Lettre n°61 - **Avril 2017** - **disponible sur omc.ceis.eu**

Brève du mois

« If the German military's networks are attacked, then we can defend ourselves. As soon as an attack endangers the functional and operational readiness of combat forces, we can respond with offensive measures »[1] - Ursula von des Leyen, Ministre de la Défense allemande, à l'occasion de la cérémonie de lancement du nouveau commandement cyber à Bonn.

Table des matières

[1] http://www.reuters.com/article/us-germany-cyber-idUSKBN1771MW

AGENCES DE NOTATION EN CYBERSECURITE : RISQUES ET OPPORTUNITES

A l'instar du risque crédit ou de la responsabilité sociale et environnementale des entreprises, le niveau de cybersécurité des organisations fait désormais l'objet de notations par des sociétés américaines spécialisées. Ces prestataires surfent sur la peur des fuites de données massives et exploitent la crainte, qui se développe au sein du top management des entreprises, particulièrement aux Etats-Unis et dans certains secteurs tels que les services financiers, la santé ou la grande distribution, de voir leur responsabilité mise en cause par les actionnaires ou le régulateur. S'agit-il du dernier avatar de la conformité à l'anglo-saxonne ou d'un véritable progrès pour les entreprises qui peuvent ainsi s'évaluer et se comparer entre pairs ? Quels sont les critères de notation utilisés, en sachant que ces évaluations sont intégralement réalisées depuis l'extérieur des organisations cibles ? Quelles sont les avantages mais aussi les limites de ces dispositifs ? La concentration du marché aux mains de quelques plateformes présente-elle des risques en matière de souveraineté ?

Panorama des agences de notation spécialisées

Depuis 2015, plusieurs agences de notation spécialisées se sont développées aux Etats-Unis, pour certaines de façon très rapide grâce à des grosses levées de fonds. Bitsight domine aujourd'hui le secteur, suivi par SecurityScorecard.

Bitsight	Leader du secteur. Plusieurs offres dont l'une baptisée « BitSight Security Ratings BitSight Discover » destinée aux assureurs pour maitriser leurs agrégats de cyber risques. Bitsight a une filiale portugaise (AnubisNetworks) spécialisée en threat intelligence et proposant des abonnements à des « feeds » de menaces. L'entreprise a levé 49 millions de dollars en 2016 et a également bénéficié d'une subvention de 1 million de dollars de la National Science Foundation américaine. Chiffres clés : en 2016, 47 500 entreprises et organisation avaient déjà évaluées par l'entreprise ; 350 clients ; 180 personnes[2] ; 15 millions de CA en 2015. Site internet : https://www.bitsighttech.com/
SecurityScorecard	Entreprise créée en 2013. Signature d'un contrat avec Zurich Insurance en octobre 2015. A levé 12,5 millions de dollars. Les offres portent à la fois sur le management du risque fournisseur (« security benchmarking for vendor risk management »), l'assurance (« cyber insurance ») et les fusions acquisitions (« private equity »).

[2] http://www.xconomy.com/boston/2016/06/06/bitsight-follows-fico-model-as-cybersecurity-ratings-industry-grows/#

	Site internet : https://securityscorecard.com/
FICO (ex QuadMetrics)	FICO a racheté la société QuadMetrics en 2016. Cette acquisition a permis à FICO, au départ spécialisée dans la notation du risque crédit, de développer une activité spécifique en matière de cybersécurité. Son offre « enterprise security score » est destinée à la fois aux RSSI pour s'évaluer et aux responsables achat ou partenariat pour l'évaluation de partenaires ou fournisseurs. Site internet : http://www.fico.com/en/products/fico-enterprise-security-scoring
RiskRecon	Acteur spécialisé dans l'analyse du risque de cybersécurité fournisseur centré sur le cloud. La société a levé 3 millions de dollars en 2016. Site internet : http://www.riskrecon.com/
UpGuard (anciennement ScriptRock)	L'entreprise a levé 17 millions en 2016. Elle propose 2 offres : vendor Risk Assessment (gestion risque fournisseur et partenaire) et IT security ratings. Site internet : https://www.upguard.com/

Seules sont prises en compte ici les plateformes spécialisées en cybersécurité. On observe par ailleurs que les agences de notation classiques (Moody's, Standard & Poor's, Fitch) commencent à intégrer l'évaluation des cyber-risques parmi leurs critères d'analyse, davantage comme un critère d'accélération des risques traditionnels de solvabilité que comme un risque propre[3].

[3] http://www.lemagit.fr/actualites/4500258259/Le-risque-cyber-pris-en-compte-par-les-agences-de-notation

Comment fonctionnent ces plateformes ?

Les plateformes de notation spécialisées en cybersécurité collectent, grâce à différentes sondes et connecteurs, trois types de données :

- Des données « OSINT » sur les activités malicieuses ;
- Des « data feed » fournis par les « vendors », éditeurs de logiciels et de systèmes de sécurité et acteurs spécialisés en « threat intelligence » ;
- Des « data feed » propriétaires constitués à partir des analyses de vulnérabilités externes régulières sur les réseaux des entreprises évaluées et des capteurs positionnés en divers endroits du réseau internet (infrastructures de type pots de miel ou sinkhole).

Ces données sont ensuite agrégées et permettent, grâce à un algorithme « maison », d'établir des notes par grands indicateurs, puis une note globale. Pour Bitsight, la note globale va de 250 à 900. Pour SecurityScorecard, c'est une lettre de A à F qui est attribuée, tandis que FICO/QuadMetrics va de 0 à 900.

SecurityScorecard

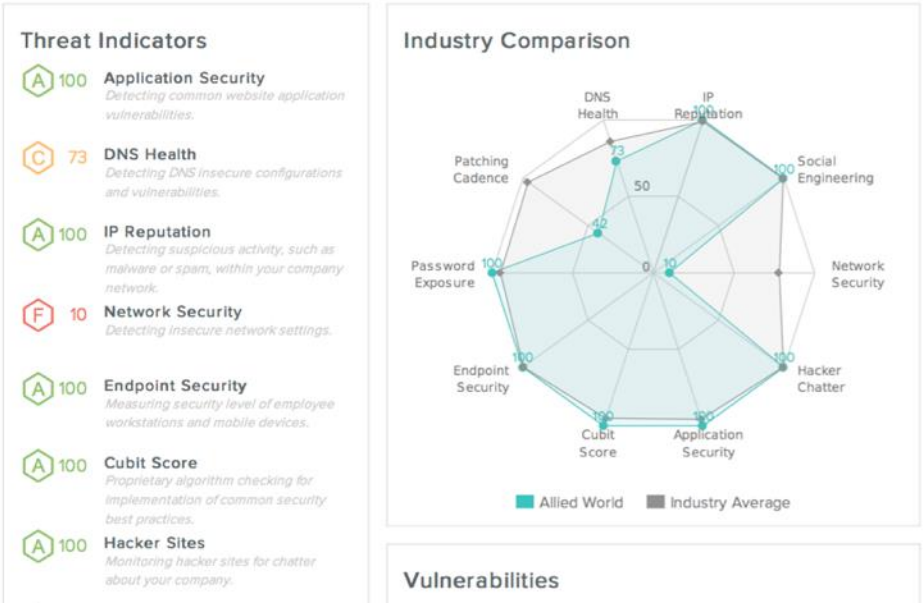
Liste des indicateurs utilisés par SecurityScorecard[4]

Indicateur	*Critère(s) et source(s) de données*
Sécurité des applications web	Vulnérabilités des sites web (*scanning* de vulnérabilités)
Sécurité des postes de travail	Vulnérabilités des *Operating Systems*, des navigateurs internet, version des plugins utilisés etc. (exploitation de métadonnées de connexion)
Sécurité des réseaux	Vulnérabilités des services réseaux (scanning de port[5])
Réputation des adresses IP	Infection des postes d'un réseau d'une entreprise par des malware grâce à la détection de ses adresses IP dans les logs de serveurs de control & command de réseaux botnets contrôlés (« sinkhole » ou « puisards »)
Santé DNS	Analyse de la configuration DNS de l'entreprise et de son historique, protections « anti-spoofing » sur les serveurs de messagerie
Social engineering	Evaluation du degré de perméabilité de l'organisation évaluée à partir de l'analyse des réseaux sociaux et des fuites d'information.
« Hacker chatter »	Apparition du nom de l'entreprise dans les sites underground, les

[4] Source : https://securityscorecard.com/platform/how-it-works/

[5] A noter que la légalité de cette technique fait l'objet de nombreux débats... Cf. note de l'OMC du 2ème trimestre 2013 de l'OMC.

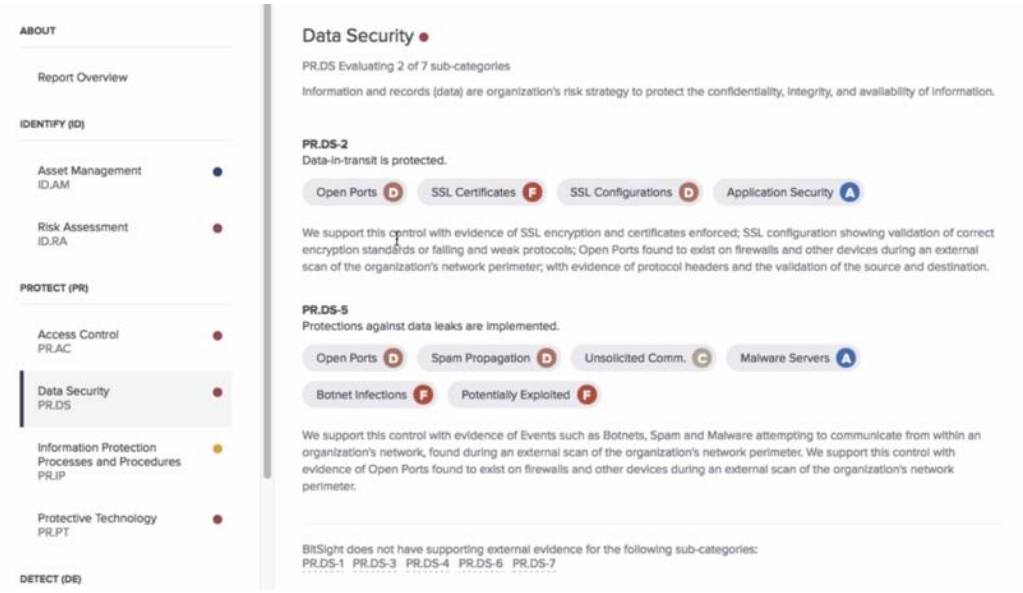
	forums utilisés par les pirates, les réseaux P2P anonymes de type TOR
« Cubit Score »	Algorithme propriétaire permettant d'exploiter les « data feed » fournis par les éditeurs spécialisés et de détecter par exemple des adresses IP appartenant à l'organisation évaluée, analyse des configurations des certificats SSL utilisés etc.
Rapidité de correction (« patching cadence)	Analyse de la période s'écoulant par exemple entre la détection d'un OS vulnérable et la mise à jour de celui-ci.
Fuite de comptes d'accès	Détection sur le « deep web » des fuites de données concernant l'entreprise, principalement des comptes d'accès



Exemple d'évaluation produite par SecurityScorecard[1]

Bitsight

De son côté, Bitsight structure ses évaluations autour des 5 fonctions du référentiel NIST (identifier, protéger, détecter, répondre, remédier) et de 22 catégories, comme l'illustre la saisie d'écran suivante de leur plateforme.



Exemple d'évaluation produite par Bitsight Technologies[1]

L'innovation de ces plateformes semble donc résider principalement dans l'exploitation intelligente de données aujourd'hui éparses, grâce à de nombreux connecteurs et à des technologies big data, et surtout dans un *business model* « multiface » particulièrement efficace.

Un business model innovant

La première caractéristique du *business model* des agences de notation est de s'appuyer sur des plateformes « multiface ». « Plateformes », car l'objectif n'est pas tant de créer un nouveau service ou produit qu'un écosystème composé des entreprises, des tierces parties (fournisseur, partenaire…), des assureurs et courtiers, des administrations, des agences étatiques, etc. « Multifaces », au sens où elles mettent en relation différents types d'acteurs qui s'enrichissent mutuellement en utilisant la plateforme.

Les cas d'usage de ces plateformes sont en effet nombreux :

- Se comparer avec ses concurrents (certaines agences disent ne pas communiquer les notes des entreprises mais simplement des agrégats) ou un ensemble d'entreprises du même secteur ou de même taille ;
- Maitriser le risque fournisseur/partenaires. Dans une optique d'entreprise étendue, les responsables achat / conformité / partenariat disposent d'une plateforme leur permettant de suivre les risques de cybersécurité de leurs contreparties. Particulièrement intéressant pour des offreurs SaaS/IaaS/PaaS/BPaaS ;
- Pour un assureur, proposer en toute connaissance de cause une police d'assurance à un client ;
- Evaluer une cible de fusion / acquisition. La notion de « cybersecurity due diligence » émerge en partant du principe qu'une mauvaise note en matière de cybersécurité reflète potentiellement un problème de gouvernance plus globale.

Pour être efficace, ce *business model* implique cependant pour les principaux opérateurs du marché de disposer très rapidement d'une taille critique significative. Fort de ses différentes levées de fonds, Bitsight a ainsi rapidement réussi à occuper une place de leader avec un « portefeuille » de plus de 50 000 entreprises évaluées à ce jour.

Quels avantages au plan opérationnel ?

Les dispositifs de notation contribuent à développer un cercle vertueux de la cybersécurité que l'on pourrait définir ainsi : 1. les attaques se multiplient, 2. personne n'est à l'abri 3. on ne peut pas se voir reprocher un manquement si l'on a mis en place au préalable les mesures nécessaires (approche « compliance »), 4. Je mets donc en place les mesures de sécurité nécessaires en interne (et éventuellement de transfert du risque résiduel vers un assureur, lequel me demandera, de toutes façons, une telle notation pour me couvrir).

Dans un contexte réglementaire de plus en plus contraignant, y compris en Europe avec le Règlement européen sur les données personnelles, cette approche est donc intéressante, notamment pour des secteurs très régulées. Il n'est d'ailleurs pas anodin de constater que les banques sont parmi les premiers clients des agences de notation en cybersécurité. Une grande banque française nous a ainsi confié avoir déjà pris un abonnement annuel à la plateforme Bitsight.

Le modèle exploite aussi le besoin de comparaison des entreprises entre elle en application de la célèbre maxime de Talleyrand « quand je m'observe, je m'inquiète. Quand je me compare, je me rassure »… Les responsables sécurité, qui doivent justifier leur budget, mesurer le retour sur investissement de leurs actions, convaincre leur top management de la nécessité de tel ou tel achat, y trouvent donc logiquement un intérêt, d'autant que le dispositif présente l'autre avantage de simplifier à l'excès, grâce à une note unique, voire de « gamifier », l'approche de la sécurité….

Le caractère objectif de la note, qui repose sur des indicateurs techniques mesurés automatiquement depuis l'extérieur de l'entreprise (et donc à moindre coût), constitue enfin un autre avantage clé. Et à ceux qui objecteront que cette vision de la sécurité est forcément partielle puisqu'elle ne repose que sur quelques indicateurs, les adeptes de la notation rétorqueront que la mesure des temps de mise à jour des *operating systems* des postes de travail est une indication sérieuse quant à l'efficacité de la politique de sécurité des systèmes d'information interne…

Quelles limites ?

Si l'approche de la sécurité par la conformité est indispensable, elle n'en possède pas moins de sérieuses limites. Conformité et sécurité ne vont pas nécessairement de pair. Une organisation peut être conforme sans pour autant atteindre un niveau de sécurité satisfaisant. Aborder la sécurité uniquement à travers le prisme de la conformité à des normes génériques revient donc à prendre la sécurité par le petit bout de la lorgnette, avec pour objectif premier de se « couvrir » en cas de problème… Une pratique souvent d'inspiration anglo-saxonne, comme le souligne Matthieu Le Louer, directeur des systèmes de paiement client chez AccordHotels.com dans un récent livre blanc de la FEVAD : *« l'approche anglo-saxonne donne parfois l'impression que le dédouanement de la responsabilité (que permet la conformité à la norme) est*

parfois aussi important que la mise en place des mesures qui empêcheraient la survenue des incidents. Nous, nous cherchons avant tout à éviter que le problème ne survienne. Eux cherchent à savoir qui portera la responsabilité si l'incident se produit ». [6]

Cette approche par la conformité ne suffit donc pas à rendre compte de toutes les dimensions de la sécurité. Elle doit être surtout vue comme un prérequis, pas une finalité en soi. Par ailleurs, les notes proposées s'appuient presque intégralement sur des analyses de vulnérabilités, sans tenir compte du contexte spécifique de l'entreprise et de son exposition aux risques. Or, quelles que soient les vulnérabilités qu'elles comportent, les entreprises sont plus ou moins exposées en fonction de leurs secteurs d'activité, de leur taille, de leur implantation géographique etc. Une approche « par les risques », individualisée, couplant audit interne et externe, reste donc indispensable et permettra de combiner une analyse précise des vulnérabilités techniques mais aussi humaines et organisationnelles de l'organisation et une vision à 360° du contexte externe (menaces).

L'aspect « boite noire » des évaluations et des algorithmes utilisés est également de nature à susciter la méfiance. Comment s'assurer par exemple de la cohérence dans le temps de la note lorsque les types de données utilisées évoluent et que l'algorithme est mis à jour ? Ces notations peuvent d'ailleurs être perçues comme très intrusives par les entreprises qui ne peuvent pas refuser d'être notées (bien que certains prestataires affirment que « l'opt-out » reste possible…), puisque l'évaluation est faite intégralement depuis l'extérieur. En cas de contestation, l'entreprise peut seulement « faire appel » de sa note (BitSight a ainsi nommé un *Ombudsman* extérieur qui sert d'arbitre) et demander une réévaluation si elle n'est pas d'accord.

Les agences ont donc potentiellement une responsabilité considérable quant à la réputation des entreprises notées. Avoir la capacité d'influencer le classement des entreprises signifie potentiellement pouvoir influencer le choix d'un prestataire au détriment d'un autre…

Quels risques en termes de souveraineté ?

Au-delà de cette dimension intrusive pour les entreprises évaluées, le développement de ces agences soulève une véritable question de souveraineté. La domination de ce nouveau *business* de la conformité par des agences américaines place celles-ci en position de « juge de paix » en leur permettant potentiellement de collecter et de traiter des données sensibles sur les entreprises non américaines. Aux données externes collectées s'ajouteront sans doute demain des données internes encore plus sensibles fournies volontairement par les entreprises évaluées, soucieuses d'améliorer leurs notes et désireuses de « laver plus blanc que blanc » pour l'obtention de tel ou tel contrat ou partenariat.

BitSight vient d'ailleurs d'annoncer qu'elle entendait désormais attribuer des notes souveraines[7] pour évaluer les performances collectives de cybersécurité des Etats, entreprises et opérateurs d'infrastructures vitales. Contrairement au Global Cybersecurity Index de l'UIT[8] qui mesure le niveau d'engagement des pays sans

[6] Livre blanc « Sécurité et e-commerce », FEVAD, octobre 2016, http://hermus.fr/wp-content/uploads/2016/11/FEVAD_Livre-Blanc_vf.pdf

[7] https://www.bitsighttech.com/sovereign-security-ratings

[8] http://www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI.aspx. Ce classement, basé sur des questionnaires, évalue le niveau d'engagement dans les domaines suivants : cadre juridique, mesures techniques,

chercher à évaluer l'efficacité des mesures prises, ce sera donc la performance de sécurité et le niveau d'hygiène numérique des Etats qui seront évalués, et surtout publiés *urbi et orbi*. Avec une dimension vertueuse sur le niveau de sécurité global, mais aussi des conséquences importantes pour les Etats et pour les entreprises, qui seraient moins bien notés. Ceux-ci seront alors contraints de se mettre au niveau, pour le plus grand bénéfice des éditeurs américains de cybersécurité, leaders du marché, ou risqueraient de voir leur attractivité et compétitivité sérieusement mises à mal au profit d'acteurs présentant des notes irréprochables. La notation de cybersécurité pourrait ainsi devenir un nouvel outil au service de la domination commerciale américaine, à l'image du Foreign Corrupt Practices Act (FCPA) américain de 1977 qui s'est progressivement imposé comme la norme universelle en matière de conformité éthique et financière…

structures organisationnelles, renforcement des capacités et coopération internationale. La France apparaît en 9ème position dans le classement de 2015.

DE L'OPPORTUNITE DU HACK-BACK

Les 6 et 7 avril 2017 s'est tenue la conférence internationale « Construire la paix et la sécurité internationales de la société numérique » à l'UNESCO[9]. Lors de cette conférence, un sujet a particulièrement retenu l'attention des acteurs publics et privés : le hack back. Cette pratique peut être définie comme « *le fait, pour la victime d'une cyberattaque, de riposter contre son* auteur »[10]. Le hack back s'inscrit dans une cyberdéfense active. Elle comprend les techniques de riposte qu'une victime peut employer afin de causer la mise hors service des réseaux et systèmes de l'attaquant, mais également le recueil de données sur celui-ci ou encore la récupération de données dérobées.

L'intérêt que suscite aujourd'hui le hack back, tant pour les Etats que pour le secteur privé, fait l'objet de controverses. Plus encore en ce qui concerne le secteur privé où le hack back est considéré comme une pratique illégale. Généraliser sa pratique constituerait-il une opportunité tant pour la cyberdéfense que la cybersécurité ? Quel est l'état actuel de la pratique pour les acteurs publics et privés ? Est-il possible d'encadrer juridiquement le hack back ? Enfin, le hack back présente-t-il plus d'avantages ou d'inconvénients ?

L'état actuel de la pratique du hack back

Selon l'étude « Cyberattaques – Prévention-réactions : rôle des Etats et des acteurs privés » de Karine Bannelier et Théodore Christakis[11], il faut distinguer le hack back encadré du hack back sauvage.

Le premier concerne les Etats et les entreprises privés mandatées pour le compte de celui-ci. Ce hack back encadré est soumis aux règles du droit international et le recours à une telle pratique engage la responsabilité de l'Etat, qu'il ait agi directement ou par l'intermédiaire d'une entreprise. En outre, Les pays industrialisés prévoient, en droit interne, la possibilité pour l'Etat de répondre aux attaques. Ainsi, la Grande-Bretagne a annoncé, en 2016, sa volonté de recourir au hack back dans le cadre d'une attaque contre sa souveraineté ou ses infrastructures[12]. De même, l'article 21 de la loi de programmation militaire française de 2013 prévoit que des agents habilités de l'Etat peuvent s'introduire dans les infrastructures d'un attaquant afin de faire cesser une attaque[13].

---

[9] https://jesuisinternet.today/

[10] Karine BANNELIER et Théodore CHISTAKIS, *Cyberattaques – Prévention-réactions : rôle des Etats et des acteurs privés*, Les Cahiers de la Revue Défense Nationale, Paris, 2017, p. 61.

[11] Karinne Bannelier est maître de conférences-HDR à l'Université Grenoble Alpes et Théodore Christakis est professeur à l'Université Grenoble Alpes et à l'institut Universitaire de France.

[12] http://securityaffairs.co/wordpress/52966/cyber-warfare-2/uk-active-defence.html

[13] http://www.lefigaro.fr/secteur/high-tech/2017/04/10/32001-20170410ARTFIG00136-cyberguerre-une-course-a-l-armement-preoccupante.php

De son côté, le hack back sauvage, qui ne concerne que les entreprises privées agissant dans le cadre de leur propre sécurité, est considéré comme illégal. En effet, si le droit international reste muet sur cette question, la plupart des législations nationales, sous l'impulsion notamment de la Convention de Budapest sur la cybercriminalité de 2001 du Conseil de l'Europe, prohibent cette pratique. En France, la loi Godfrain sanctionne pénalement les atteintes aux systèmes de traitement automatisés de données, sans distinction de motif[14]. Il en va de même pour la loi américaine « Computer Fraud and Abuse Act (CFAA) »[15].

Pourtant, la question du recours au hack back pour les entreprises privées afin de répondre à leur besoin en cybersécurité se pose de plus en plus, notamment avec l'augmentation des cyberattaques. A ce titre, on peut citer l'affaire marquante de Sony Pictures qui aurait sollicité une société de cybersécurité pour déclencher une attaque DDoS contre des serveurs qui hébergeaient des données volées à l'entreprise en 2014[16]. Peu de temps après, dans le cadre de son enquête sur une attaque de type DDoS contre la banque américaine JPMorgan, le FBI a découvert qu'une tierce personne avait lancé une contre-attaque sur les serveurs utilisés par les attaquants. De ce fait, le FBI a ouvert une seconde enquête afin de savoir si une entreprise américaine était à l'origine de la contre-attaque[17]. Ainsi, il existerait, dans le secteur privé, une utilisation officieuse du hack back, à plus forte raison parce que cette pratique se situe dans une « zone grise » de la cyberdéfense active[18]. En ce sens, il est aujourd'hui difficile de savoir avec certitude quelles sont les techniques offensives qui relèvent du hack back et donc qui entrent ou non dans le cadre de la loi. Par exemple, dans le cas d'une cyberattaque ayant pour objet de voler des données, la victime peut vouloir entreprendre une mission de récupération de ces données sans pour autant être dans une position de contre-attaque vis-à-vis de l'attaquant. Autrement dit, une même action technique peut être perçue comme du hack back ou comme une mission de sauvetage selon l'intentionnalité[19] de la victime. Cependant, dans les deux cas, la mesure présente un risque et constitue une action illégale alors qu'elle pourrait être perçue comme légitime.

[14] http://www.netpublic.fr/wp-content/uploads/cyberbase/5348/5348_piece_jointe_27.pdf

[15] https://energy.gov/sites/prod/files/cioprod/documents/ComputerFraud-AbuseAct.pdf

[16] http://time.com/3629768/sony-hack-hackers/

[17] https://www.bloomberg.com/news/articles/2014-12-30/fbi-probes-if-banks-hacked-back-as-firms-mull-offensives

[18] https://cchs.gwu.edu/sites/cchs.gwu.edu/files/downloads/CCHS-ActiveDefenseReportFINAL.pdf

[19] Le terme « intentionnalité » est entendu au sens juridique, c'est-à-dire que l'intention de la victime est déterminée par son comportement

FIGURE 2. ACTIVE DEFENSE: THE GRAY ZONE

Source: GWU CCHS “Into the Gray”

Par ailleurs, il apparait que l’idée d’un droit à la légitime défense pour les entreprises privées victimes d’une cyberattaque pourrait être envisageable[20]. En effet, depuis quelques années, des discussions sont engagées afin de légaliser le hack back et d’en préciser les limites. Aux Etats-Unis, une proposition de loi souhaite d’ailleurs légaliser la pratique. En revanche, tous les Etats ne sont pas en faveur de la légalisation du hack back, notamment parce qu’il est très difficile de définir des critères juridiques applicables à cette pratique.

Une légalisation encore incertaine

En février 2017, le député américain Tom Graves a introduit la proposition de loi « Active Cyber Defense Certainty Act » qui a pour objet de légaliser le hack back pour les entreprises privées victimes d’une cyberattaque[21]. Cependant, l’idée d’une légalisation du hack back en droit américain n’est pas nouvelle puisqu’il avait déjà été envisagé, en 2013, de réglementer cette pratique pour lutter contre les atteintes à la propriété intellectuelle[22]. Dans ce cadre, le hack back avait seulement pour objectif de permettre à la victime de retrouver les informations dérobées par un attaquant ou de les rendre indisponibles[23]. Il ne s’agissait donc pas d’autoriser des mesures telles que l’implantation d’un malware chez l’attaquant qui aurait une finalité de sabotage de son ordinateur. Ainsi, il avait été recommandé de permettre de recourir légalement au hack back en précisant, toutefois, que les mesures ne devaient pas causer de dommages à des tierces personnes. Il est à noter que cette recommandation de légalisation dans le domaine de la propriété intellectuelle s’inscrivait dans le cadre particulier de la politique étrangère des Etats-Unis vis-à-vis de la Chine, soupçonnée de mener une politique industrielle encourageant les atteintes à la propriété intellectuelle.

[20] https://www.ft.com/content/c75a0196-2ed6-11e5-8873-775ba7c2ea3d

[21] https://tomgraves.house.gov/uploadedfiles/discussion_draft_ac-dc_act.pdf

[22] http://www.ipcommission.org/report/IP_Commission_Report_052213.pdf

[23] http://www.bankinfosecurity.com/panel-use-hack-back-to-mitigate-ip-theft-a-5784

Afin de répondre aux risques que représentent les cyberattaques pour le secteur privé et de dissuader leurs auteurs d'agir en tenant compte des difficultés qu'il y a à appréhender légalement ceux-ci, le député Tom Graves souhaite aujourd'hui mettre en place un droit de légitime défense au profit des victimes[24]. Selon le député, l'« Active Cyber Defense Certainty Act », qui a pour objet de modifier la loi « Computer Fraud and Abuse Act », suscite l'intérêt du secteur privé, mais aussi des politiques qui pourraient voter la loi dans les mois à venir. Le projet de loi délimite le champ d'application du hack-back de la façon suivante :

- Le terme de victime signifie toute personne ou organisation victime d'une intrusion non autorisée persistante dans son système d'information ;
- La riposte doit être opérée par la victime ou à sa demande. Elle consiste à accéder sans autorisation à l'ordinateur de l'attaquant afin de récupérer des informations sur l'identité de ce dernier et les partager avec les autorités, ou pour faire cesser l'attaque ;
- Les mesures entrainant la destruction d'informations stockées dans des systèmes d'information de personnes autres que l'attaquant, causant des dommages physiques à une autre personne ou créant une menace pour l'ordre public et la sécurité sont exclues du champ de la loi.

L'« Active Cyber Defense Certainty Act » offre une définition insuffisamment précise du hack back et soulève un certain nombre de questions[25]. En effet, selon la définition de l'attaque pouvant faire l'objet d'une riposte, les victimes d'attaques DDoS ne pourraient pas se prévaloir de la loi puisque celle-ci ne constitue pas une intrusion persistante. En outre, les termes « persistent » et « intrusion » peuvent faire référence à de nombreuses situations et faire l'objet de différentes interprétations. La proposition de loi ne précise pas non plus suffisamment ce que l'on peut entendre par « the computer of the attacker », notamment dans le cas d'une chaine d'ordinateurs qui intervient dans l'attaque. Enfin, la proposition de loi qui prévoit d'exclure certaines mesures du régime du hack back légal n'envisage pas certaines situations telles que le risque de modifications des informations stockées dans d'autres ordinateurs ou de rendre indisponibles ces données ou des services, le texte ne proposant d'exclure que les mesures entrainant la destruction d'informations.

Si la proposition de loi américaine tente de légaliser la pratique du hack back tout en la limitant, de nombreuses questions entourent cette pratique. A ce titre, les questions de la régulation et du contrôle des armes informatiques occupent une place importante dans la limitation du hack back et nécessite un consensus au niveau international[26]. En effet, la généralisation de la vente d'armes informatiques entrainerait nécessairement une augmentation de la pratique du hack back. A ce sujet, la France souhaiterait rendre universel l'arrangement de Wassenaar[27] dans l'optique d'interdire toute forme de hack back qui constituerait, selon David Martinon, une internationalisation du second amendement de la Constitution des Etats-Unis qui permet de porter une arme[28], et serait donc susceptible d'entrainer une prolifération des cyber armes.

Enfin, bien que le hack back fasse l'objet de discussions sur sa légalisation et d'une proposition de loi aux Etats-Unis, les risques que présente cette pratique sont nombreux, notamment en ce qui concerne le risque

[24] https://www.cyberscoop.com/hacking-back-bill-tom-graves-active-cyber-defense-certainty-act/

[25] https://www.lawfareblog.com/legislative-hackback-notes-active-cyber-defense-certainty-act-discussion-draft

[26] http://www.liberation.fr/futurs/2017/04/05/l-ideal-du-numerique-peut-devenir-une-sorte-de-leviathan_1560817

[27] Etabli le 12 mai 1996, l'arrangement de Wassenaar coordonne les politiques de 41 pays, dont la France, les Etats-Unis et la Russie, sur le contrôle des exportations d'armes conventionnelles et de biens technologiques à double usage

[28] http://www.silicon.fr/3-propositions-france-enrayer-course-armements-cyber-171815.html

d'endommager un ordinateur innocent utilisé par un cyberattaquant, sujet qui fait l'objet d'une attention particulière pour l'encadrement du hack back[29]. Quoi qu'il en soit, le hack back présenterait plus de risques que d'avantages selon la majorité des experts.

Un bilan avantages/inconvénients en défaveur du hack back

A l'instar de l'étude menée par Karine Bannelier et Théodore Christakis, de nombreux écrits sont consacrés à la présentation des avantages et des inconvénients du hack back[30]. De manière générale, le hack back aurait notamment pour avantages :

- De pallier l'insuffisance des autorités gouvernementales pour assurer la sécurité des entreprises contre les cyberattaques ;
- D'être un moyen plus rapide et efficace pour faire cesser une cyberattaque ;
- D'éviter la divulgation des vulnérabilités des entreprises.

A l'inverse, il pourrait avoir pour conséquences :

- Une escalade des cyberattaques ;
- Un risque pour les relations diplomatiques ;
- De freiner l'activité de lutte contre la cybercriminalité ;
- De provoquer des dommages à des tierces personnes ;
- De créer une disparité entre les acteurs pouvant recourir au hack back et ceux qui ne le peuvent pas et ainsi déstabiliser la société numérique ;
- Plus encore, le hack back pourrait avoir des effets pervers en donnant l'opportunité à des entreprises d'attaquer leurs concurrents dans un contexte où l'imputabilité des cyberattaques est difficile à déterminer[31].

Pour de nombreux experts en cyberdéfense et en cybersécurité, la pratique du hack back présente plus d'inconvénients que d'avantages et provoquerait une augmentation de la conflictualité dans le cyberespace[32]. Par ailleurs, le FBI a toujours conseillé aux victimes de cyberattaques de ne pas riposter à une attaque afin de ne pas entraver les enquêtes et de ne pas causer de dommages collatéraux[33]. En ce sens, James Comey, l'actuel directeur du FBI, s'est opposé publiquement à l'idée de légaliser le hack back[34].

Si la question de la généralisation du hack back est devenue une importante préoccupation tant d'un point de vue juridique que pratique en matière de cyberdéfense active, d'autres alternatives sont actuellement en voie de développement. Ainsi, la France souhaite introduire l'idée d'une obligation de vigilance de la part des

---

[29] http://www.bankinfosecurity.com/interviews/legal-merits-hack-back-strategy-i-1729

[30] A titre d'exemple, il peut être mentionné un article de 2016 de l'U.S. National Science Foundation : http://ethics.calpoly.edu/hackingback.pdf

[31] http://www.silicon.fr/le-droit-a-la-cyber-riposte-pour-tous-inquiete-anssi-170414.html

[32] http://www.bankinfosecurity.com/case-against-hack-back-a-7759

[33] https://www.justice.gov/sites/default/files/opa/speeches/attachments/2015/04/29/criminal_division_guidance_on_best_practices_for_victim_response_and_reporting_cyber_incidents.pdf

[34] https://motherboard.vice.com/en_us/article/fbi-director-tells-companies-not-to-hack-back-against-hackers

Etats afin de réguler, prévenir et responsabiliser les acteurs pouvant user du hack back[35]. D'autre part, le développement de capacité défensives reposant sur l'apprentissage machine, auxquelles seules les entreprises (et les Etats) pourraient prétendre, pourrait réduire en grande partie la justification du hack-back.

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

[35] http://www.liberation.fr/futurs/2017/04/05/l-ideal-du-numerique-peut-devenir-une-sorte-de-leviathan_1560817