Lettre n°65 - Août 2017 - disponible sur omc.ceis.eu

Brève du mois

«It will always be a requirement to bring together our coalition partners and move to combining doctrine with operations to create a better model. We all go about cyber in a different manner, and by taking advantage of the visiting national military representatives and senior leaders being here, we help build the community framework. »[1] - Brigadier général Robert Mazzolin, vice-directeur des projets et stratégies de des états-majors de la défense canadienne.

TABLE DES MATIERES

[1] https://www.defense.gov/News/Article/Article/1238082/

GAFA : UN ROLE CROISSANT EN MATIERE DE REGULATION DES CONTENUS

La régulation d'Internet préoccupe les Etats qui souhaitent renforcer les moyens de contrôle des contenus jugés illicites. En témoignent les récentes discussions franco-britanniques sur la responsabilité des GAFA dans le cadre de la lutte contre le terrorisme[2]. Des entreprises comme Google, Twitter ou Facebook sont en effet en première ligne dans la modération des contenus diffusés sur internet. Le secteur privé assure ainsi, à la place des autorités publiques, l'équilibre entre la censure et la sauvegarde des libertés sur les réseaux sociaux ou les moteurs de recherche. Cette situation inédite ne va pas sans soulever de nombreuses questions politiques, juridiques ou techniques. Comment les GAFA définissent-ils un contenu illicite ? Quels sont les outils et les moyens dont ils disposent pour réguler ces derniers ? Quelles en sont les conséquences politiques et juridiques ?

Définition d'un contenu illicite

Les plateformes du web peuvent être amenées à modérer un contenu (image, son, texte, vidéo) lorsque celui-ci est considéré contraire aux conditions générales d'utilisation du service (CGU) ou considéré illicite au regard de la loi.

Sur le premier point, Google, Facebook et Twitter définissent de la même manière les contenus illicites dans leurs CGU : il s'agit des contenus à caractères terroriste, haineux ou encore pédopornographique. Les standards définis par les GAFA dans leurs CGU ont également en commun leur application universelle, c'est-à-dire qu'ils s'appliquent à tous les utilisateurs quel que soit le pays. En outre, les GAFA s'appuient sur les textes internationaux relatifs aux droits fondamentaux et les législations démocratiques pour définir les contenus considérés comme illicite dans leur CGU.

Par ailleurs, il est intéressant de noter que les plateformes russe et chinoise (Vkontakte et WeChat) adoptent des CGU similaires à celles des GAFA. En revanche, la proximité de ces plateformes avec les gouvernements russe et chinois, étant donnée la législation stricte encadrant l'usage d'internet dans ces pays, laisse à penser que ces plateformes interprèteront leur CGU en fonction des directives des autorités.

[2] http://www.zdnet.fr/actualites/contenus-illegaux-france-et-uk-plaident-pour-une-responsabilite-legale-des-gafa-39853608.htm

Contenus illicites selon les CGU des différentes plateformes (liste non exhaustive)

Plateforme	Contenus illicites
Google[3]	• Contenu visuel choquant et violent ; • Contenu à caractère terroriste ; • Contenu à caractère explicitement sexuel ; • Incitation à la haine ou à la violence ; • Harcèlement, intimidation, menaces ; • Mise en danger d'enfants ; • Encouragement des activités dangereuses ou illégales.
Twitter[4]	• Contenu cru (sexuel notamment) ; • Menaces violentes (terrorisme notamment) ; • Harcèlement ; • Conduite haineuse ; • Diffusion d'informations privées ; • Usurpation d'identité ; • Conduite autodestructrice.
Facebook[5]	• Menaces de violence physique, de vol, vandalisme, préjudices financiers ; • Incitation au suicide ou à l'automutilation ; • Contenu soutenant des groupes impliqués dans des activités violentes ou criminelles (terrorisme notamment) ; • Harcèlement ou intimidation ; • Propos haineux ; • Incitation à la violence ou à l'exploitation sexuelle.
WeChat[6]	• Contenu violent ; • Harcèlement ; • Encouragement au suicide ou à l'automutilation ; • Contenu à caractère pornographique ou sexuellement explicite ; • Usage pour des activités illégales ou potentiellement illégales selon l'appréciation de WeChat.
Vkontakte[7]	• Propagande raciste, fasciste, religieuse, ethnique ; • Divulgation d'informations sur des secrets d'affaires ou d'Etat ; • Propagande d'activités criminelles.

Si certains contenus peuvent être facilement identifiés comme illicites, d'autres se situent dans une « zone grise ». Si l'identification de contenus à caractère terroriste ou pédopornographique ne soulève pas de difficulté puisqu'il existe de nombreux textes internationaux, législatifs et réglementaires qui définissent le terrorisme ou la pédopornographie à travers le monde et de manière uniforme, il n'en va pas de même pour les contenus haineux ou à caractère sexuel qui peuvent recevoir des interprétations différentes selon les pays et les cultures. Ainsi, lors de la modération d'un contenu se situant dans la « zone grise », les GAFA s'adapteront à la législation locale applicable au contenu litigieux. A titre d'exemple, en matière de contenus haineux, les discours négationnistes sont définis pénalement en France mais pas aux Etats-Unis. En outre, certains contenus controversés peuvent apparaitre licites mais contenir des informations illicites. Exemple :

[3] https://support.google.com/youtube/topic/2803176?hl=fr&ref_topic=2676378

[4] https://support.twitter.com/articles/75576#

[5] https://www.facebook.com/communitystandards

[6] http://www.wechat.com/en/acceptable_use_policy.html

[7] https://vk.com/terms

les vidéos qui contiennent des contenus controversés à caractère religieux ou suprémaciste sans pour autant être interdites par les CGU de la plateforme[8].

Afin de clarifier cette « zone grise », certains pays adoptent une législation spécifique. On peut citer le cas de la « loi Facebook » israélienne qui a pour objectif de permettre à la justice de l'Etat hébreu de contraindre les GAFA à supprimer des contenus incitant à la haine et à la violence tels qu'ils seront définis par le texte[9]. Ce projet de loi fait toutefois l'objet de critiques en raison des craintes qu'il suscite sur les risques de dérives dans la censure par les autorités. En France, la loi pour la confiance dans l'économie numérique (LCEN) de 2004 précise de son côté que les entreprises telles que les GAFA doivent réguler les contenus « manifestement » illicites. Autrement dit, la loi française oblige les GAFA à réguler les contenus illicites facilement identifiables (terroriste ou pédopornographique par exemple) tout en laissant la régulation des contenus se situant dans la « zone grise » à l'appréciation des GAFA.

Outils et moyens de régulation des contenus illicites

L'un des enjeux de la régulation des contenus illicites concerne la capacité des plateformes à détecter et modérer un contenu le plus rapidement possible sans pour autant entrer dans une censure abusive. Il est ainsi nécessaire de mettre en place des dispositifs humains et techniques adéquats.

L'utilisation de l'IA et la place de l'humain dans la modération

Afin de mieux détecter les contenus illicites, les GAFA se reposent de plus en plus sur l'Intelligence artificielle (IA). Les techniques de correspondance d'image (*photo matching*) ou d'analyse sémantique reposant sur l'apprentissage machine (*machine learning*) sont en effet devenus suffisamment performantes, notamment dans la détection des contenus illicites facilement identifiables tels que les contenus terroriste ou pédopornographique[10].

Les contenus se situant dans la « zone grise » tels que les discours haineux nécessitent cependant d'être modérés à l'aide de l'expertise humaine en raison des considérations culturelles et linguistiques qui sont attachées à ce type de contenu. C'est la raison pour laquelle Facebook a annoncé le recrutement de 3000 modérateurs supplémentaires[11]. L'intervention humaine reste également essentielle pour décider du retrait d'un contenu afin d'éviter toute censure systématique et limiter le risque de faux positifs. A titre d'exemple, l'IA actuellement employée, à l'instar de celle développée par Facebook pour les contenus à caractère

[8] http://www.lemonde.fr/pixels/article/2017/08/15/messages-blocages-et-demission-apres-charlottesville-la-silicon-valley-reagit_5172607_4408996.html

[9] http://www.rfi.fr/moyen-orient/20170313-israel-loi-facebook-fait-craindre-derives

[10] https://www.theguardian.com/technology/2017/aug/01/google-says-ai-better-than-humans-at-scrubbing-extremist-youtube-content

[11] http://www.lemonde.fr/pixels/article/2017/05/03/facebook-va-embaucher-3-000-moderateurs-supplementaires-d-ici-un-an_5121678_4408996.html

terroriste[12], ne permet de détecter et supprimer préventivement que les contenus qui ont déjà fait l'objet d'une censure.

Les capacités d'intelligence artificielle, dans lesquelles les GAFA investissent lourdement, devraient cependant nettement progresser dans un futur proche[13]. De son côté, WeChat, application mobile de messagerie textuelle et vocale développée par le Chinois Tencent, a annoncé vouloir développer l'intelligence artificielle pour lutter contre les contenus jugés illicites par les autorités chinoises. Des filtres équipent d'ailleurs les services WeChat dans le cadre de la censure chinoise de l'Internet[14].

Les autres mesures de modération

D'autres techniques sont également mises en œuvre, comme la mise en valeur de discours alternatifs grâce à des algorithmes analysant les requêtes des internautes et proposant des « contre-discours ». Grâce à l'outil Redirect Method développé par la branche Jigsaw de Google[15], un aspirant djihadiste se verrait ainsi redirigé en direct vers des contenus alternatifs comme des témoignage de djihadistes repentis ou des images de la vie quotidienne dans les territoires contrôlés par l'Etat Islamique, censés le détourner de son objectif initial. L'utilité de ces techniques reste cependant très discutable puisqu'elles omettent totalement le fait que c'est d'abord l'écosystème dans lequel sont plongés les individus qui les font adhérer à une cause donnée[16].

D'autres mesures permettent enfin d'éviter une censure trop générale et trop absolue, tout en réglant les conflits entre les CGU et les législations locales qui peuvent être plus restrictives :

- Le géoblocage ;
- Les restrictions de contenus en fonction de l'âge ;
- le retrait des recommandations sur les pages web ;
- Les alertes à destination des utilisateurs portant sur l'existence d'un contenu « non désirable » ;
- La visibilité limitée donnée à un contenu controversé mais non illicite et la restriction d'accès à certaines fonctionnalités[17].

Une coopération entre les plateformes du web

Le développement de ces différentes techniques n'est pas sans conséquence sur les comportements des internautes désirant publier des contenus jugés illicites. Alors qu'il sera de plus en plus difficile de poster des contenus illicites sur les plateformes des GAFA, les groupes malveillants chercheront à diffuser leurs propos sur de nouvelles plateformes moins rigoureuses en termes de modération (Mastodon par exemple) ou

[12] http://www.numerama.com/tech/267555-entre-ia-et-moderation-humaine-facebook-devoile-ses-outils-contre-la-propagande-terroriste.html

[13] http://www.liberation.fr/futurs/2017/05/19/intelligence-artificielle-hemispheres-en-surchauffe_1570833

[14] http://www.lemonde.fr/economie/article/2013/09/19/reseaux-sociaux-tencent-la-censure-au-quotidien_3480270_3234.html

[15] https://redirectmethod.org/

[16] https://motherboard.vice.com/fr/article/bm7z5v/avec-redirect-method-google-veut-couper-lherbe-sous-le-pied-de-daesh

[17] http://www.lemonde.fr/pixels/article/2017/08/15/messages-blocages-et-demission-apres-charlottesville-la-silicon-valley-reagit_5172607_4408996.html

encore sur le *dark web*, là où il est impossible d'opérer un contrôle. Conscients des risques de migration et « d'enfoncement » des groupes malveillants dans les profondeurs du réseau mondial, les GAFA entendent désormais développer une coopération plus étroite entre les plateformes, notamment en développant des outils communs comme une base de données partagée regroupant les empreintes (hash) des messages à caractère terroriste[18]. Pour être efficace, cette coopération devra cependant s'étendre aux nouvelles plateformes ou aux acteurs plus petits.

Notons enfin, le rôle de plus en plus important du signalement des contenus illicites par les utilisateurs eux-mêmes en matière de régulation des contenus sur internet.

Quelles conséquences politiques et juridiques ?

Au plan politique

Alors que la censure de propos jugés illicites est une décision relevant normalement des autorités publiques à l'instar du CSA pour le cinéma par exemple, celles-ci sont relativement impuissantes lorsqu'il s'agit de propos diffusés sur internet. Les plateformes du web se voient donc confier par défaut la difficile tâche de censurer les contenus illicites sur internet tout en s'efforçant d'assurer la promotion de la liberté d'expression et la diffusion des savoirs. Pour conserver leur indépendance, les géants du web réagissent cependant très prudemment en fonction des évènements et des demandes des autorités. La modération des contenus à caractère terroriste s'est par exemple accentuée suite aux attentats commis par l'Etat islamique, notamment sous la pression des gouvernements et de l'opinion publique. Plus récemment, dans l'affaire de Charlottesville, les GAFA semblent être cependant sortis de leur neutralité en condamnant ouvertement les groupes suprémacistes et néonazis et en adoptant des mesures pour censurer ces groupes sur internet[19].

Ce nouveau rôle illustre parfaitement l'évolution que connaît la souveraineté étatique avec la mondialisation et l'explosion du numérique. Il n'est pas rare, en effet, qu'un membre des GAFA s'oppose aux autorités d'un Etat qui souhaitent recueillir des informations ou censurer des contenus sur internet. Par ailleurs, si cette conflictualité fait l'objet de législations responsabilisant les plateformes telles que la LCEN de 2004, certains Etats comme la Russie[20], Israël ou encore l'Allemagne[21], renforcent leur législation relative à l'usage de l'internet, réaffirmant ainsi leur souveraineté dans l'espace numérique. Cette érosion progressive de la souveraineté étatique soulève en effet de sérieuses questions quant au caractère a-démocratique d'une gouvernance purement technicienne, voire automatisée, des contenus. Un équilibre doit donc être trouvé entre la préservation des libertés publiques dont les Etats restent les garants et la nécessaire lutte contre les contenus illicites, en particulier dans le contexte terroriste actuel.

---

[18] https://www.nextinpact.com/news/102398-facebook-microsoft-twitter-et-youtube-sunissent-contre-contenus-terroristes.htm

[19] http://www.latribune.fr/technos-medias/haine-sur-internet-apres-charlottesville-la-silicon-valley-agit-contre-les-neonazis-747277.html

[20] http://www.silicon.fr/russie-bannir-tor-vpn-proxies-181359.html

[21] http://www.clubic.com/pro/blog-forum-reseaux-sociaux/actualite-832960-allemagne-oblige-reseaux-sociaux-supprimer-contenus-haineux.html

Au plan juridique

La modération des contenus est effectuée en l'absence de l'intervention d'un juge ou d'une autorité administrative habilitée par la loi alors même qu'il s'agit de restreindre ou non la liberté d'expression. On peut dès lors parler de « justice privée » puisque des plateformes telles que celles des GAFA sont supposées garantir le respect des libertés sur internet. Même s'il existe des possibilités de recours à des médiateurs pour contester une décision de modération d'une plateforme[22], il reste difficile de prévenir les risques d'abus de la censure, surtout lorsque celle-ci s'automatise. Se pose alors la question de l'adaptation de la justice à la modération des contenus sur internet et à la vitesse à laquelle ces contenus sont diffusés. Faudra-t-il automatiser également la justice pour suivre le rythme ?

L'absence d'un cadre juridique et judiciaire clair en matière de régulation de contenus illicites par les plateformes du web peut également entrainer des difficultés juridiques pour ces dernières en termes de responsabilité. Ces opérateurs peuvent en effet faire l'objet de poursuites judiciaires pour censure abusive[23] et, inversement, engager leur responsabilité pour ne pas avoir modéré un contenu jugé illicite. De nombreuses plaintes ont ainsi été déposées contre les GAFA accusés de prêter assistance à la diffusion de la propagande du groupe Etat islamique[24].

La régulation des contenus sur internet par les géants du numérique nécessite enfin d'appréhender un très grand nombre de données qui doivent être contextualisées, notamment en fonction des différentes législations et cultures, ce qui constitue un frein à l'automatisation de la modération et un risque de conflictualité avec les autorités publiques ou l'opinion publique. Cette « justice privée » est en réalité ambivalente : elle peut profiter au respect et à la promotion des libertés comme nuire à ces dernières selon l'interprétation des GAFA et les Etats concernés. Une coopération de confiance entre les plateformes et les autorités publiques demeure donc la solution la plus adaptée en l'absence de tout cadre juridique international contraignant.

[22] https://support.twitter.com/forms/general?subtopic=suspended

[23] http://www.zdnet.fr/actualites/facebook-juge-en-france-pour-censure-abusive-39815856.htm

[24] http://www.lefigaro.fr/international/2016/12/21/01003-20161221ARTFIG00128-twitter-google-et-facebook-attaques-en-justice-apres-la-tuerie-d-orlando.php

LE ROLE ESSENTIEL DU SECTEUR PRIVE EN MATIERE DE RENSEIGNEMENT « CYBER »

Le renseignement « cyber », ou cyber intelligence, se divise en deux familles complémentaires qui se recoupent en partie. D'un côté, le Renseignement d'Origine Cyber (ROC) concerne l'ensemble des informations obtenues par le vecteur numérique. Il peut s'agir là aussi bien de lutte contre la fraude (circuit de contrefaçons, marchés noirs etc.), d'investigations sur les réseaux sociaux (social engineering) ou d'infiltration dans les systèmes de communication adverses dans le cadre d'opérations anti-terroristes ou militaires. Le Renseignement d'Intérêt Cyber (RIC), en revanche, concerne l'ensemble des informations et renseignements concernant l'espace numérique. Parmi ses objectifs : alimenter la connaissance des cybermenaces pour permettre à une organisation d'ajuster sa posture de cyberdéfense au plus près des menaces et d'anticiper les incidents de sécurité à venir. C'est alors que les frontières classiques entre communauté du renseignement « étatique » et secteur privé ont tendance à s'estomper.

D'une part, les agences étatiques doivent faire face à des menaces similaires à celles visant le secteur privé (cybercriminalité, hacktivisme) puisqu'elles s'appuient massivement sur des produits de cybersécurité du marché, ce qui induit une dépendance à l'égard de quelques fournisseurs d'autant plus critiques que ceux-ci fournissent généralement aussi des données techniques (vulnérabilités, signatures, IoC etc.) grâce à leur parc installé.

D'autre part, les analyses des sociétés privées de cyber intelligence sont désormais brandies par les Etats eux-mêmes comme caution lors de tensions internationales impliquant des cyberattaques. Pour ces deux raisons, disposer d'un écosystème privé de confiance est donc devenu un nouvel enjeu de souveraineté.

Le secteur privé, première source de données et de standards

Publiques comme privées, les organisations doivent faire face à des typologies de menaces sensiblement similaires (cybercriminalité, hacktivisme), utilisant des méthodologies d'attaques (TTPs) et des outils identifiables.

Estimé par le Gartner à $ 1,5 milliards en 2018 au niveau mondial contre 250 M$ en 2013, le marché de la cyber intelligence est amené à se développer fortement d'ici à 2020 mais reste encore largement émergent en France. Si le marché reste pour l'heure majoritairement orienté sur les couches « basses » (Opérationnel

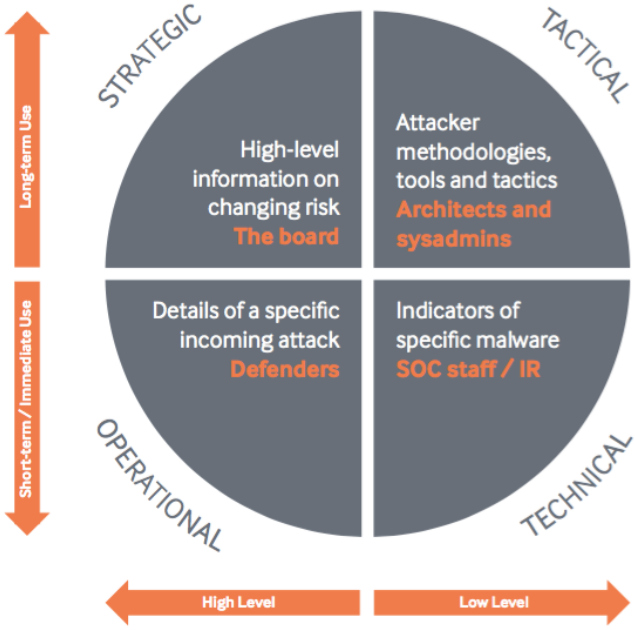

Figure 1 : Les différents types de cyber threat intelligence

Source : Livre Blanc *Threat Intelligence : Collecting, Analysing, Evaluating – MWR Infosecurity* Mars 2015

et Technique) permettant d'améliorer les capacités de détection, la tendance tend à remonter vers des analyses de plus haut niveau permettant de mieux comprendre les modes opératoires et anticiper les attaques.

Grâce à leurs équipes d'experts réparties aux quatre coins du monde, à l'instar de l'Unité 42 de Palo-Alto ou de l'organisation Talos de Cisco, les sociétés privées, par essence transnationales disposent donc de moyens et de capacités que ne peuvent avoir des seules agences étatiques. Ce constat est d'autant plus vrai lorsque celles-ci s'allient au sein de consortium comme la Cyber Threat Alliance regroupant Fortinet, Palo-Alto, Symantec, Intel Security, Check Point et Cisco.

Ainsi, avec une installation dans plus de 270 000 entreprises à travers le monde[25] (Kaspersky) ou 9 millions de terminaux déployés[26] (FireEye), ces constructeurs et vendeurs de solutions de cybersécurité recueillent et analysent en temps réel une masse énorme de données techniques provenant des systèmes et réseaux de leurs clients (listes de domaines malveillants, adresses IP malveillantes, serveurs compromis etc). Ces remontées continues de données leur permettent d'avoir un accès direct et primaire aux informations techniques. Cet accès privilégié aux données provenant de leurs systèmes propriétaires disséminés dans le monde entier confère à ces groupes privés une position dominante face à des acteurs régaliens par définition nationaux. La structuration du partage d'informations devient alors fondamentale.

[25] https://www.kaspersky.fr/

[26] https://www.fireeye.fr/company/why-fireeye.html

Souvent issues d'une coopération entre sphères publique et privée, à l'instar de MISP[27] (Malware Information Sharing Platform), de nombreuses initiatives *open source* ou propriétaires (ThreatQuotient) voient le jour pour agréger les données techniques issues de l'ensemble des fournisseurs et les diffuser à leurs clients/abonnés. Même si ces plateformes constituent une première étape utile, la multiplicité des formats de données issus de *providers* aux langages différents reste un frein. La structuration des langages de remontée d'informations permettant le partage sur des plateformes communes devient donc un enjeu pour le développement de l'industrie de cyber intelligence. Appuyés par l'US Department of Homeland Security avec le concours d'industriels, STIX (Structured Threat Information eXpression) et TAXII (Trusted Automated eXchange of Indicator Information) visent ainsi à s'imposer comme les standards internationaux du marché, de même que IDMEF (Intrusion Detection Message Exchange Format) en Europe. Ces nouvelles plateformes de partage d'informations structurées, calibrées et actionnables pourront permettre la multiplication des sources pour les communautés en charge de la cybersécurité des infrastructures critiques.

La surface d'exposition croissante des organisations, l'interconnexion des systèmes et des réseaux, la multiplication des législations relatives à la cybersécurité au sens large (RGPD, directive NIS sur les infrastructures essentielles, LPM etc.) ainsi que la prolifération de cyberarmement[28] constituent autant de leviers favorisant l'éclosion du marché, largement dominé par les Etats-Unis et Israël.

Unité 8200, le renseignement militaire au cœur de l'industrie cyber[29]

Historique :

L'unité 8200 est l'une des plus anciennes agences de renseignement, existant avant même la création d'Israël. Créée sous le mandat britannique au début des années 1930, elle a pour principale mission d'intercepter les communications des pays arabes voisins. Elle est intégrée en 1948 au Forces armées israéliennes (IDF) sous le numéro « Unité 515 », puis « Unité 848 » (1956). Après la débâcle de la Guerre du Kippour (1973), une refonte complète du renseignement militaire intervient pour arriver à la montée en puissance de l'Unité 8200 actuelle. Spécialisée dans le renseignement technique et cyber, elle participe à l'ensemble des opérations de renseignements israéliennes. « 90% du renseignement israélien provient de l'Unité 8200 » avance même un ancien cadre de l'unité.

Recrutement :

Du fait du service militaire obligatoire, la sélection se fait très tôt, dès le lycée. L'unité 8200 a ainsi créé son propre programme de cours du soir, le programme Magshimim[30], pour pouvoir présélectionner les meilleurs profils. La sélection est aussi rigoureuse que clandestine. Linguistes arabophones, mathématiciens et ingénieurs informatiques sont évidemment parmi les compétences les plus appréciées. A la différence des services de renseignement britanniques ou américains qui privilégient l'expérience, l'unité 8200 retient avant

[27] http://www.misp-project.org/

[28] https://www.observatoire-fic.com/wannacry-le-defi-de-la-proliferation-cyber/

[29] Tiré de l'article original de Richard Behar Inside Israel's secret startup machine – Forbes, Mai 2016

[30] http://www.slate.com/articles/technology/future_tense/2016/07/israel_s_magshimim_program_trains_teenagers_to_work_on_cybersecurity.html

tout le potentiel des (très) jeunes recrues : capacités d'apprentissage, d'adaptation au changement, de travail en équipe ou d'originalité dans la résolution des problèmes, quel que soit leur parcours académique. Cette rude sélection n'empêche pas de devoir faire face à turn-over important, de près de 25% par an.

Organisation :

Répartis en petites équipes indépendantes, les 5 000 militaires travaillent en mode projet pour apporter des réponses très opérationnelles aux enjeux des forces armées et des autres agences de renseignement. Les recrues sont soumises à une activité intellectuelle intense, toujours en équipe, avec des contraintes temporelles, matérielles, humaines ou financières parfois très dures, qui les obligent à se dépasser pour atteindre les objectifs fixés. L'apprentissage par l'action et par l'erreur, la responsabilisation des équipes, la valorisation de la prise de risque ou encore la (relative) faible rigidité hiérarchique en font une unité à part au sein des IDF. Le mentorat est par ailleurs favorisé grâce à l'apport de la réserve opérationnelle (3 semaines par an, obligatoire jusqu'à 40 ans) constituée des anciens de l'unité. L'incubation et l'esprit « start-up » et entrepreneurial sont donc fortement ancrés dans la culture de l'unité.

Passage au secteur privé :

Le fait d'appartenir à l'unité 8200 constitue en soi une carte de visite, véritable réseau parallèle, gage de crédibilité auprès de l'ensemble de l'écosystème et notamment des investisseurs israéliens mais aussi américains. L'accès à un réservoir de compétences pointues, passées par l'unité, facilite des recrutements rapides par cooptation. Depuis près de 10 ans, ce sont plus de 1 000 sociétés de technologies qui ont été fondées par les quelques 8000 « alumnis » de l'unité, en particulier en matière de cybersécurité et de cyber intelligence. Grâce aux fonds d'investissement et autres incubateurs créés par les vétérans (citons notamment Team 8), l'Unité 8200 continue de développer tout projet innovant susceptible de l'intéresser pour ses besoins propres. Parmi les *success stories*, on compte notamment CheckPoint et Palo-Alto, devenues depuis américaines, ou encore iSIGHT Partner et SenseCy, références en matière de services de cyber intelligence.

L'influence de l'unité 8200 en matière de cyber intelligence :

Il est désormais public[31] que *Stuxnet* a été co-créé par la CIA et les experts de l'unité 8200 des IDF afin de viser les systèmes industriels d'enrichissement d'uranium de l'usine de Natanz. Avec plus de 25 millions lignes de code et des méthodologies d'attaques inédites, *Stuxnet* a marqué un tournant en matière de cybersécurité. Fort de ces expériences acquises au sein de l'unité en matière d'«*offensive security »,* les vétérans ont pu mettre à profit leurs expertises techniques et leurs méthodologies de travail au profit de la cybersécurité des organisations. Du fait de la nature de leurs opérations, les membres de l'unité 8200 ont donc véritablement contribué à l'évangélisation du marché de la cyber intelligence en amenant les doctrines et l'emploi de ce type de prestations dans le secteur privé, en Israël mais surtout aux Etats-Unis, premier marché mondial de la cybersécurité.

[31] Voir notamment l'ouvrage Obama - Guerres et secrets de David E. Sanger - 2012

Les sociétés privées comme outil politique

Le cyberespace est devenu un espace de conflictualité affectant les relations internationales, notamment en raison de la quasi-impossibilité d'attribution et d'imputabilité. Avec l'attaque du Parti Démocrate, la dernière élection présidentielle américaine pourrait en ce sens servir de modèle.

Accusée publiquement d'en être à l'origine, la Russie a été mise en cause par un rapport[32] du DHS et du FBI détaillant l'opération nommée *Grizzly Steppe.* Ce rapport a pour but d'analyser les « activités cyber malicieuses russes » visant à « compromettre et exploiter réseaux et terminaux associés à l'élection, ainsi qu'à un éventail d'entités du gouvernement, du monde politique ». Or, outre le fait que le rapport mélange pêle-mêle campagnes, groupes d'acteurs, *malwares* et indicateurs techniques, les seuls indicateurs de compromission (IOC) présentés sont tirés des investigations forensic de la société Crowdstrike, à qui le Parti Démocrate avait fait appel. Une situation qui soulève deux problèmes majeurs. Le premier réside dans le flou entretenu entre des éléments « macro » de cyber intelligence (cyber threat intelligence stratégique) récoltés par des organismes étatiques légitimes dans le cadre d'une enquête officielle (DHS et FBI) et les éléments techniques « micro » (cyber threat intelligence tactique et technique) tirés d'une investigation forensic réalisée par un acteur privé (Crowdstrike) dans le cadre d'une réponse à incident. Au regard du droit international, il semble assez hasardeux de pouvoir baser une accusation sur des analyses de renseignement émanant d'un acteur non-étatique. Le second problème soulevé ici concerne précisément les éléments techniques de compromission fournis par Crowdstrike. Selon Chris Gonsalves, directeur de recherche à l'IANS, cité dans le MagIT[33], ceux-ci ne seraient pour l'essentiel qu'un « mélange inutile de de nœuds de sortie Tor, de proxies et de serveurs de réseau privé virtuel ». Or, il est impossible avec de tels IOC de pouvoir raisonnablement faire la moindre attribution et d'apporter quelque conclusion que ce soit sur les auteurs de ces cyberattaques. Il est donc légitime de s'interroger sur l'utilisation politique de ce rapport, techniquement peu pertinent, par les autorités américaines.

Comme cela avait été déjà le cas les années précédentes avec le piratage de Sony Picture (ouverture de l'enquête du FBI et mise en cause de la Corée du Nord par le biais du rapport de cyber intelligence réalisé par AlienVault et Kaspersky sur Lazarus), les rapports d'analyse des sociétés de cyber intelligence semblent désormais être pleinement intégrés à l'arsenal américain. Tout comme ils sont sans doute utilisés par la Russie pour incriminer la NSA américaine au travers du rapport produit par Kaspersky sur l'Equation Group. Politiquement, il semble effectivement plus aisé pour un Etat d'utiliser ces sociétés comme « proxy » pour porter des accusations publiques que de dévoiler ses propres capacités offensives et courir le risque d'une escalade.

La cyber Intelligence, un autre enjeu de souveraineté

Nettement moins mature que le monde anglo-saxon en matière de cyber intelligence, la France gagnerait à voir se développer un écosystème dynamique en la matière. Il s'agit même là d'un enjeu de souveraineté majeur.

---

[32] https://www.us-cert.gov/sites/default/files/publications/JAR_16-20296A_GRIZZLY%20STEPPE-2016-1229.pdf

[33] http://www.lemagit.fr/actualites/450410414/Et-le-renseignement-cyber-apparu-privatise

La multiplication des sources offertes à la communauté du renseignement au sens large permet en effet d'affiner la connaissance globale de l'état de la menace et des méthodologies d'attaques visant les opérateurs publics comme privés. On voit donc toute la pertinence qu'il y aurait à favoriser un cadre d'échange structuré en matière de Threat Intelligence stratégique, partagé entre public et privé. C'est d'ailleurs bien l'ambition du GCHQ britannique avec la création du National Cyber Security Center visant à favoriser l'éclosion d'un tel écosystème autour de lui et permettant l'échange d'informations classifiées entre public et privé.[34]

Du point de vue capacitaire, c'est d'ailleurs toute la philosophie de la Loi de Programmation Militaire avec la création de « sondes souveraines » qualifiées par l'ANSSI (Thales, Airbus, Gatewatcher) permettant la remontée primaire de données techniques « brutes » vers des organisations de confiance.

Les principaux acteurs de la Cyber Intelligence dans le monde

Société	Nationalité	Activités
Airbus DS Cybersecurity	FR	MSSP *
AlienVault	USA	Pure Player**
Aleph Networks	FR	Editeur technologique***
Anomali	USA	Pure Player
Blueliv	Espagne	Editeur technologique
Booz Allen Hamilton	USA	MSSP
Certego	Italie	Editeur technologique
Checkpoint	USA	MSSP
Crowdstrike	USA	Pure Player
CybelAngel	FR	Editeur technologique
Cyjax	UK	Editeur technologique
Cyveillance	USA	Pure Player

[34] Intelligence Online du 21/06/2017

Dell SecureWorks	USA	Pure Player
Deloitte	USA	MSSP
Digital Shadow	UK	Editeur technologique
EclecticIQ	Pays-Bas	Pure Player
ESET	Hongrie	Editeur technologique
EY	UK	Editeur technologique
F-Secure	Finlande	Editeur technologique
Fortinet	USA	Editeur technologique
Fox-IT	Pays-Bas	Editeur technologique
Groupe IB	Russie	Pure Player
IBM	USA	MSSP
Intrinsec	FR	MSSP
iSIGHT Partner (racheté par FireEye)	Israel	Pure Player
Kaspersky	Russie	MSSP
Lexsi (racheté par Orange)	FR	Pure Player
Lockheed Martin	USA	MSSP
McAfee	USA	MSSP
Mendiant (racheté par FireEye)	USA	Pure Player
Palo-Alto	USA	MSSP
PwC	UK	MSSP
Recorded Future	USA	Editeur technologique
RSA	USA	MSSP
SecuInsight	FR	Pure Player
Sekoia	FR	MSSP

SenseCy	Israel	Pure Player
SurfWatchLabs	USA	Pure Player
Symantec	USA	MSSP
Team Cymru Research	UK	Editeur technologique
Thales	FR	MSSP
ThreatMetrix	USA	Pure Player
ThreatQuotient	USA	Editeur technologique
ThreatStream	USA	Pure Player
TrendMicro	Japon	MSSP
Verisign iDefense	USA	MSSP
Verizon	USA	MSSP
Webdrone	FR	Editeur technologique

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