L'intelligence collective et la veille technologique pour faire face aux défis de la cyberdéfense

Autor(en): **Mallart, Thomas / Mermoud, Alain**

Objekttyp: **Article**

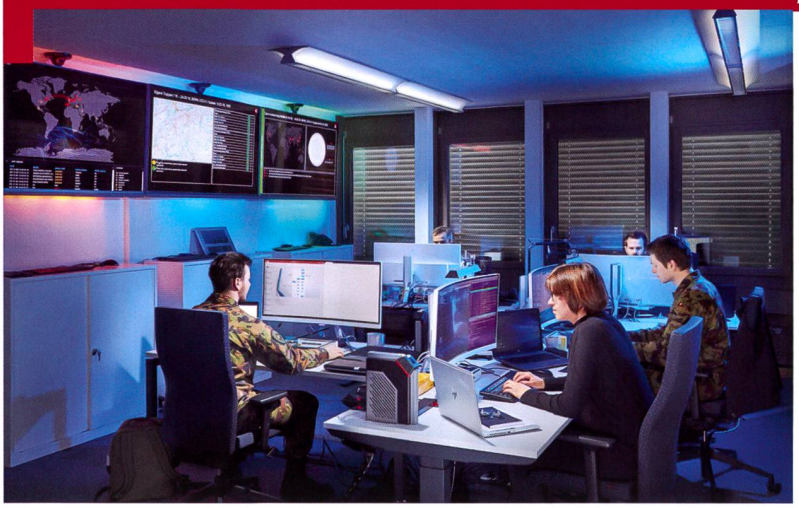
Zeitschrift: **Revue Militaire Suisse**

Band (Jahr): **- (2020)**

Heft 3

PDF erstellt am: **22.07.2024**

Persistenter Link: https://doi.org/10.5169/seals-913873



Notre système de milice est un type d'intelligence collective qu'il convient d'optimiser pour favoriser l'émergence d'une cyberdéfense collaborative.

Cyberdéfense

L'intelligence collective et la veille technologique pour faire face aux défis de la cyberdéfense

Dr. Thomas Maillart*, Dr. Alain Mermoud**

* Maitre d'Enseignement et de Recherche (MER) à l'Université de Genève, Département de Management et d'Economie

** Chef veille technologique Cyber-Defence Campus, armasuisse Sciences et Technologies (S+T)

Pour faire face à l'accélération de l'évolution des cyber-menaces, les systèmes d'information et leurs usages doivent être adaptés en permanence. Cette anticipation est, et sera encore longtemps, un privilège et une responsabilité des humains. Les responsables de la sécurité doivent donc trouver des solutions pratiques à des problèmes complexes, dans un temps de plus en plus court, et si possible avant la matérialisation des menaces. Dans cet article, nous proposons de mobiliser l'intelligence collective humaine afin d'assurer un niveau de résilience satisfaisant face aux incertitudes liées à l'anticipation des cyber-menaces. Nous considérons que le système de milice suisse représente une chance unique pour déployer une approche *bottom-up* d'intelligence collective et de veille technologique. Enfin, nous proposons trois axes stratégiques de préparation et illustrons notre propos à l'aide des projets *Crowd-GPS-Sec* et STM, développés par armasuisse.

L'intelligence collective fait partie de l'ADN d'Internet

Le réseau Internet tel qu'on le connaît aujourd'hui est le résultat de pratiques basées sur l'action collective, et de choix techniques fondamentaux concernant l'absence d'implémentation de sécurité dans l'Internet Protocol (IP).[1] La conjonction de cette technologie et d'un état d'esprit d'ouverture a permis l'avènement d'une révolution technologique du savoir, dont l'humanité a connu uniquement trois précédents au cours de son histoire : (i) le langage, (ii) l'écriture, et (iii) l'imprimerie.

Ainsi, ce réseau a permis une explosion de la production, de l'échange et de la recombinaison innovante de l'information, qui est à la fois la source et la conséquence de l'innovation. Depuis plus de deux décennies, chaque humain connecté à Internet peut partager ses expériences uniques (i.e., ses innovations au sens large) avec le reste du monde. De même, chaque humain connecté a accès à un trésor de savoir, permettant d'innover, et donc d'améliorer son environnement de vie de manière très concrète, et éventuellement de repartager son expérience. Ainsi, le cyberespace est capable de générer collectivement des nouvelles innovations, mais qui paradoxalement, le rend fragile dans le sens où l'innovation elle-même force sa propre adaptation. Anticiper et aller plus vite qu'un changement issu d'une intelligence collective humaine massive est devenu un véritable défi que seule l'intelligence collective (et l'anticipation par la veille technologique) peut en général surmonter.

L'intelligence collective est aussi pratiquée par les criminels

La capacité d'innovation et d'adaptation collective offerte par les technologies de l'information est aussi à disposition de la cybercriminalité, qui, par définition, n'a pas vocation à respecter les lois en vigueur. A mesure qu'Internet a été utilisé pour des tâches plus critiques (transactions financières, échanges et stockage de données personnelles, contrôles de systèmes critiques, civils, gouvernementaux et militaires, etc.), la cybercriminalité s'est organisée pour en tirer des revenus et autres avantages en conséquence. De la même manière, les *advanced persistent threats (APT)* dont la source est principalement les états, visent les infrastructures critiques, à des fins de violation de la confidentialité, de l'intégrité ou de la disponibilité des systèmes.

L'absence de *security by design* favorise l'attaquant

1 Maillart, T. 2011. Mechanisms of Internet Evolution and Cyber Risks, ETH Zurich Dissertation. Cette thèse de doctorat est disponible au téléchargement à l'adresse suivante: https://ethz.ch/content/dam/ethz/special-interest/mtec/chair-of-entrepreneurial-risks-dam/documents/dissertation/PHD_Maillart_Final_thesis.pdf (consulté le 9.10.19)

L'héritage technologique du protocole IP, destiné à transférer l'information rapidement et de manière robuste mais non sécurisée, fait fondamentalement pencher la balance en faveur de l'offensive. En effet, Internet est toujours sécurisé après coup par l'addition de couches de sécurité au fur et à mesure que les applications se développent, sont propagées, et deviennent donc critiques. En principe, cette approche réactive pourrait fonctionner, à condition que les organisations impliquées puissent réagir presque instantanément à l'évolution des menaces. Ceci n'est évidemment pas le cas pour deux raisons : (i) certaines menaces existent avant qu'elles soient connues de leurs cibles (par ex., les vulnérabilités *zero-day*), et (ii) les organisations en général s'adaptent trop lentement face à une menace qui évolue de manière très soudaine, selon les dynamiques non linéaires de l'innovation sur Internet, et en grande partie grâce à l'intelligence collective des cybercriminels, qui utilisent le *darknet* pour échanger et mutualiser leur savoir. En exploitant cette asymétrie d'information, les criminels ont souvent une longueur d'avance.

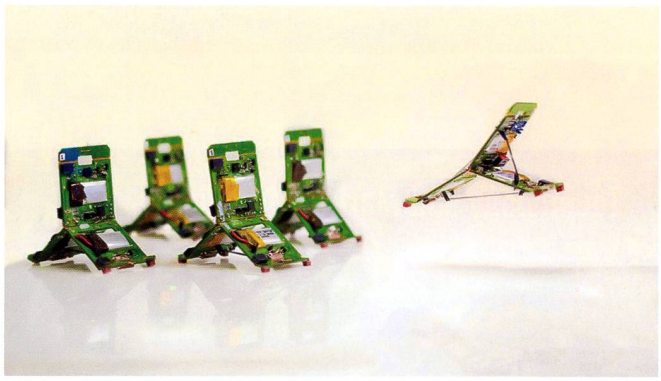
Une surprenante capacité de résilience du défenseur

Internet représente donc un changement de paradigme dans le sens où pour la première fois dans l'histoire de l'humanité un système de communication se met à jour de manière quasi autonome et évolutionnaire par le fait de la réduction des frictions dans la transmission de l'information et des interfaces. Ces évolutions, le plus souvent *bottom-up*, ne sont pas linéaires, difficiles à anticiper et peuvent transformer soudainement le cyberespace, avec toutes sortes d'enjeux économiques, politiques, sociaux, et culturels. Ces changements rapides et difficiles à prévoir posent un défi d'adaptation fondamental, notamment dans le cadre de stratégies de cyberdéfense. Bien que le monde de la cybersécurité soit profondément imprégné d'une culture du secret, largement héritée de l'industrie de la défense, la promotion d'une culture de partage des données peut changer cette culture. Il s'agit donc d'établir un compromis entre les risques de divulgation d'informations sensibles et le potentiel de résoudre un problème compliqué et critique dans le temps en le soumettant à l'intelligence collective d'un cercle plus large.[2]

Construire des stratégies de cyberdéfense adaptives grâce à la veille technologique

Dans ce contexte d'innovations rapides des systèmes d'information, de leur utilisation et des cyber-menaces, un grand danger serait de baser une stratégie de cyberdéfense sur des menaces existantes. Lorsque la première stratégie nationale de cyberdéfense suisse a été conçue en

2 La thèse de doctorat [2] du deuxième auteur, déjà évoquée dans la RMS N°6 / 2018, s'intéresse précisément au mécanisme incitatif permettant de favoriser le partage de l'information utile à la cybersécurité entre opérateurs d'infrastructures critiques, telles que les banques systémiques, les réseaux électriques ou de télécommunications. Cette thèse est téléchargeable depuis SERVAL, le dépôt institutionnel académique de l'UNIL : https://serval.unil.ch/notice/serval:BIB_5D54879D8F67 (consulté le 15.08.19)



Inspirés de l'intelligence collective des fourmis, de petits robots (baptisés « Tribots ») de 10 grammes développés à l'EPFL peuvent communiquer entre eux, s'attribuer différents rôles et réaliser ensemble des tâches complexes. Dotées d'une structure simple, ces machines reconfigurables sont capables de sauter et ramper pour se déplacer sur des surfaces accidentées.

2011, la désinformation massive sur les réseaux sociaux n'existait quasiment pas. Aujourd'hui, nous savons que les *fakes news* et le profilage psychologique ont été utilisés par des puissances étrangères pour déstabiliser des élections démocratiques aux Etats-Unis, et probablement en Grande Bretagne et en France. Dans les mois qui viennent, les *deep fakes* pourraient devenir rapidement une nouvelle menace contre l'intégrité de l'information. De manière plus générale, les menaces futures pourraient exploiter toutes sortes de failles humaines et logicielles nouvelles sans qu'il soit vraiment possible pour une personne de se rendre compte qu'elle a été trompée.

Une plateforme d'anticipation pour surveiller les technologies et les marchés

Historiquement, la base technologique et industrielle performante (BTIS) d'armasuisse constituait un élément important de la politique d'armement.[3] La BTIS englobait les instituts de recherche et les entreprises installés en Suisse et disposant de compétences, connaissances et capacités en matière de sécurité et de défense. En 2018, la procédure d'auto-inscription dans la base de données BTIS a été remplacée par la plateforme « *Surveillance des Technologies et des Marchés* » (STM) automatisée. Les données sont désormais récoltées via un robot d'indexation (*web crawler*) qui explore des sources publiques comme les registres du commerce, les sites web d'entreprise ou encore les réseaux sociaux. Les données sont recherchées à intervalles réguliers et mises à jour tous les mois dans la plateforme STM. La STM permet de retrouver des entreprises ainsi que les informations qui s'y rapportent, comme les produits, les services et les technologies qu'elles proposent. Ces entreprises sont par conséquent visibles tant comme fournisseurs (ou sous-traitants) potentiels que comme partenaires de compensation éventuels dans le cadre d'une acquisition.

3 https://www.ar.admin.ch/fr/beschaffung/ruestungspolitik-des-bundesrates/sicherheitsrelevante-technologie-und-industriebasis-stib.html (consulté le 08.04.20)

A l'avenir, la plateforme STM – Technology Intelligence for National Security (TMM en anglais) devra également être capable de suivre les développements technologiques relatifs au cyber afin d'établir une image globale et en déduire des conséquences pour soutenir les développements du DDPS, comme prévu dans le Plan d'Action Cyberdéfense (PACD).[1]

Détection précoce des tendances ou technologies et acquisition des connaissances utiles

Par ailleurs, le développement de STM répondra à la mesure 4.1 «*acquisition de compétences et de connaissances*» de la stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC) 2018-2022, formulée ainsi: «*les nouvelles tendances ou technologies dans le domaine de l'informatique ainsi que les opportunités et les risques qui en résultent doivent être identifiés à intervalles réguliers et de bonne heure. Les résultats de ce monitoring seront communiqués aux acteurs scientifiques, économiques, politiques et sociaux. La recherche fondamentale et appliquée sera encouragée dans le cadre des structures et processus en place (par ex. des programmes nationaux de recherche), en fonction des besoins et des possibilités*».[4]

Trois niveaux d'adaptation collective

Pour assurer la résilience face à des cyber-menaces connues, mais aussi inconnues, il est nécessaire d'adopter une stratégie de cyberdéfense qui intègre les capacités d'adaptation et d'innovation des citoyens et des mondes académique, économique et militaire.

1. Adaptation par l'expérience et l'apprentissage collectif. La protection des systèmes d'information et des comportements humains nécessite une vigilance généralisée. Certaines menaces ne peuvent être détectées ou contrées uniquement à l'aide de ressources humaines distribuées. Le projet *Crowd-GPS-Sec* est une solution pratique qui utilise l'intelligence collective (voir encadré ci-dessous). La totale autonomie des citoyens participants à *Crowd-GPS-Sec* peut rendre quasi impossible la neutralisation du système distribué de détection de *spoofing* GPS. De plus, le déploiement d'un tel système peut constituer une expérience d'apprentissage collectif d'un outil de détection et de prévention de menaces. La *cybersécurité participative* pourrait engager de manière similaire les citoyens cyber-miliciens pour un grand nombre d'autres problèmes de cybersécurité.

2. Adaptation par la recherche collective. Un autre problème qui intéresse la cybersécurité est la recherche et la découverte de vulnérabilités dans les logiciels. Il a été montré qu'un moyen de maximiser la découverte d'erreurs de code et de vulnérabilités, passe par l'exposition d'un grand nombre de chercheurs au code source. En conséquence, un nombre croissant d'organisations lance des *bug bounty programs* qui mobilisent l'intelligence collective pour trouver des vulnérabilités. Une étude scientifique récente a montré qu'une explication possible à la performance limitée d'une seule personne pourrait tenir au phénomène de *charge cognitive* qui fait que cette personne a une perspective limitée sur la nature du code à inspecter et trouvera probablement des bugs plutôt dans son propre champ de perspective. Une autre personne avec une perspective différente trouvera d'autres bugs, et ainsi de suite [3].

3. Adaptation par la veille technologique et l'engagement collectif. L'exemple *Crowd-GPS-Sec* nous enseigne une autre leçon très importante : l'innovation pratique qui peut être déployée facilement a des atouts considérables d'adaptation. Il est critique d'encourager la multiplication des innovations que l'on peut qualifier de frugales, et s'assurer que tout le monde les comprenne et les utilise. Réduire les cycles d'innovation et les possibilités de dissémination effective (par exemple par un choix de partage en logiciel ouvert) doit permettre l'adaptation rapide si et quand cela est nécessaire. D'une manière générale, ces innovations doivent être nombreuses, et doivent être pratiquées et testées de manière régulière. En outre, les cyber-miliciens doivent être formés, de la même manière que pour l'usage du matériel militaire physique.

Le système de milice est une forme d'intelligence collective

Conférence du Cyber-Defence Campus le 3 et 4 novembre au SwissTech Convention Center de l'EPFL

Les pirates informatiques ont une longue histoire dans le domaine du partage d'expériences, d'outils et de vulnérabilités, ce qui a contribué au succès de la majorité des cyberattaques. L'objectif de cette conférence du CYD Campus est d'explorer diverses mesures pour rendre la veille technologique, le partage d'informations et l'intelligence collective également efficaces du côté des défenseurs. Ainsi, cette conférence réunira des acteurs de l'économie, du monde politique, académique et de l'armée. Inscription et information sur l'application «Events ar WT» ou via le site internet du CYD Campus : https://www.ar.admin.ch/fr/armasuisse-wissenschaft-und-technologie-w-t/cyber-defence_campus

4 https://www.isb.admin.ch/isb/fr/home/ikt-vorgaben/strategien-teilstrategien/sn002-nationale_strategie_schutz_schweiz_cyber-risiken_ncs.html (consulté le 08.04.20)

La notion de système de milice désigne un principe d'organisation couramment pratiqué dans la vie publique en Suisse. Elle repose sur l'idée républicaine selon laquelle le citoyen qui en a les capacités doit assumer des charges et des tâches publiques à titre extraprofessionnel et bénévole. Cette expression propre à la Suisse est empruntée au vocabulaire militaire (lat. *militia*). C'est par ce système que le transfert de connaissance entre la société civile et la défense se fait, d'une manière classique, en Suisse et en Israël. Ce transfert permet à l'armée de disposer rapidement de compétences rares et précieuses à un coût réduit [4]. Ce système doit être maintenu, voire renforcé, comme c'est déjà le cas pour l'instruction dans le domaine cybernétique qui permet d'obtenir un diplôme fédéral de *Cyber Security Specialist*.[5] Dans cette perspective, le système de milice est un type d'intelligence collective qu'il convient aujourd'hui d'appliquer massivement aux défis de la cyberdéfense.

T.M., A.M.

Scanner ce code QR pour visionner une vidéo de présentation de *Crowd-GPS-Sec.*

Bibliographie

[1] Jansen, K., Schäfer, M., Moser, D., Lenders, V., Pöpper, C., & Schmitt, J. 2018. *Crowd-gps-sec*: Leveraging crowdsourcing to detect and localize gps spoofing attacks. In *2018 IEEE Symposium on Security and Privacy (SP)* (pp. 1018-1031). IEEE.

[2] Mermoud, A. 2019. Three Articles on the Behavioral Economics of Security Information Sharing: A Theoretical Framework, an Empirical Test, and Policy Recommendations. *Doctoral Dissertation, Université de Lausanne, Faculté des hautes études commerciales.*

[3] Maillart, T., et al. 2017. Given enough eyeballs, all bugs are shallow? Revisiting Eric Raymond with bug bounty programs. *Journal of Cybersecurity* 3.2: 81-90.

[4] Percia David, D., Keupp, M.M., Marino, R., & Hofstetter, P. 2019. The Persistent Deficit of Militia Officers in the Swiss Armed Forces: An Opportunity Cost Explanation, *Defence and Peace Economics*, 30:1, 111-127.

5 https://www.vtg.admin.ch/fr/actualite/themes/cyberdefence.html#Instruction-cybernetique (consulté le 15.08.19)

Exemple concret d'un système d'intelligence collective développé par armasuisse S+T

En collaboration avec une équipe internationale de chercheurs, le domaine de compétences Sciences et technologies (S+T) d'armasuisse développe un système basé sur l'intelligence collective pour protéger l'espace aérien global contre les cyberattaques visant le système de navigation par satellites GPS. L'exemple ci-dessous démontre comment l'intelligence collective en source ouverte permet de résoudre concrètement un important problème de cybersécurité.

***Crowd-GPS-Sec*: un système pour détecter et localiser les attaques par *spoofing* GPS**

L'article scientifique [1] résumé ici présente *Crowd-GPS-Sec*, un système indépendant pour détecter et localiser les attaques par *spoofing* (usurpation d'identité) du Global Positioning System (GPS) dans le contexte du trafic aérien. Les signaux transmis par ce système mondial de positionnement par satellites peuvent être librement reçus et exploités par quiconque, par exemple avec un assistant de navigation comme TomTom ou Garmin embarqué dans une automobile.

Le problème: la dépendance croissante de l'industrie de l'aviation à l'égard du GPS pour faciliter la navigation et la surveillance du trafic aérien ouvre de nouvelles possibilités d'attaques. Aujourd'hui, il est relativement facile et peu coûteux de manipuler le système GPS avec un émetteur d'ondes radioélectriques disponible en vente libre sur Internet. Couplé avec une radio logicielle, ce type d'appareil permet de générer un faux signal GPS – indétectable par les récepteurs GPS classiques – afin d'interférer avec le trafic aérien. L'attaquant peut ainsi potentiellement détourner un drone, comme ce fut probablement le cas avec le drone américain RQ-170 *Sentinel* capturé en 2011 par l'armée iranienne.

La solution: les auteurs répondent à cette vulnérabilité critique avec une solution en deux étapes:
1) La détection: *Crowd-GPS-Sec* permet de détecter les attaques par *spoofing* en vérifiant si les données transmises par un aéronef – potentiellement victime d'un *spoofer* (l'attaquant) – sont conformes aux données issues du crowdsourcing (production participative). Concrètement, les attaques sont détectées par une infrastructure indépendante qui analyse en permanence le contenu et les heures d'arrivée de signaux aériens diffusés périodiquement par les avions à des fins de contrôle de la circulation aérienne. Ces données existantes sont collectées selon le principe du *crowdsourcing* par OpenSky Network, une association à but non lucratif basée en Suisse qui met à la disposition du public les données relatives aux communications sur le trafic aérien.
2) La localisation: lorsqu'une attaque est détectée, *Crowd-GPS-Sec* va chercher à localiser les dispositifs du *spoofer*. Cette deuxième étape permet de traquer un attaquant afin de prendre les mesures appropriées pour arrêter l'attaque. Le système estime la position du *spoofer* en analysant les différences de temps entre les positions reçues de l'avion et la position réelle estimée par *Crowd-GPS-Sec*. Les auteurs démontrent que *Crowd-GPS-Sec* est capable de détecter les attaques par *spoofing* GPS en moins de deux secondes et de localiser l'attaquant avec une précision de 150 mètres après 15 minutes de surveillance. Un avantage important de ce système est qu'il n'exige aucune mise à jour de l'infrastructure GPS, contrairement aux tentatives précédentes de sécurisation du GPS.