes).

Le GDA Didier Tisseyre a répondu aux questions de la commission parlementaire qui ont notamment porté sur :

- la coordination entre actions françaises et européennes dans le domaine de la cyberdéfense ;
- les cyberattaques potentielles contre les intérêts majeurs de la France ;
- l'articulation entre la « cyberdéfense » et la « cybersécurité ».

[23] Type de cyberattaque consistant à voler des informations de compte type identifiants et mots de passe associés pour obtenir un accès non autorisé à des comptes utilisateurs : https://www.wired.com/story/what-is-credential-stuffing/

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