La veille technologique au services de l'écoystème fédéral de la cyberdéfense

Autor(en): **Cuche, Kilian / Mermoud, Alain**

Objekttyp: **Article**

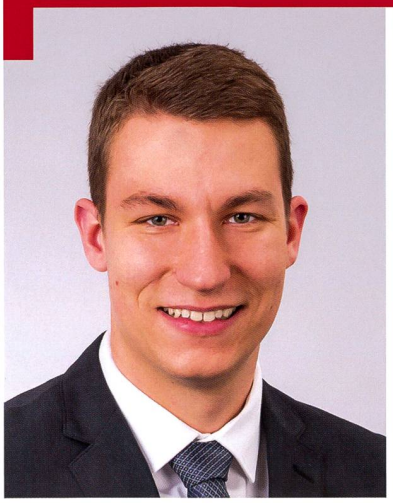
Zeitschrift: **Revue Militaire Suisse**

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

Heft 6

PDF erstellt am: **27.07.2022**

Persistenter Link: http://doi.org/10.5169/seals-913935



La veille et l'anticipation technologique permettent une planification des investissements et des développements plus agiles, surtout dans le domaine cyber, où les technologies changent très rapidement.

Armasuisse S+T

La veille technologique au service de l'écosystème fédéral de la cyberdéfense

MSc Kilian Cuche*, Dr. Alain Mermoud**

* Master of Science HES-SO in Business Administration, orientation Management des Systèmes d'Information

** Chef veille technologique Cyber-Defence Campus, armasuisse S+T

Ces dernières années, on a pu observer une évolution constante des cybermenaces. Elles se développent de manière exponentielle au développement des nouvelles technologies qui apportent des risques mais également des opportunités. Les attaques sont toujours plus sophistiquées et impliquent désormais de l'intelligence artificielle ainsi que des techniques de *social engineering* toujours plus poussées. En fin de compte, l'attaquant a presque toujours une longueur d'avance sur le défenseur qui est constamment sous la pression d'une nouvelle attaque ou d'un nouveau mode de fonctionnement. Les équipes de sécurité sont très souvent en mode réactif, dépendante des actions des attaquants avant de pouvoir prendre des mesures. En effet, une approche *all hazard* (prête pour tous les dangers) impliquerait des coûts beaucoup trop élevés pour les organisations et les Etats.

Une contribution à la mesure 1 et 2 de la SNPC

Pour faire face à ces nouveaux défis, la cybersécurité s'est énormément développée ces dernières années. Les secteurs publics, privés et académiques redoublent d'efforts pour augmenter le niveau de sécurité et de résilience de la société face aux menaces cyber. La défense dans le domaine cyber est devenue un nouvel enjeu de sécurité nationale. Pour répondre à ces nouvelles menaces, la Suisse a élaboré plusieurs stratégies dont la principale est la stratégie nationale de protection de la Suisse contre les cyberrisques 2018-2022[1] (SNPC ou NCS en allemand) qui en est déjà à sa deuxième version. Le Département fédéral de la défense, de la protection de la population et des sports (DDPS) a développé son propre plan appelé Plan d'Action Cyberdéfense[2] (PACD) qui est actuellement en révision car il date de 2017. Ces deux documents présentent des mesures à implémenter au sein de l'administration fédérale, mais pas seulement, afin d'augmenter la défense et la résilience cyber de la Suisse.

On constate également que ce domaine est en constante évolution et que les stratégies évoluent avec les menaces, leurs formes et leur intensité. Actuellement, la collaboration entre les différentes entités dédiées au cyber pourrait être améliorée. L'échange d'informations, de connaissances et de compétences est présent, mais pourrait être amélioré et renforcé. La mise en place du nouveau centre national pour la cybersécurité (NCSC) devrait pallier à ce manque une fois qu'il sera totalement fonctionnel.

En partant de ces constats, une thèse de master en systèmes d'information a été réalisée dans ce domaine avec l'ambition d'apporter une pierre à l'édifice de la SNPC et du PACD, et par extension à la cyberdéfense en Suisse.[3]

Une collaboration CYD Campus, ACAMIL, HES-SO

Ce travail de master réalisé à la Haute école spécialisée de Suisse occidentale (HES-SO) s'est inscrit dans deux projets de recherche appliqués menés par des unités du DDPS impliqués dans la cyberdéfense. Premièrement, la chaire d'économie de défense de l'Académie militaire (ACAMIL) qui a lancé deux projets au sujet de la gestion des ressources (humaines et matérielles) pour la cyberdéfense[4]. Afin de mener à bien ces projets, il était nécessaire de comprendre et connaître l'écosystème public Suisse dédié aux aspects cyber au niveau fédéral. Le deuxième projet dans lequel s'inscrit cette thèse est

1 https://www.isb.admin.ch/isb/fr/home/themen/cyber_risiken_ncs/ncs_strategie.html

2 https://www.vbs.admin.ch/fr/defense/protection-cyberattaques.detail.document.html/vbs-internet/fr/documents/defense/cyberattaques/Aktionsplan-Cyberdefense-f.pdf.html

3 Cette thèse est disponible sur demande auprès du premier auteur par e-mail : kilian.cuche@vtg.admin.ch

4 Voir article consacré à la chaire d'économie de défense dans ce numéro RMS.

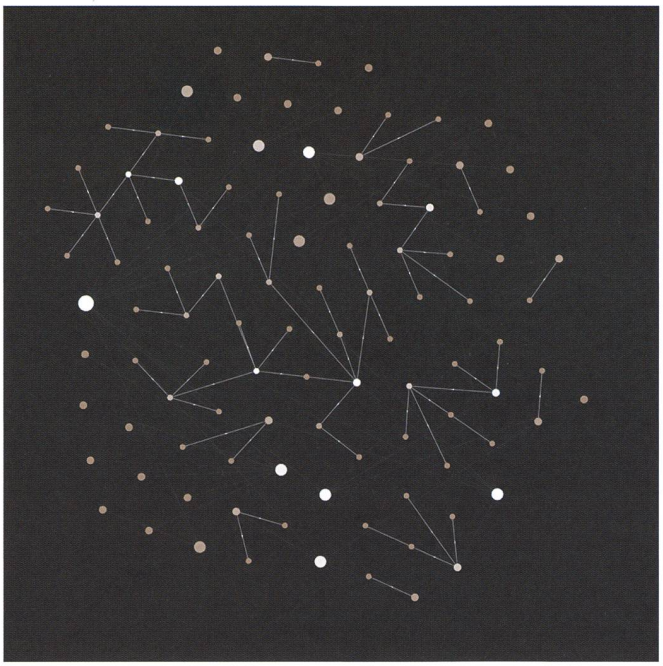
le développement d'un nouvel outil d'anticipation et de veille technologique (Technology and Market Monitoring 2.0 – TMM 2.0) par le Cyber-Defence Campus basé à l'École polytechnique fédérale de Lausanne (EPFL). Cet outil doit, à terme, servir de soutien à l'anticipation technologique pour tous les acteurs fédéraux impliqués dans le domaine cyber.

Les trois objectifs principaux étaient les suivants: Premièrement, il s'agissait de cartographier de manière interactive les acteurs publics impliqués dans la cyberdéfense au niveau fédéral avec leur mission et leurs compétences pour déterminer qui fait quoi. Ensuite, afin d'aider au développement de l'outil TMM 2.0, une analyse business (compréhension du contexte, des parties prenantes et récolte des besoins des utilisateurs) a été menée parmi les acteurs identifiés. Finalement, une série de recommandations ont été fournies pour le développement de TMM 2.0 afin d'offrir un maximum de valeur ajoutée aux utilisateurs finaux.

Audience cible: les acteurs cyber de la Confédération

Pour réaliser cette cartographie et identifier les acteurs publics actifs dans le domaine cyber, deux types de données ont été synthétisées. Premièrement, les données *open data* au travers des documents stratégiques de la Confédération et les publications scientifiques et techniques dédiées au domaine cyber en Suisse. Puis, ces éléments ont été complétés par des données qualitatives récoltées au travers d'une quarantaine d'interviews semi-directifs menés avec des acteurs du domaine cyber au sein de l'administration fédérale et du DDPS.

Cet écosystème, considéré comme une organisation, est finalement représenté de deux manières. Premièrement sous la forme d'un graphe en réseau qui représente les relations hiérarchiques entre les unités administratives.



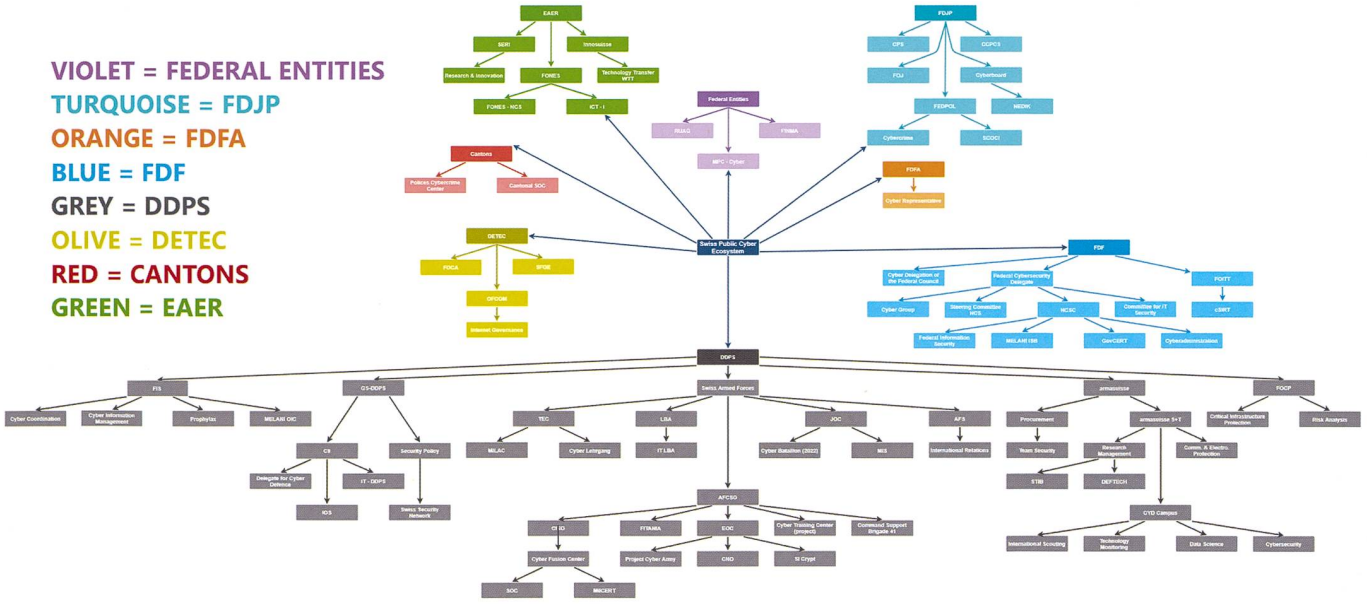
Ce graphe en réseau disponible en ligne permet de naviguer entre les différentes unités administratives fédérales impliquées dans le domaine cyber (nœuds) ainsi que de visualiser leurs relations hiérarchiques (arcs).

L'outil en ligne *Rhumbl* a permis de rendre le résultat accessible pour tout le monde.[5] Cette représentation est vouée à être améliorée et complétée. Toute remarque ou complément sont les bienvenus à l'adresse email mentionnée ci-dessus.

Finalement, cette analyse a également permis de réaliser des tableaux qui présentent et détaillent les activités de 100 entités actives dans le domaine cyber au niveau fédéral. Le graphe en réseau présenté précédemment étant

5 https://rhumbl.com/app/share/5e8afc1e64f2a64af2d40d47

Cet organigramme disponible sur demande en fichier numérique permet de visualiser l'écosystème fédéral dédié au domaine cyber. Il est séparé par couleurs qui font références aux différents départements de l'administration fédérale.



principalement destiné à des analyses pour la recherche, une autre visualisation plus accessible, sous la forme d'un organigramme structurel a également été réalisée.

Analyse des besoins en veille technologique

La deuxième phase de cette thèse consistait à analyser les besoins en veille technologique de ces différentes parties prenantes afin d'optimiser le développement de l'outil TMM 2.0. Pour commencer, le contexte du projet a été analysé en collaboration avec les acteurs d'armasuisse Sciences et Technologies (S+T). Ensuite, une analyse de l'outil existant (TMM 1.0)[6] a été réalisée afin de se familiariser avec l'outil et ses capacités.

Finalement, des acteurs externes ont été approchés afin d'avoir une vision de leurs principaux besoins en veille technologique dont par exemple le chef de l'armée, le délégué fédéral à la cybersécurité, les personnes responsables du cyber au secrétariat général du DDPS, le chef de la base d'aide au commandement (BAC), ainsi que le responsable du réseau national de sécurité (RNS). A la fin, ce sont une quarantaine de personnes qui ont été approchées afin de contribuer à l'analyse des besoins pour TMM 2.0.

Une contribution à la plateforme TMM

La plateforme TMM est issue d'un projet itératif avec différentes étapes. A la base, TMM était un projet de recherche qui visait à tester des méthodes d'analyse quantitatives pour évaluer l'émergence des technologies en utilisant des informations *open data* comme les publications scientifiques, les brevets et le registre du commerce. En deuxième instance, ce projet a remplacé la base technologique et industrielle importante pour la sécurité (BTIS). Actuellement, TMM permet principalement de rechercher des entreprises en fonction de leurs différentes technologies. Cet outil offre également des analyses sur les tendances technologiques ainsi que des classements d'entreprises, d'organisations et de chercheurs sur des technologies spécifiques. Il est également possible de trouver des brevets, des publications ainsi que des offres d'emploi selon différents secteurs technologiques.

Pour faire suite aux deux stratégies mentionnées en début d'article, le projet TMM 2.0 est né avec pour objectif de répondre aux mesures concernant le développement d'une capacité d'anticipation technologique. Afin de prioriser le développement pour répondre aux besoins principaux, des groupes d'utilisateurs ont été créés afin de pouvoir déterminer leurs besoins essentiels et les représenter sous la forme de produits minimum viables (*MVPs*).

Cependant, avant de déterminer les nouveaux besoins, plusieurs points d'amélioration possible lors du passage de TMM 1.0 à TMM 2.0 ont été identifiés. Ces derniers concernent la définition du cadre et des limitations de l'outil ou encore la différentiation de l'outil par rapport à ses concurrents ou partenaires tel que le programme de prospective technologique DEFTECH. L'augmentation de l'usage ainsi qu'une amélioration des interfaces et des fonctionnalités ont également été relevés. Finalement, il s'agissait d'augmenter la qualité des données et la précision du *crawler* afin de pouvoir délivrer différents scores en toute transparence.

Recommandations pour TMM 2.0

Afin de supporter la prise de décision dans la conduite de ce projet, trois types de recommandations ont été proposées. La première concerne la réalisation de *MVPs*. Un *MVP* global présente une priorisation des besoins de tous les utilisateurs afin d'apporter un maximum de valeur lors du développement de l'outil. De plus, les besoins spécifiques de chaque groupe d'utilisateurs sont présentés sous la forme de *MVPs* indépendants. Cette priorisation est réalisée au moyen d'une formule mathématique qui prend en compte l'importance des parties prenantes ainsi que la fréquence du besoin demandé.

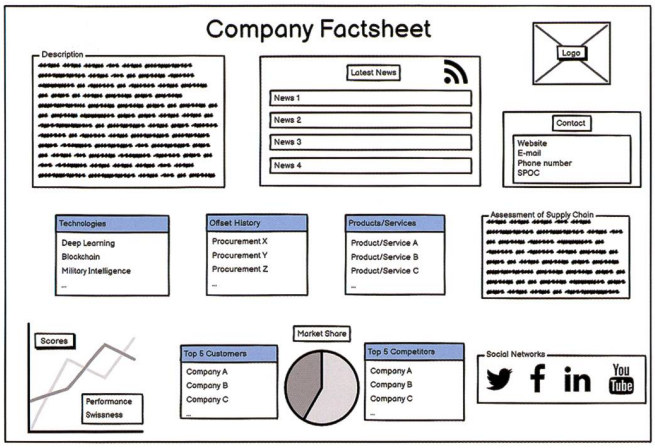
Le besoin principal identifié pour cette plateforme réside dans son approche. Le cadre de recherche doit être international et global au niveau des technologies surveillées. Néanmoins, il est nécessaire d'avoir un focus sur la Suisse afin que cet outil puisse permettre des analyses qualitatives au sein des différentes unités fédérales.

En ce qui concerne les principales fonctionnalités identifiées comme primordiales pour le futur de l'outil, on peut citer la génération de fiches techniques (sur les entreprises et les technologies), la possibilité de s'abonner à des alertes afin d'être averti en cas de changements majeur dans le paysage technologique ou le marché de la défense ainsi que l'accès à des rapports sur mesure centrés sur une technologie ou une entreprise particulière.

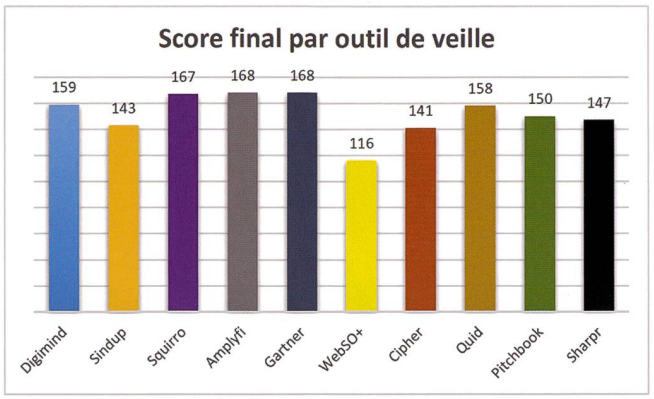
La visualisation des données prend également une place importante, que cela soit sous la forme de tableaux de bord stratégiques ou de *hub* d'export de données pour les chercheurs. Finalement, des nouvelles possibilités de filtres ont été demandées (actuellement, le seul filtre disponible est celui des types de technologies) comme des filtres par secteur d'activité basé sur la nomenclature générale des activités économiques (NOGA), par capacité militaire ou encore par région, pays et date.

L'outil devra être capable d'intégrer des sources internes ainsi que des données non-structurées tout en disposant d'une interface utilisateur agréable et moderne (*responsive*). Concernant la transition de TMM 1.0 vers TMM 2.0, certains points d'importance ont relevés tels que l'intégration et la communication avec les parties prenantes tout au long du processus ainsi que la possibilité de former les potentiels utilisateurs sur l'outil. Finalement, la classification des informations aura une énorme importance suite à la possible intégration de sources internes. Il s'agira de bien gérer les droits d'accès ainsi que les différents niveaux de classification.

6 https://tmm.dslab.ch/#/home



Cette fiche technique est une visualisation des informations jugées comme primordiales pour la représentation d'une entreprise. Elle représente les besoins exprimés par les parties prenantes sous une forme visuelle et permet de définir la forme d'un livrable potentiel pour TMM 2.0.



Ce graphique représente le score final attribué pour les outils testés en fonction de différents critères d'analyse. Ces critères font références aux besoins identifiés pour TMM 2.0 et sont basés sur des benchmarks utilisés dans le domaine de l'Intelligence Economique.

De plus, des maquettes d'interfaces et de fonctionnalités ont été ajoutées afin d'aider au développement de l'outil. Ci-dessus, on trouve un exemple d'une fiche technique d'entreprise qui pourrait être générée avec l'outil TMM 2.0.

Pour terminer, une série de recommandations managériales ont été formulées afin de supporter les décisions stratégiques. Ces dernières insistent sur le fait d'utiliser des méthodes agiles dans le développement de ce projet afin d'éviter une trop grande différence entre les résultats finaux et les besoins évolutifs des utilisateurs. En effet, ces derniers sont sujets à des variations en fonction de l'évolution des métiers et des technologies. Sur un projet d'une telle ampleur, il serait dangereux de fixer des exigences au début du processus et de ne pas pouvoir revenir sur celles-ci en cours de route.

D'autres recommandations au sujet de l'intégration des sources internes et du niveau d'analyse des informations ont été formulées afin d'aider à la prise de décision sur ces points essentiels pour le futur de l'outil TMM. Pour terminer, ce travail a été mené conjointement avec une thèse de bachelor réalisée à la Haute Ecole de Gestion de Genève par David Marques. Son travail avait pour but d'analyser différents outils choisis en fonction des besoins identifiés pour TMM 2.0. Cette analyse a permis de classer ces différentes plateformes afin d'aider à la prise de décision concernant l'intégration, ou non, de ces dernières.

Conclusion

Premièrement, ce travail a permis de découvrir et cartographier l'écosystème mis en place par la Confédération pour lutter contre les cyberrisques. Les unités administratives impliquées dans la cyberdéfense sont connues, mais manquent parfois d'une vue d'ensemble et d'une coordination interdépartementale efficace. C'est pour pallier à ces problématiques que le nouveau centre national pour la cybersécurité (NCSC) a été mis en place. Il a pour but d'être le point central pour les questions liées à la cybersécurité ainsi que de mettre en œuvre et coordonner la SNPC.

On peut également remarquer une faiblesse structurelle dans cet écosystème due au système d'économie planifiée de l'administration fédérale. En effet, la plupart des unités doivent lutter entre elles pour avoir les ressources nécessaires pour produire de la cyberdéfense. Comme cela implique plusieurs départements, certaines querelles politiques s'ajoutent sur ce problème. De ce fait, un certain temps est investi dans des activités de *lobbying* pour obtenir plus de financement ou de ressources humaines et cela au détriment du travail effectif dédié à augmenter la sécurité de la Suisse. Bien entendu, ce n'est pas le cas partout, mais ce genre de comportements économiques a pu être relevé plusieurs fois. Afin de pallier à ces problématiques, il est nécessaire de bien définir les missions et compétences de chaque entité dédiée au domaine cyber, mais également d'investir les moyens nécessaires pour la défense dans le domaine cyber, au même titre que dans les autres sphères d'opérations.

On peut aussi remarquer que la cyberdéfense est trop souvent perçue par son point de vue technique. Bien entendu, la sécurité informatique nécessite une forte composante technique, mais une approche holistique est nécessaire si l'on veut être efficace et efficient. Des domaines variés tels que le management, l'économie et les sciences sociales sont nécessaires pour développer une cyberdéfense complète. Cela permet par exemple d'optimiser la gestion des ressources, d'implémenter des politiques et des prescriptions légales et d'optimiser les partenariats entre les différents écosystèmes (publics, privés et académiques).

Finalement, une fois les futurs développements effectués pour TMM 2.0, on pourrait envisager d'automatiser la réalisation de cartographies ou de réaliser d'autres projets impliquant des analyses de données quantitatives relatives au domaine cyber. Cet outil devra à terme selon la SNPC, servir à toute l'administration fédérale comme référence concernant l'anticipation technologique.

K. C. & A. M.