Lettre n°63 - Juin 2017 - disponible sur omc.ceis.eu

Brève du mois

« As business leaders continue to ignore the "eat right and exercise" advice from their security pros, we can't be surprised when they are having the cyber security equivalent of heart failure. As long as organizations fail to address basic security problems, they will be victims of common attacks »[1] - CTO de Stealthbits Technologies, au sujet du ransomware NotPetya.

TABLE DES MATIERES

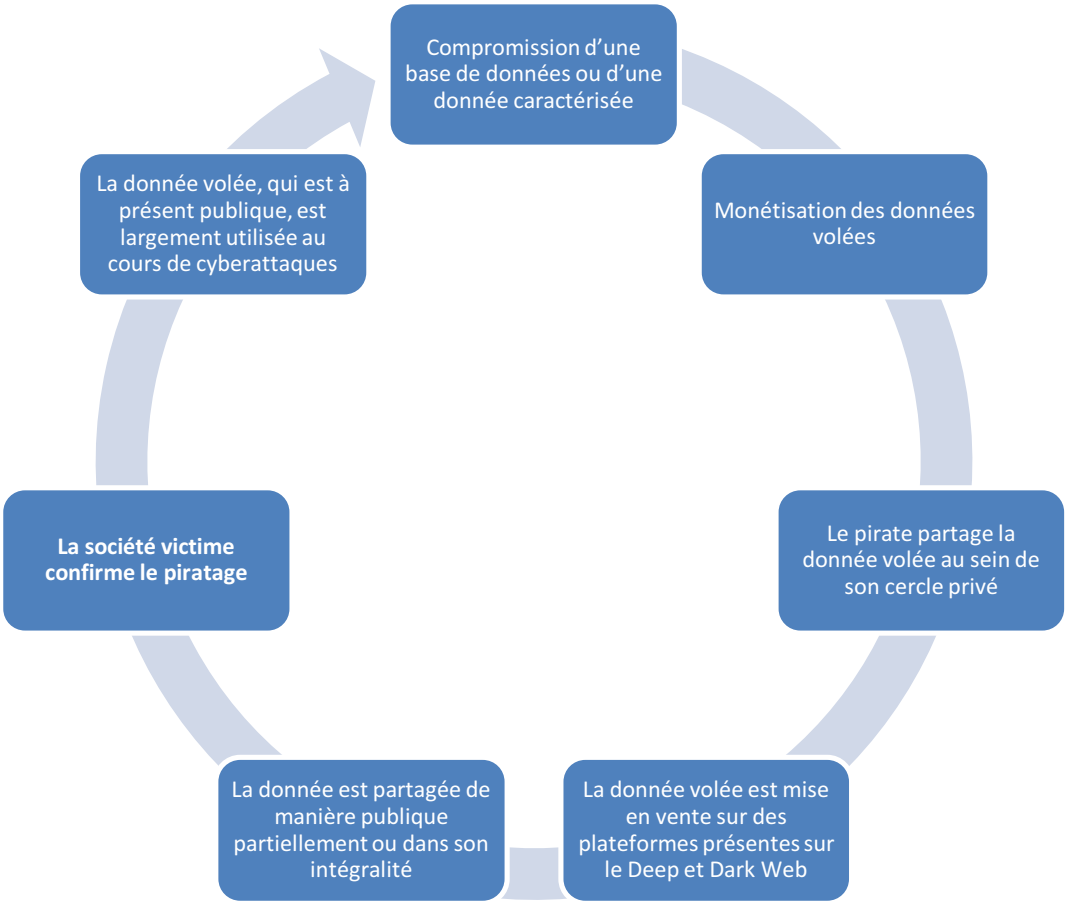
[1] http://www.informationsecuritybuzz.com/expert-comments/petya-ransomware-attack/

LE CYCLE DE VIE DES DONNÉES VOLÉES

Un piratage informatique effectué par un cybercriminel cupide se traduit généralement par **un vol de données**. Les cas les plus courants sont les suivants :

- **La compromission d'une base de données appartenant à une société**. Dailymotion, Yahoo, Tumblr ou encore LinkedIn ont été victimes d'actes malveillants qui ont été révélés en 2016. Ces bases de données dérobées peuvent notamment contenir des identifiants et mots de passe associés, des numéros de cartes bancaires ou encore des coordonnées personnelles d'utilisateurs des plateformes ciblées.
- **Le vol d'une donnée caractérisée appartenant à un particulier**. Leur nature est **quasi-identique** aux données contenues dans les fichiers volés à des entreprises. La différence est que ces données ne sont pas dérobées dans une base de données mais **directement sur la machine des particuliers au travers d'applications ciblées**. A noter que la compromission de l'ordinateur d'un particulier peut également permettre **la compromission du réseau de sa société**. Enfin, cet ordinateur personnel peut aussi contenir **des fichiers sensibles de son entreprise** et pas seulement les données personnelles de la victime.

Une fois le vol effectué, le pirate cherche systématiquement **à monétiser son recel** via différents processus. Il est ainsi possible d'établir un **cycle de vie des données volées** :



- **La compromission d'une base de données ou d'une donnée caractérisée**

Le mode opératoire qui consiste à voler une base de données ou une donnée caractérisée est **quasi-similaire** et ne diffère qu'au moment de l'étape finale :

- Dans un premier temps, l'attaquant envoie **un spam** à sa victime qui peut se présenter sous la forme d'une fausse facture ;
- Ce spam contient **une pièce-jointe malveillante** (par un exemple un fichier Excel ou Word avec une demande d'activation des macros) ou **un lien vers un site d'apparence légitime mais qui est en réalité infecté** ;
- **Les exploits kits**[2] présents dans la pièce-jointe ou sur le site compromis tentent d'exploiter silencieusement un ensemble de vulnérabilités qui pourraient être présentes sur la machine-cible en raison de **la non-application des mises à jour** ;
- Une fois le système compromis, l'attaquant peut :
    - **dérober un fichier sensible,** s'il se trouve sur une machine présente sur un réseau d'entreprise (ou personnelle mais contenant des fichiers professionnels) ;
    - **déployer le malware de son choix** : cheval de Troie bancaire, ransomware, keylogger, etc.) afin de voler une donnée caractérisée.

- **Monétisation des données volées**

La plupart des bases de données volées à une société s'apparentent à **des fichiers clients, fournisseurs, employés ou encore utilisateurs**. Ils contiennent des informations qui peuvent être **d'ordre personnel ou professionnel**. Ces dernières permettent au pirate de mettre en place **des fraudes et escroqueries basées sur de l'ingénierie sociale** comme l'arnaque au président ou escroquerie aux faux ordres de virement.

Des informations bancaires peuvent également être présentes dans ces bases de données. Leur utilisation est alors identique à celles dérobées à un particulier : afin de monétiser son recel, le pirate effectue **des actions de « carding »**, c'est-à-dire qu'il monétise la donnée volée en achetant des produits ou des services sur des plateformes peu sécurisées qui ne disposent pas de protocoles comme « Verified By Visa » ou « MasterCard SecureCode ». Les fraudeurs proposent ensuite ces produits/services **par le biais d'annonces sur les plateformes cybercriminelles underground**. Cette approche leur permet de fournir de réels produits/services **à un prix inférieur à leur valeur réelle d'acquisition** :

[2] https://fr.wikipedia.org/wiki/Exploit_(informatique)

Produit ou service offert	Prix en pourcentage du prix initial
Location de véhicules	25 à 30%
Billets de train	25 à 30%
Produits issus de sites e-commerce (High-tech, prêt-à-porter, parfumerie, pièces automobile/moto)	20 à 25%
Services de restauration	20 à 40%
Cartes cadeaux	25 à 40%
Carding du type drive	20 à 30%
Chambres d'hôtel	25%
Location de villa/appartement	15 à 25%
Location chez un particulier	30%
Location village vacances	20%
Billets événements / concerts / parcs d'attraction	20 à 25%

Source : étude CEIS

Exemple d'une annonce postée sur un forum fermé francophone :

Source : étude CEIS

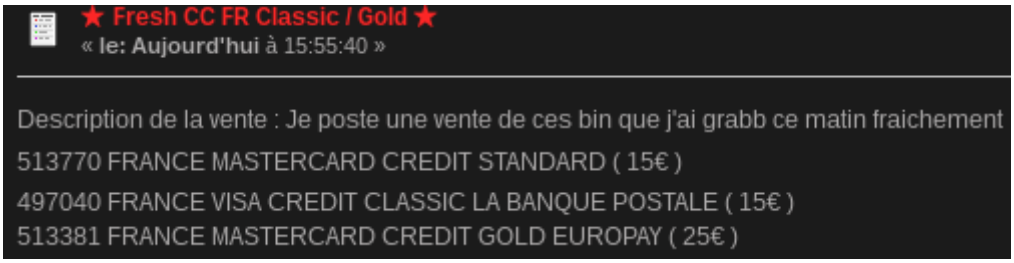
- **Le pirate partage la donnée volée au sein de son cercle privé**

Au lieu d'utiliser la donnée volée à des fins personnelles, l'attaquant peut aussi décider de la partager dans son entourage proche. Cette action s'explique de plusieurs façons : le pirate ne sait pas quoi faire de son butin ou **ignore son processus de monétisation**, il décide alors de s'appuyer sur quelqu'un de plus compétent pour l'épauler dans ses démarches. Une autre possibilité est que le **fraudeur ne dispose tout simplement pas de temps** et préfère déléguer la tâche à une personne de confiance. Enfin, un autre cas de figure possible est **la recherche de notoriété** : un nouveau membre d'une communauté de piratage cherche à faire ses preuves et décide alors **de partager en exclusivité les résultats de son acte malveillant**. Ce fut le cas en février 2015 pour le pirate *ROR[RG]* qui décida de diffuser sur le forum privé underground Hell la base de données clients du site Adult FriendFinder. *ROR[RG]* était un nouveau venu sur la plateforme : il décida d'exposer ses compétences techniques en partageant **de manière exclusive son recel auprès d'une communauté très fermée et élitiste** :

Source : étude CEIS

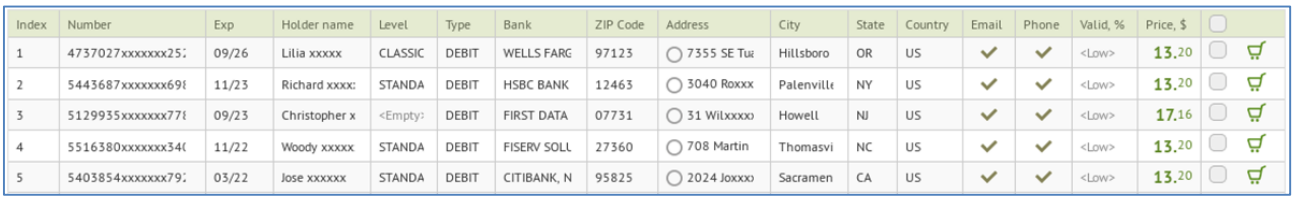
- **La donnée volée est mise en vente sur des plateformes présentes sur le Deep et Dark Web**

Les actions de « carding » nécessitent du temps pour monétiser le numéro de carte bancaire. C'est pourquoi certains pirates préfèrent **directement vendre les données volées sur des plateformes sous la forme d'annonces** :



Source : étude CEIS

La revente directe tend à se professionnaliser. Le principe d'annonces est peu à peu remplacé par le développement de nouvelles plateformes dites **autoshops**. L'acheteur va procéder à l'acquisition des données **bancaires en quelques clics sur une plateforme automatisée sans avoir besoin de communiquer directement avec le vendeur** :



Index	Number	Exp	Holder name	Level	Type	Bank	ZIP Code	Address	City	State	Country	Email	Phone	Valid, %	Price, $
1	4737027xxxxxxx25:	09/26	Lilia xxxxx	CLASSIC	DEBIT	WELLS FARG	97123	7355 SE Tu:	Hillsboro	OR	US	✓	✓	<Low>	13.20
2	5443687xxxxxxx69!	11/23	Richard xxxx:	STANDA	DEBIT	HSBC BANK	12463	3040 Roxxx	Palenville	NY	US	✓	✓	<Low>	13.20
3	5129935xxxxxxx77!	09/23	Christopher x	<Empty>	DEBIT	FIRST DATA	07731	31 Wilxxxx	Howell	NJ	US	✓	✓	<Low>	17.16
4	5516380xxxxxxx34(	11/22	Woody xxxxx	STANDA	DEBIT	FISERV SOLL	27360	708 Martin	Thomasvi	NC	US	✓	✓	<Low>	13.20
5	5403854xxxxxxx79:	03/22	Jose xxxxxx	STANDA	DEBIT	CITIBANK, N	95825	2024 Joxxx	Sacramen	CA	US	✓	✓	<Low>	13.20

Source : étude CEIS

À noter que les autoshops ne concernent plus seulement la vente de données bancaires : ils ont tendance à se diversifier en proposant des couples identifiant / mots de passe associés **à des services de divertissement de type VOD**.

- **La donnée est partagée de manière publique partiellement ou dans son intégralité**

Lorsque les données volées ont été utilisées à des fins personnelles, diffusées au sein du cercle privé et suffisamment monétisées, les attaquants décident alors généralement **de diffuser le résultat de leurs actions – de manière partielle ou intégrale – à un public le plus large possible à des fins de communication/revendication**. Le dernier exemple en date fait suite aux fuites de données émanant du groupe Shadow Brokers, groupe de hackers connu pour avoir dévoilé en 2016 des outils d'espionnages, entre autres, de l'Equation Group, une unité de pirates soupçonnée d'être liée à la National Security Agency (NSA). Le collectif a publié ces données sur Tumblr, GitHub et Pastebin (trois réseaux sociaux et forums très populaires). L'ensemble fut médiatisé à outrance via son compte Twitter (@shadowbrokerss) avec une série de Tweets s'adressant à de grands journaux et chaines de télévision américains[3].

- **La société victime confirme le piratage**

Face à l'impact médiatique engendré par ces actes malveillants, les sociétés victimes n'ont d'autres choix que **de communiquer sur le piratage subi**. Suite à la compromission massive de 500 millions de comptes survenue en 2014 et rendue publique fin 2016, l'entreprise Yahoo publia un communiqué officiel sur son site web en soulignant le fait qu'un groupe sponsorisé par un État était à l'origine de l'attaque[4].

- **La donnée volée, qui est à présent publique, est largement utilisée au cours de cyberattaques**

Une fois la donnée volée partagée de manière publique, cette dernière est **massivement utilisée par les pirates lors de cyberattaques**. Ce fut notamment le cas de la campagne basée sur WannaCry qui toucha plus de 300 000 machines réparties dans environ 150 pays. Le ransomware est couplé à un exploit qui exploite une faille appelée « EternalBlue » de Windows découverte par la NSA. Ce malware est l'un des outils créés par la NSA et qui ont été publiés sur le web le 14 avril 2017 par le groupe de pirate Shadow Brokers.

Le cycle de vie des données volées est « **un cercle vertueux »**. En effet, la dernière étape au cours de laquelle la donnée volée est utilisée lors de cyberattaques **a pour finalité la compromission d'une machine et donc potentiellement un nouveau vol de données**. À ce titre, les identifiants et mots de passe associés de particuliers ou d'employés sont très recherchés par les cybercriminels afin d'accéder à un système d'information. La sensibilisation, les alertes anticipées et les mesures de lutte contre les fuites de données sont essentielles pour réduire les chances de réussite d'une attaque s'appuyant sur les vols de données initiaux.

[3] https://fr.wikipedia.org/wiki/The_Shadow_Brokers

[4] http://webcache.googleusercontent.com/search?q=cache%3Ahttps%3A%2F%2Finvestor.yahoo.net%2Freleasedetail.cfm%3FReleaseID%3D990570&oq=cache%3Ahttps%3A%2F%2Finvestor.yahoo.net%2Freleasedetail.cfm%3FReleaseID%3D990570&aqs=chrome..69i57j69i58.1711j0j4&sourceid=chrome&ie=UTF-8

L'IMPUTABILITE DES CYBERATTAQUES ET LA CHARGE DE LA PREUVE

En février dernier, Guillaume Poupard, directeur général de l'ANSSI, soulignait, devant les sénateurs de la Commission des affaires étrangères, de la défense et des forces armées, que « *la question de l'attribution des attaques [était] le grand problème du cyber. On a la plupart du temps une idée de qui est derrière, mais on ne peut pas prouver l'origine devant un juge par exemple* »[5].

L'attribution consiste à imputer une cyberattaque à un attaquant identifié en y apportant des éléments de preuve. Avec l'augmentation des cyberattaques dans le monde, la question de l'attribution préoccupe les Etats dans la conduite de leurs relations internationales. En effet, l'imputabilité d'une cyberattaque entraine nécessairement des relations conflictuelles entre l'Etat accusateur et l'Etat accusé, d'autant plus que la preuve irréfutable d'une attaque est aujourd'hui encore difficile à apporter.

Pourtant, certains Etats n'hésitent pas à imputer des cyberattaques en tentant d'apporter des éléments de preuve comme les Etats-Unis avec la Russie ou la Corée du Nord. A ce titre, quel rôle jouent alors l'imputabilité et la preuve dans l'attribution d'une cyberattaque en droit international ? Quels sont les principes qui régissent ces deux opérations ? A qui appartient la charge de la preuve et comment est-elle produite ? Enfin, quelle est la portée de l'imputabilité et de la preuve d'une cyberattaque ?

Les principes en matière d'imputabilité et de preuve d'une cyberattaque

Précisons, tout d'abord, que pour la plupart des Etats, le droit international est applicable aux cyberopérations. Le Groupe d'experts gouvernementaux (GGE) ou encore le Manuel de Tallinn 2.0 ont en effet considéré que des cyberattaques peuvent constituer une violation du droit international ou constituer un acte d'agression armée. Ainsi, les principes relatifs aux contre-mesures[6] et à la légitime défense gouvernent l'imputabilité et la preuve des cyberattaques.

En droit international, une cyberattaque doit nécessairement être imputable à un Etat et constituer une violation, par action ou omission, du droit international dans le cadre des contre-mesures ou un acte d'agression armée dans le cadre de la légitime défense. Néanmoins, qu'il s'agisse des contre-mesures ou de la légitime défense, le droit international reconnait qu'une action d'un groupe non-étatique peut être considérée comme imputable indirectement à un Etat, notamment[7] lorsque :

- L'Etat habilite des acteurs privés à exercer des prérogatives de puissance publique ;
- Des acteurs privés agissent sur les instructions, les directives ou le contrôle d'un Etat ;
- L'Etat a reconnu les actions des acteurs privés comme étant les siennes.

[5] http://www.senat.fr/compte-rendu-commissions/20170130/etr.html

[6] « Mesures qui seraient contraires aux obligations internationales de l'Etat lésé vis-à-vis de l'Etat responsable, si elles n'étaient prises par le premier en réaction à un fait internationalement illicite commis par le second, aux fins d'obtenir la cessation et la réparation » (article 1 du projet de la CDI sur la responsabilité).

[7] Projet de la Commission du droit international sur la responsabilité internationale des Etats adoptée en 2001

L'objectif de l'imputabilité pour les Etats victimes d'une cyberattaque est donc de dénoncer une violation du droit international ou une agression armée de la part d'un Etat, ce qui permet alors d'engager une action en responsabilité internationale, l'adoption de contre-mesures ou encore le recours à la force dans le cadre de la légitime défense. Notons que le Conseil de sécurité de l'ONU est également compétent, en vertu du chapitre VII de la Charte des Nations Unies, pour recourir à la force en cas d'agression armée ou de menace contre la paix, et ce même si aucune cyberattaque n'a pour le moment été imputée à un Etat par le Conseil. En revanche, certains Etats comme les Etats-Unis ont, dans la pratique, imputé des cyberattaques à d'autres Etats, en particulier la Russie[8] et la Corée du Nord[9]. En outre, dans le cadre des affaires Sony Pictures et des élections présidentielles américaines, il est intéressant de souligner que les cyberattaques ont été attribuées à des acteurs privés[10] qui auraient agi pour le compte ou sous le contrôle de la Russie et de la Corée du Nord. De son côté, la Corée du Nord a également imputé directement des cyberattaques aux Etats-Unis et à la Corée du Sud[11].

Dans le cadre de ces affaires, les Etats ont généralement imputé les cyberattaques en fournissant certains éléments de preuve sans pour autant que ceux-ci soient irréfutables. Le droit international n'exige d'ailleurs pas des Etats d'apporter des preuves relatives à l'attribution d'une cyberattaque[12]. Plus précisément, le projet sur la responsabilité internationale des Etats de la Commission du droit international de l'ONU exprime le principe en ses termes au sujet des contre-mesures :

« *Un Etat qui prend des contre-mesures le fait à ses propres risques, si sa perception de la question de l'illicéité se révèle mal fondée. Un Etat qui recourt à des contre-mesures en fonction d'une appréciation unilatérale de la situation le fait à ses propres risques et peut encourir une responsabilité à raison de son propre comportement illicite dans l'hypothèse d'une appréciation inexacte* »[13].

Autrement dit, les Etats sont libres d'apporter ou non des preuves de leurs allégations et dans la manière de produire ces preuves. La charge de la preuve et l'administration de la preuve dans le domaine des cyberattaques font cependant débat tant sur le plan du droit international que sur le plan pratique.

Usage de la force à l'encontre d'une cyberattaque	Type de cyberattaques	Principes relatifs à l'imputabilité et à la preuve
Légitime défense	Cyberattaques constituant un acte d'agression armée	* Imputable à un Etat ou à un acteur privé agissant pour son compte * Absence de règle gouvernant l'administration de la preuve mais nécessité de démontrer que la gravité de la cyberattaque constitue un acte d'agression armée
Contre-mesures	Cyberattaques constituant une violation d'une norme internationale	* Imputable à un Etat ou à un acteur privé agissant pour son compte * Absence de règles gouvernant l'administration de la preuve

[8] http://www.liberation.fr/planete/2016/12/15/aux-etats-unis-la-russie-accusee-d-avoir-pirate-la-presidentielle_1535395

[9] http://www.lapresse.ca/international/etats-unis/201412/19/01-4829701-piratage-de-sony-la-coree-du-nord-impliquee.php

[10] Le groupe APT pour la Russie et le groupe Lazarus pour la Corée du Nord

[11] http://www.francetvinfo.fr/monde/coree-du-nord/la-coree-du-nord-accuse-les-etats-unis-de-cyberattaque_281835.html

[12] Dans le cadre de la légitime défense, l'Etat doit cependant démontrer l'existence d'une agression armée. En matière de responsabilité, il reviendra à la juridiction saisie par les Etats de déterminer l'administration de la preuve.

[13] ACDI 2001, *supra* note 19, p. 139, §3.

La charge de la preuve et l'administration de la preuve d'une cyberattaque

En principe, la charge de la preuve incombe à l'Etat qui se prétend victime d'une cyberattaque par un autre Etat. Aucun texte ne vient, en revanche, juridiquement affirmer ce principe, ni préciser les modalités relatives à la charge de la preuve. L'absence de textes encadrant l'administration de la preuve dans l'attribution des cyberattaques laisse alors place au pragmatisme. Celui-ci se heurte cependant à deux obstacles : la difficulté de prouver de façon certaine l'attribution d'une cyberattaque et l'intervention controversée des entreprises du numérique dans les mécanismes d'attribution.

Sur le premier point : des progrès techniques ont été accomplis en matière d'attribution des cyberattaques, notamment dans la collecte et le traitement des logs[14] à l'aide du Big data et du SIEM (Security Event Management)[15] mais aussi avec le développement d'algorithmes capables de reproduire l'expertise humaine dans le domaine de l'attribution des cyberattaques[16]. Toutefois, il reste encore difficile d'identifier avec certitude l'attaquant, notamment lorsque les hackers ont recours à des techniques de dissimulation pour faire croire, par exemple, que l'attaque a été lancée par quelqu'un d'autre[17]. De plus, même si les enquêteurs remontent jusqu'à l'attaquant par le biais d'un faisceau d'indices[18], l'attaquant est généralement un groupe *supposé* privé comme Lazarus en Corée du Nord, ce qui rend d'autant plus difficile l'attribution de l'attaque à l'Etat qui pourra toujours réfuter ses liens avec le groupe privé.

A ces difficultés s'ajoute le fait que des entreprises spécialisées du numérique se chargent d'attribuer des cyberattaques, notamment pour le compte des Etats, ce qui est inédit en droit international[19]. L'intervention du secteur privé dans le domaine de l'attribution peut être risquée, voire même dangereuse : un Etat pourrait en effet être tenté d'encourager cette « attribution privée » pour accuser un autre Etat sans avoir à assumer ce rôle et, inversement, les intérêts des acteurs privés (commerciaux, recherche de gains, publicité) peuvent entrer en contradiction avec ceux de l'Etat. L'intrication publique-privée en matière d'attribution pourrait ainsi avoir des conséquences négatives dans les relations internationales. A ce titre, si le droit international est

---

[14] Les logs sont des données générées par les applications et les équipements réseaux et qui correspondent à l'historique des évènements d'un système d'informations.

[15] https://www.observatoire-fic.com/detecter-les-signaux-faibles-des-cyberattaques-ou-pourquoi-vous-devriez-analyser-vos-logs-par-charles-ibrahim-bull/

[16] https://www.lesechos.fr/03/01/2017/LesEchos/22353-054-ECH_des-algorithmes-pour-traquer-les-coupables-des-cyberattaques.htm

[17] On peut citer à titre d'exemple le document Vault 7 « Marble » de WikiLeaks qui révèle que la CIA dissimule la langue utilisée pour ses malwares, notamment en la remplaçant par une autre comme le chinois, le russe ou encore l'arabe : https://wikileaks.org/vault7/#Marble Framework. Il est également possible de dissimuler l'origine d'une cyberattaque en modifiant les fuseaux horaires dans les métadonnées d'un malware.

[18] Une cyberattaque d'origine étatique peut être détectée à partir du type de malware (APT, notamment non connu et difficilement repérable et à analyser) ; des moyens financiers, humains et techniques utilisés pour mettre en œuvre l'attaque (compétences de très haut niveau, utilisation de codes complexes, infrastructure coûteuse) ; du but poursuivi par l'attaquant (destruction d'infrastructures vitales, vol d'informations sensibles, répercussions politiques).

[19] Pour la première fois, dans l'histoire du droit international, des acteurs privés assument l'imputation d'un fait à l'Etat en lieu et place des acteurs publics.

muet sur l'encadrement des « attributions privées », l'Etat peut toujours venir encadrer la pratique des entreprises privées en droit interne et assurer un contrôle de la pertinence de l'attribution.

Par ailleurs, pour répondre aux problèmes que pose l'attribution des cyberattaques en droit international, il pourrait aussi être envisagé la création d'un mécanisme international d'attribution. Une instance internationale disposant de l'expertise technique nécessaire serait alors chargé d'enquêter sur l'attribution, de manière fiable et indépendante, des cyberattaques pouvant constituer une violation du droit international. Cet organe pourrait s'inspirer de l'Agence internationale de l'énergie atomique (AIEA) ou de l'Organisation internationale pour l'interdiction des armes chimiques (OIAC) qui disposent d'une expertise technique dans leur domaine et la capacité de procéder à des vérifications, notamment en ce qui concerne les déclarations des Etats. Cette proposition qui avait été soulevée au sein du GGE fait cependant l'objet de critiques de certains Etats qui estiment que le mécanisme d'attribution relève de considérations plus politiques que techniques.

Enfin, lorsqu'une cyberattaque est attribuée à un Etat par un autre Etat, la question de la reconnaissance de la responsabilité se pose. La compétence de la Cour internationale de justice (CIJ) pourrait-elle être retenue ? Ou bien serait-il préférable de s'en remettre à une sentence arbitrale ou à une juridiction spécialisée ?

L'engagement de la responsabilité de l'Etat devant la CIJ apparait comme la solution la plus légitime, d'autant plus que la Cour peut prendre toutes les mesures qu'elle estime nécessaire pour l'administration de la preuve[20]. Toutefois, les positions divergentes des Etats sur l'application du droit international aux cyberattaques constituent un obstacle, notamment parce que la compétence de la CIJ demeure facultative et dépend de la volonté des Etats. Il en va de même s'agissant du recours à une sentence arbitrale, même si cette solution présente l'avantage de recourir à un arbitre choisi par les Etats et qui serait qualifié en matière de cyberattaques. Enfin, il pourrait être envisagé la création d'une juridiction internationale spécialisée qui chercherait et poursuivrait les auteurs d'une cyberattaque violant le droit international, à l'instar des tribunaux pénaux internationaux pour le Rwanda et l'ex-Yougoslavie. Néanmoins, pour qu'une telle solution soit retenue, il faudrait qu'une cyberattaque entraine une violation grave du droit international, notamment humanitaire, sur le territoire d'un Etat. Or, aucune cyberattaque n'a atteint pour le moment un tel niveau de gravité.

L'attribution des cyberattaques demeure donc un exercice pratique qui appartient discrétionnairement aux Etats, mais aussi à des acteurs privés agissant pour leur propre compte ou pour celui de l'Etat. En revanche, cette pratique n'est pas encadrée par le droit international, notamment en raison de la portée juridique de l'imputabilité et des preuves d'une cyberattaque.

Portée de l'imputabilité et des preuves d'une cyberattaque

L'attribution d'une cyberattaque, en imputant le fait à un Etat et en y apportant des preuves, n'a pas de véritable portée juridique et constitue, avant tout, une décision politique. Pourtant, l'attribution semble faire l'objet d'une « fiction juridique », c'est-à-dire que le fait d'imputer une cyberattaque à un Etat à l'aide de

[20] http://www.icj-cij.org/documents/index.php?p1=4&p2=2&p3=0&lang=fr

faisceaux d'indices serait juridiquement valable et permettrait, à ce titre, de justifier les mesures que pourrait prendre l'Etat victime.

Ce principe de « fiction juridique » à l'attribution peut avoir des conséquences positives comme négatives sur la conduite des relations internationales en matière de cyberattaques. L'attribution permettrait en effet, d'une part, de légitimer les allégations de l'Etat victime et, d'autre part, de donner l'opportunité à l'Etat accusé de confirmer ou d'infirmer ces allégations sur la base des éléments de preuve qui auront été présentés. En revanche, elle pourrait aussi entrainer davantage de tensions dans les relations internationales, notamment lorsque l'attribution est utilisée pour stigmatiser certains Etats. En outre, l'acceptation du principe de « fiction juridique » pour l'attribution pourrait avoir pour effets de favoriser et faciliter la normalisation du *hack back*.

Quoi qu'il en soit, l'attribution constitue l'une des difficultés majeures dans la maitrise de la conflictualité dans l'espace numérique sur le plan international et soulève la question de savoir s'il est nécessaire d'aller plus loin dans la régulation des cyberopérations menées par les Etats. Si le Manuel de Tallinn 2.0 ou le rapport du GGE de 2015 ont établi le principe de l'applicabilité du droit international au cyberspace, de nombreuses limites existent encore en pratique, ainsi qu'un manque d'harmonisation de la position des Etats sur la manière d'appliquer le droit international aux cyberattaques. Certains Etats entendent donc définir plus clairement ce qui peut être acceptable ou non en matière de cyberopérations à l'aide notamment d'une meilleure coopération internationale, ce qui pourrait se traduire par l'élaboration de normes communes, juridiquement non contraignantes mais politiquement engageantes. En ce sens, Microsoft a émis l'idée de l'élaboration d'une « Convention de Genève » spécifique au cyberespace[21]. Malgré l'avantage indéniable que procure la difficulté d'attribuer des cyberattaques pour les actions malveillantes des Etats, ces derniers, dans un but de pacification des relations internationales, pourraient s'inspirer des initiatives précédemment mentionnées pour réguler et harmoniser la pratique de l'attribution qui en l'état actuel exacerbe des tensions entre certains Etats.

[21] https://www.letemps.ch/opinions/2017/03/26/une-convention-proteger-internautes-temps-paix

La **Direction Générale des Relations Internationales et de la Stratégie (DGRIS)** propose les analyses politiques et stratégiques contribuant à renforcer l'appréciation des situations et l'anticipation. Elle soutient la réflexion stratégique indépendante, en particulier celle menée par les instituts de recherche et organismes académiques français et étrangers. Elle contribue au maintien d'une expertise extérieure de qualité sur les questions internationales et de défense.

A ce titre, la **DGRIS** a confié à **CEIS** la réalisation de cet **Observatoire du Monde Cybernétique**, sous le numéro de marché 1502492543. Les opinions développées dans cette étude n'engagent que leur auteur et ne reflètent pas nécessairement la position du Ministère de la Défense.

Ministère de la Défense
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.eu