Cyber sécurité et cyber défense : perpétuer les efforts engagés et surtout renforcer les partenariats entre tous les secteurs de l'économie

Autor(en): **Therre, Jean-Pierre**

Objekttyp: **Article**

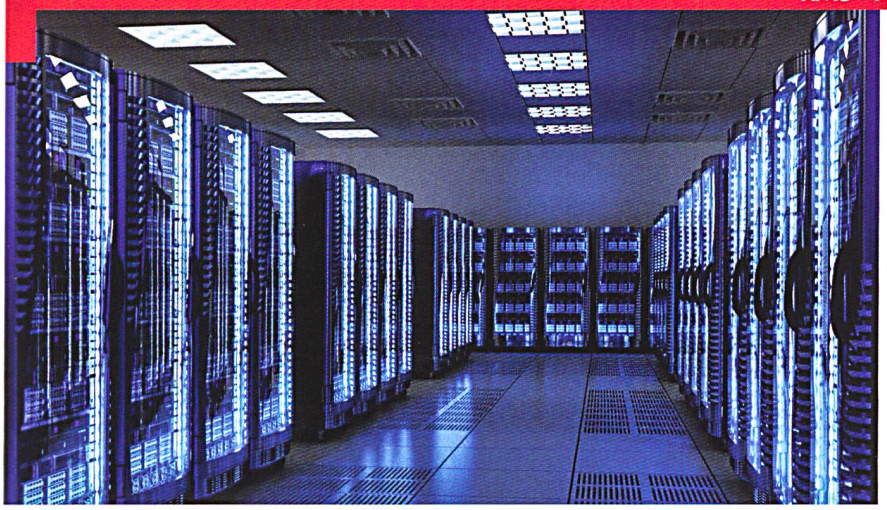
Zeitschrift: **Revue Militaire Suisse**

Band (Jahr): **- (2018)**

Heft [2]: **Numéro Thématique 2**

PDF erstellt am: **22.07.2024**

Persistenter Link: https://doi.org/10.5169/seals-823458



L'industrie et l'économie dépendent de la sécurité de leurs données et de leurs serveurs.

Cyber

Cyber sécurité et cyber défense: Perpétuer les efforts engagés et surtout renforcer les partenariats entre tous les secteurs de l'économie.

Jean-Pierre Therre
Executive Vice President, Head of Cybersecurity, Div. Technology & Operations, Banque Pictet & Cie

Comme chacun d'entre nous peut le constater dans les médias ou dans de nombreux articles spécialisés, l'ensemble de l'économie mondiale fait face, jour après jour, à un flux continu de menaces et d'attaques cyber. Parfois massives et souvent internationales, ces attaques ont de forts impacts organisationnels, financiers et réputationnels pour les entreprises et les institutions qui les subissent. Cette réalité n'est certes pas nouvelle mais c'est bien son amplification continue qui interpelle le citoyen béotien comme les meilleurs experts.

Le risque cyber, sous ses différentes composantes, s'inscrit aujourd'hui en tête des cartographies de risques publiées par les institutions publiques et les entreprises, tous secteurs d'activités confondus. Et les enjeux financiers de ces cyber attaques estimés à environ 8 trillions de USD sur les 5 prochaines années par des organes comme le World Economic Forum ou par les grands cabinets de conseils sont particulièrement préoccupants pour tous les acteurs économiques (Réf. 2).

De fait, les menaces et les attaques cyber auxquelles doivent faire face aujourd'hui tous les acteurs éco-nomiques se déclinent selon un large spectre de typologies qui sont elles-mêmes en constante évolution. Elles sont caractérisées par leur complexité intrinsèque, par leur intensité parfois dramatique et par la haute fréquence de leurs évolutions. En particulier des attaques cyber majeures comme par exemple « WannaCry » et « NotPetya » en 2017 ou encore « Spector & Meltdown » en 2018 ont mis en exergue à la fois l'ampleur internationale des attaques cyber de dernière génération mais aussi l'interdépendance avérée entre les acteurs économiques et publics ainsi que le partage des vulnérabilités. Ces attaques témoignent de l'agilité et de la capacité d'innovation des équipes cybercriminelles qui les initient. Et les meilleurs experts de la cyber sécurité sont en alerte permanente pour anticiper les paradigmes de menaces cyber émergentes, en particulier associés au développement des nouvelles technologies numériques (i.e. Cloud, Intelligence Artificielle, etc.) (Réf. 3).

En termes de volumétrie, la grande majorité des cyber attaques recensées est de nature plutôt « traditionnelle », c'est-à-dire sous forme de *spams*, *scams*, *phishing*, *spear phishing*, DDoS, *ransomware*, etc. Ces cyber attaques sont le plus souvent d'origine criminelle et ont pour premier objectif des gains financiers rapides aux dépends de particuliers ou d'entreprises. Mais depuis deux-trois ans émergent des formes beaucoup plus sophistiquées et subtiles d'attaques, dites attaques APT - *Advanced Persistent Threat*. Ces APTs, dont l'origine est le plus souvent étatique, se caractérisent par un comportement malveillant complexe qui vise le plus souvent à l'exfiltration silencieuse, et dans la durée, de données sensibles, confidentielles ou stratégiques. Aujourd'hui du fait de la sous-traitance de certaines activités gouvernementales vers des entités privées (USA-NSA à Equation Group, Corée du Nord à Lazarus Group, etc.), on observe malheureusement une diffusion plus élargie de ces APTs.

Mais il serait réducteur de se limiter à cette seule catégorisation simpliste car les attaques cyber ma-jeures et complexes s'inscrivent souvent dans un contexte militaire ou géostratégique. Elles ciblent par exemple les infrastructures critiques du pays dans des secteurs comme l'approvisionnement énergétique, les télécommunications, etc. Dans un contexte de guerre économique latente et de concurrence internationale acharnée, les pôles stratégiques de compétitivité comme par exemple le secteur bancaire et financier, ou encore le secteur pharmaceutique et de la chimie fine, l'armement et l'aéronautique, sont aussi devenus des cibles régulières. On soulignera aussi les attaques à vocation terroriste ou géo-économique destinées à altérer l'information (Fake News) et à influencer activement la perception d'une population ou d'une communauté. De nombreux articles et ouvrages spécialisés récents décrivent cette nouvelle évolution dans le spectre des attaques cyber.

Dans ce contexte de faits, la cybersécurité et la cyber défense sont au centre des préoccupations et priorités

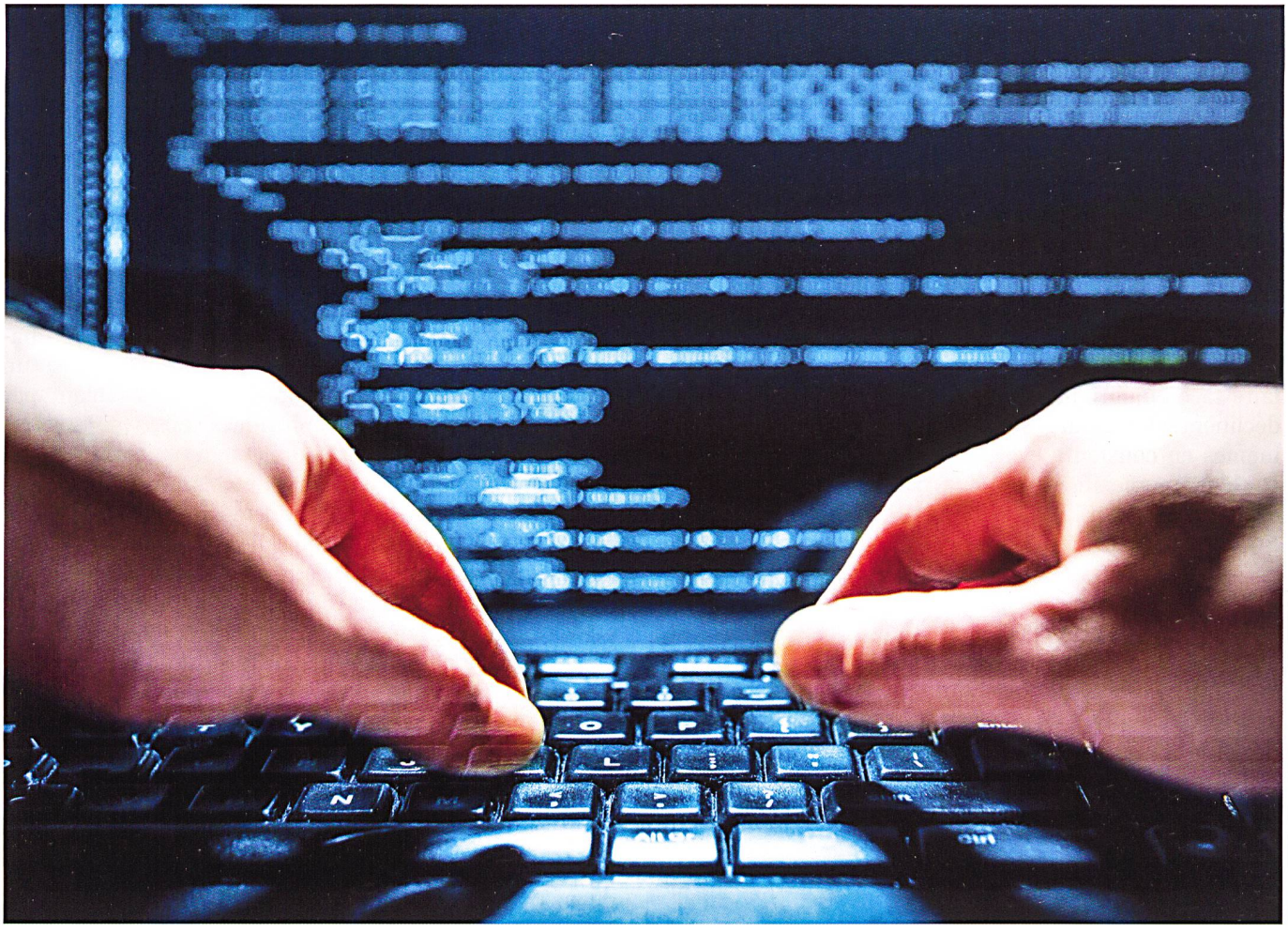
affichées par les entreprises du secteur privé, au même titre que la protection des savoirs-faire ou celle des données personnelles. Cette situation s'est très sensiblement accélérée avec l'avènement de la révolution digitale et la numérisation « à marche forcée » des processus, des activités et des services déployés par les entreprises. Le renforcement du cadre législatif international ou national (EU GDPR/LPD, etc.) et en particulier des cadres règlementaires et normatifs propres à de nombreux secteurs économiques est également un des inducteurs importants de cette évolution.

Le cyber espace est ainsi devenuu n vaste et global théâtre d'opérations où se côtoient les intérêts et les motivations les plus divers. Et ce sont tous les pans de l'économie qui sont aujourd'hui concernés par le tryptique constitué de la cyber criminalité, de la cyber sécurité et de la cyber défense. En Suisse, comme partout ailleurs, cette situation est maintenant au centre de toutes les attentions des autorités compétentes (Confédération, Cantons, DDPS, MPC, etc.) et la cyber sécurité est devenue en soi un marché économique en pleine extension.

Les responsabilités et les besoins des acteurs de l'économie privée

A la lumière des évocations précédentes quant à la diversité, à la fréquence et aux évolutions successives des attaques cyber, il est devenu essentiel pour toutes les institutions et entreprises suisses, grandes, moyennes ou petites :

- d'entretenir une analyse permanente des risques afin de pouvoir anticiper en temps utiles les menaces cyber émergentes, par exemple en participant à des efforts permanents de veille collective (par exemple souscription à des « Security Operations Centers » sectoriels) ;
- d'intégrer les cyber menaces et les scénarios d'attaques dans le management de crise et leurs plans de contingence ou de continuité des affaires ;
- d'informer en temps utiles les autorités et leurs pairs et surtout d'organiser des réponses adaptées ;
- de soutenir les efforts de prévention par la sensibilisation continue et la formation de leurs propres personnels ;
- de coopérer de manière continue avec tous les acteurs institutionnels mais aussi avec les autres secteurs de l'économie ;
- d'assurer la confiance numérique de toutes les parties prenantes ainsi que la protection de leurs patrimoines informationnels respectifs ;
- en fonction de leurs moyens, de contribuer à la protection des infrastructures les plus critiques pour leurs secteurs respectifs d'activités ;
- de promouvoir et soutenir au niveau politique ou



sectoriel le renforcement des capacités de lutte contre la cybercriminalité.

Par ces différentes mesures il s'agit bien d'assurer la bonne résilience des entreprises mais aussi de participer à la défense des intérêts économiques nationaux, en particulier des principaux pôles de compétitivité stratégiques et des infrastructures critiques du pays.

Un grand besoin d'échanges et de coordination intersectorielle

Dans ce contexte, il apparaît aujourd'hui fondamental que tous les acteurs de l'économie nationale, qu'ils soient publics et privés, puissent se coordonner selon une feuille de route commune et claire pour anticiper collectivement les différents types de menaces cyber et leur faire face de manière structurée et concertée. En effet, les processus de veille, prévention, détection et réaction, ainsi que les principes de gestion de crise, ne peuvent plus être l'apanage de quelques institutions publiques hautement compétentes ou des seules grandes entreprises. Surtout, il faut qu'émerge une organisation ou des structures transversales de collaboration qui permettent d'anticiper et de faire face collectivement aux menaces et attaques cyber émergentes dont la fréquence et les caractéristiques évolutives ont été soulignées.

Mais de fait, notre pays ne part pas de zéro dans la lutte organisée contre les menaces et les atteintes cyber puisque de nombreux acteurs au sein de la Confédération, des Cantons, des Hautes Ecoles, mais aussi de nombreux experts et professionnels spécialisés en sécurité de l'information, s'en préoccupent depuis de très nombreuses années.

Dans ce contexte d'attention et de préoccupations générales, les grands acteurs de l'économie privée ont d'abord cherché à entretenir, de manière souvent individualisée, des contacts structurés avec les institutions compétentes au niveau fédéral (MELANI, CYD DDPS, SRC, MPC), cantonal (Police/Brigades de criminalité informatique, Ministères publics) ou académique (EPFL-ETHZ, Unis, HES). Ces échanges se sont le plus souvent développés de manière concertée à travers des *curriculums* spécialisés de formation, des conférences nationales ou des événements dédiés (forums ou séminaires). Il s'agissait aussi parfois d'approches plus électives par l'instauration de groupes de travail thématiques et/ou l'activation de groupes d'experts.

Malheureusement, de par leurs mandats et missions, ainsi que du fait d'un manque avéré de ressources propres, ces mêmes institutions publiques n'ont pas toujours été à même de répondre de manière complète aux attentes de l'économie. Des échanges ont pu néanmoins se développer « ad personam » et se perpétuent encore aujourd'hui.

Plus récemment et de manière synchrone avec la multiplication et la complexification des menaces et attaques cyber, se sont développées au sein de l'économie privée des initiatives sectorielles plus directes de coordination entre les experts de la gestion des risques et de la sécurité de l'information. En effet, ces spécialistes cherchent à structurer conjointement la capacité de détection et de protection de leurs entreprises respectives. Des plateformes spécialisées d'échanges ont ainsi émergé à l'initiative des milieux patronaux et des associations professionnelles en sécurité de l'information. Par exemple, au sein du secteur bancaire et financier, la commission de sécurité de l'Association Suisse des Banques, recentrée depuis 2017 en groupe d'experts en cyber sécurité et cyber défense, a joué un rôle déterminant de catalyseur dans l'élaboration de recommandations, de canaux d'échanges (par exemple le réseau bancaire e-Alarm) et de recommandations pratiques sur lesquelles peuvent aujourd'hui s'appuyer l'ensemble des acteurs de ce secteur.

Il faut aussi relever le rôle important joué par les entreprises de services informatiques et de conseils en sécurité de l'information qui, à travers des publications et des évènements marketing réguliers, ont stimulé de manière significative les milieux professionnels. Confrontés lors de ces événements aux bonnes ou mauvaises expériences de leurs pairs, les professionnels de la gestion des risques et de la sécurité ont pris pleine conscience des vrais enjeux de la cyber sécurité et ont commencé à structurer leurs efforts en termes de veille et de réponses à apporter.

Amplifier la coordination et la collaboration entre le secteur public et le secteur privé

Au niveau fédéral, on se souviendra que la première version de la stratégie nationale de protection contre les cyber risques (SNPC) avait été initiée autour de 2008 et au final publiée en 2012, c'est-à-dire à une époque où cette thématique ne retenait pas encore véritablement l'attention générale. Sans revenir sur l'historique des propositions formulées au fil des ans par de nombreux experts aux perspectives parfois fort différentes, les dernières orientations annoncées récemment par le Conseil Fédéral paraissent très encourageantes pour les entreprises.

En effet, le 4 juillet 2018, le Conseil Fédéral a annoncé vouloir intensifier les efforts en matière de prévention et de lutte contre les cyber risques. En particulier, il a formulé quelques décisions de principe et attribué pour ce faire différents mandats en vue de la création d'un centre de compétences dans le domaine cyber. D'autres décisions complémentaires sont encore attendues dans les prochains mois.

Le Conseil Fédéral souhaite, par ces nouvelles orientations, renforcer le niveau de maturité en cyber sécurité et cyber défense afin de préserver la confiance des acteurs économiques. Il s'agit bien de favoriser des avancées significatives dans la défense des intérêts stratégiques les plus essentiels de notre pays mais aussi de protéger la numérisation et la digitalisation en marche de l'économie. Selon ces mêmes orientations, il devient important de structurer la coordination des tâches et responsabilités au sein de l'administration fédérale, de favoriser la prévention et aussi de renforcer les moyens-

compétences à impliquer pour répondre aux demandes des cantons et des milieux économiques.

De manière incidente, le Conseil Fédéral répond ainsi à plusieurs interventions parlementaires récentes, lesquelles réclamaient un renforcement significatif des efforts et des compétences en cyber sécurité mais aussi une clarification des responsabilités en matière de cyber sécurité, de poursuite contre la cyber criminalité et de cyber défense.

Sans entrer dans le détail des missions, rôles et responsabilités des différents organismes de la Confédération et des Cantons engagés dans la problématique cyber, deux grands acteurs méritent d'être évoqués pour leur volonté avérée de favoriser les synergies et les collaborations avec les entreprises et les professionnels.

MELANI :

Dans le cadre de la stratégie nationale de protection de la Suisse contre les cyber risques (SNPC 2018-2022) (Réf. 4), les objectifs stratégiques dévolus depuis juin 2012 à la Centrale d'Enregistrement et d'Alarme pour la Sûreté de l'Information – MELANI - sont et restent la détection précoce des menaces et des dangers dans le cyber espace, la réduction des cyber risques liés en particulier à la cyber criminalité, au cyber espionnage et au cyber sabotage, ainsi que le renforcement de la capacité de résistance des infrastructures critiques.

Dans ce contexte essentiel pour favoriser la bonne résilience opérationnelle de tous les acteurs économiques publics ou privés, l'équipe MELANI, malgré des ressources qui restent encore trop limitées, s'attache avec diligence et intelligence à répondre aux objectifs fixés. Elle s'efforce aussi de consolider dans le cadre de son « Cercle Fermé » des initiatives dédiées visant à renforcer le partage d'informations pertinentes ainsi que des échanges structurés et réguliers entre les acteurs des différents secteurs économiques. Une opportunité que nombre d'entreprises ont bien comprise et utilisent maintenant avec beaucoup d'intérêts. Par ailleurs, le partenariat développé entre MELANI et l'association inter-entreprises Swiss Cyber Experts est également exemplaire car il permet de regrouper les connaissances des experts de tous les secteurs avec pour objectif de renforcer un diagnostic efficace et d'anticiper une réponse adaptée en cas de grave attaque cybernétique.

Les unités CYD du DDPS :

Le plan d'action de cyber défense (PACD) publié par le DDPS en novembre 2017 (Réfer. 5) s'inscrit en parfaite cohérence avec la stratégie nationale pour la protection de la Suisse contre les cyber risques (SNPC). Et il est important de relever la volonté affichée du DDPS de favoriser dans le PACD une collaboration renforcée avec ses propres partenaires (exploitants des infrastructures critiques, Groupement Défense), mais aussi avec l'économie et les hautes écoles, afin de constituer un pôle unifié de compétences reconnues en cyber défense. On y relève ainsi une déclinaison pertinente de prestations et de processus d'engagement des ressources et des compétences disponibles. Ceux-ci s'appuient sur une organisation logique des fonctions de cyber défense et de gestion de crise (la conduite, l'anticipation, la protection, la prévention, la réaction, l'action et l'assistance). Il faut aussi souligner la mise en œuvre progressive d'un pôle de ralliement dit CYD-Campus qui doit cristalliser les compétences et les échanges d'informations entre tous les acteurs de la cyber défense. Sont ainsi explicitement recensés : les partenaires opérationnels nationaux et internationaux, les acteurs de l'industrie et de l'économie ainsi que les hautes écoles. Une telle approche constitue un signe fort qui doit stimuler l'engagement de tous les partenaires institutionnels et surtout des acteurs de l'économie.

On relèvera que cette approche d'enrôlement milicien de spécialistes ou d'experts cyber des secteurs de l'économie privée a déjà été mis en œuvre depuis une à deux décennies avec beaucoup de réussite dans les grands pays Européens et Anglo-Saxons.

Il est aussi opportun de souligner que cette volonté de coordination et de partenariat se traduit déjà par l'invitation et l'implication active de quelques représentants seniors de l'économie dans des réflexions thématiques orchestrées depuis 2017 par la l'Académie Suisse des Sciences et Techniques – SATW – et le conseil cyber du DDPS. Ces initiatives exemplaires favorisent la multiplication d'échanges en confiance entre des acteurs très compétents mais qui ont peu l'opportunité de collaborer ensemble de manière naturelle et régulière. Pour les entreprises de tous les secteurs économiques, ces approches sont essentielles car il s'agit bien de déployer une plateforme commune de veille et d'anticipation, de renforcer l'interopérabilité des compétences et des capacités techniques-opératives ainsi que d'attirer les talents dans une communauté dynamique de cyber sécurité et cyber défense.

Les axes de renforcement préconisés par le secteur financier sont ainsi la sensibilisation des collaborateurs et des clients, la veille permanente et l'analyse concertée des menaces cyber émergentes, le partage d'information avec les autorités compétentes à travers des groupes sectoriels fermés (MELANI), la gestion des incidents et la gestion de crise dans une perspective technique mais aussi légale et systémique (notamment avec la BNS) et pour finir le renforcement des compétences des instances de poursuite pénale.

Les partenariats publics-privés

De fait, de telles démarches confèrent sa pleine substance au concept de partenariat public-privé en cyber sécurité et cyber défense évoqué dès la fin des années 2000 par quelques visionnaires (pour mémoire le PPP « Swiss Cyber Resilience » proposé en 2010) et depuis appelé de leurs vœux par de nombreux experts des entreprises du fait de la multiplication et de la complexité ainsi que du caractère toujours plus international des menaces cyber. Par la priorisation des thématiques, l'identification des enjeux clés et la volonté de faciliter la prise de conscience des acteurs, il est intéressant de constater que ces démarches reflètent avec pertinence les efforts également structurés par la Communauté Européenne dans le cadre du cPPP « Sécurité du numérique & Europe », un contrat de partenariat public privé embarquant plusieurs centaines d'entreprises européennes et doté d'un budget qui devrait atteindre à terme 2 milliard d'euros.

Il appartient maintenant aux acteurs politiques et économiques de la communauté nationale d'amplifier ces initiatives, et aussi de les soutenir financièrement, afin de garantir la pérennité des actions pertinentes de cyber sécurité et cyber défense déjà engagées et surtout d'assurer la multiplication des ressources et des compétences impliquées.

J.-P. T.

Réferences:

Global Risks Report 2018 : Fractures, Fears and Failures, World Economic Forum, http://reports.webforum.org/global-risks-2018/global-risks-2018-fractures-fears-and-failures
MIT Technology Review, Six Cyber Threaths to Really Worry About in 2018, by Martin Gilles, January 2018.
Stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC) 2018-2011, 18.04.2018, http://www.upic.admin.ch
Plan d'action cyberdéfense DDPS (PACD), version publiée du 09.11.2017, http://www.vbs.admin.ch/defense//protection-cyberattaques.html

News

Un «mouchard» et l'indispensable secret des opérations militaires

L'application Strava, compatible avec de nombreuses montres connectées et permettant de mémoriser, d'échanger et de visualiser les performances physiques en temps réel, a connu un grand engouement au sein de la communauté militaire internationale.

L'émotion suscitée, au début février 2018, en raison des risques de sécurité liés au mode de cartographie en ligne fusionnant les treize mille milliards de coordonnées GPS collectées auprès des utilisateurs, a créé un vent de panique au sein des services de sécurité. Il touchait au niveau d'activités de certaines installations militaires, aux itinéraires utilisés lors des patrouilles et leurs fréquences, les zones réservées. On a interdit l'utilisation de l'application. Cette information a tout du réchauffé, cette carte étant disponible et exploitée par les experts du renseignement depuis plusieurs années.

Quelles informations inédites peut-on exploiter sur Strava? Sans recourir à des outils complémentaires, cette cartographie a pu livrer d'emblée la localisation de plusieurs FOB en Afghanistan, les transits sur la base russe de Kuzminsky à la frontière ukrainienne, le centre de commandement sol-air taïwanais, la batterie de missiles émiratie Patriot au Yémen. Couplée à Google Earth, Strava est donc un moyen puissant pour identifier le niveau d'activité des sites militaires sensibles, qui se distinguent la plupart du temps à l'image par la présence de périmètres de sécurité.

L'enrichissement des cartes par des données de terrain issues de la communauté des utilisateurs de Wikimapia ou d'Openstreetmap permet d'aller encore plus loin et d'identifier les gisements d'activités dans les zones désertiques, comme la sécurisation des pipelines en Syrie, les détours utilisés par les trafiquants, les circuits des tour-opérateurs... Strava permet aussi de révéler certains paradoxes. Ainsi aucun personnel militaire ne semble autorisé à pénétrer dans le camp 7 de Guantanamo, qui reste interdit aux rapporteurs de l'ONU et où sont détenus les djihadistes à plus «haute valeur (...). Les coordonnées GPS collectées à proximité de certains sites moscovites sensibles (Kremlin, aéroport Vnukovo...) sont sans rapport avec la réalité et démontrent l'efficacité des dispositifs de brouillage GPS mis en place par les autorités russes.

En somme, les ressources ouvertes de Strava permettent d'imaginer les fonctionnalités offertes par les malwares commerciaux, qui permettent de suivre simultanément plusieurs dizaines de milliers d'individus!

TTU No 1095, 7 février 2018.