Technometrics : la science au service de la veille technologique pour la cyberdéfense

Autor(en): **Mermoud, Alain / Percia David, Dimitri / Maillart, Thomas**

Objekttyp: **Article**

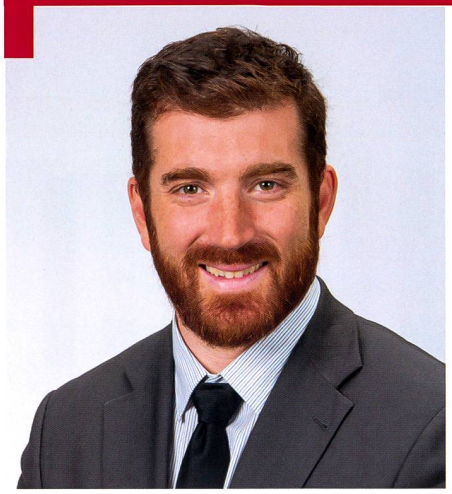
Zeitschrift: **Revue Militaire Suisse**

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

Heft 6

PDF erstellt am: **26.06.2024**

Persistenter Link: https://doi.org/10.5169/seals-913936



Le Dr. Dimitri Percia David est bénéficiaire du premier Cyber-Defence Campus (CYD) *Distinguished Postdoctoral Fellowship* et chercheur postdoctoral à la Faculté d'Economie et de Management de l'Université de Genève, plus précisément à l'Information Science Institute. Son superviseur, le Dr. Thomas Maillart est maître d'enseignement et de recherche dans la même faculté et le même institut, et est spécialisé dans la recherche sur l'intelligence collective et les cyber-risques. Interview conjoint.

Armasuisse S+T

Technometrics : La science au service de la veille technologique pour la cyberdéfense

Propos recueillis par le Dr. Alain Mermoud
Rédacteur adjoint RMS+

Comment fonctionne la collaboration entre l'Université de Genève et le *CYD Campus* d'armasuisse Sciences et Technologies (S+T) ?

Dimitri Percia David (DPD) : *L'École polytechnique fédérale de Lausanne (EPFL) et le CYD Campus s'engagent conjointement en faveur de la recherche et de la formation dans le domaine de la cyberdéfense. Les « CyberDefence Fellowships » sont ouverts aux chercheurs de niveau master, doctorat et postdoc. Deux postulations par année sont possibles, en principe au printemps et en automne. Une pré-sélection a lieu sur la base d'une proposition de recherche. Les candidats retenus se voient alors attribués, par un comité scientifique indépendant, un « Scientific Project Manager » du CYD Campus en fonction du sujet de recherche choisi.*[1] *Dans mon cas, c'est le Dr. Alain Mermoud, chef de la veille technologique au sein du CYD Campus, qui m'a été attribué. En parallèle, il est important de sélectionner un superviseur dans une haute école suisse qui a la volonté et la capacité d'encadrer une recherche scientifique liée à la cyberdéfense. Dans mon cas, le choix du MER Dr Thomas Maillart s'est fait naturellement et rapidement, car son expertise conjointe en innovation, intelligence collective et modèles quantitatifs liés aux cyber-risques est incontestablement unique. Si vous étudiez au sein d'une haute école suisse et souhaitez faire progresser la recherche dans le domaine des sciences de la sécurité et des données, les « CYD fellowships *» sont faits pour vous !*

Thomas Maillart (TM) : *Du point de vue de l'Université de Genève, ce « fellowship » est considéré comme une entrée de fonds de recherche, comme dans le cas de l'obtention d'une bourse du Fonds national suisse de la recherche scientifique (FNS), par exemple. D'ailleurs, les « CYD fellows » sont rémunérés et engagés aux conditions du FNS. Dans le cas d'un postdoc, le financement est garanti pour deux ans. C'est évidemment un grand honneur pour l'Université de Genève d'avoir décroché le premier postdoc « CYD fellowship » ! L'initiative d'armasuisse S+T comble un vide important et permet l'émergence d'un « DARPA helvétique » (ndlr : l'agence pour les projets de recherche avancée de défense du département de la défense des Etats-Unis), au sein duquel des projets d'innovation hors du commun (« moonshot ») ont clairement le potentiel d'émerger et d'aider à développer des délivrables concrets pour le futur de la cyberdéfense. Je me réjouis vivement de collaborer avec le CYD Campus et de contribuer au développement scientifique de la cyberdéfense via le projet Technology & Market Monitoring, déjà évoqué dans la RMS+ N°3 2020.*[2]

En quoi la veille technologique est une activité importante pour la cyber-sécurité ?

DPD : *Comme le souligne la « Stratégie nationale pour la protection de la Suisse contre les cyber-risques » (SNPC, 2018-2022), la veille de marché et l'identification précoce des technologies émergentes et/ou de rupture constitue un élément clé de la stratégique de cyberdéfense de notre pays. Parler de veille de marché et d'identification précoce, c'est parler de renseignement lié au développement technologique. Aussi, le développement d'une capacité de cyberdéfense passe nécessairement par le renseignement sur les menaces, puisque ce n'est qu'au travers de ce dernier que l'on peut classifier les menaces par niveau de dangerosité et de probabilité d'occurrence – deux facteurs-clé de l'analyse du risque. Une analyse minutieuse, systématique et continue des innovations technologiques est ainsi nécessaire pour déceler leur impact en termes de risques (menaces potentielles) et*

1 Les sujets de recherche d'intérêt pour le CYD Campus sont disponibles sur le site de l'EPFL : https://www.epfl.ch/research/services/fund-research/funding-opportunities/fellowship-mobility/cyd-fellowships/cyd-master-thesis-topics/ (consulté le 29.09.20)

2 Maillart, T. ; Mermoud, A. *L'intelligence collective et la veille technologique pour faire face aux défis de la cyberdéfense, in* Revue Militaire Suisse (RMS+) N°3 - 2020.

opportunités (réponses appropriées). Une telle analyse demande ainsi une capacité de veille du marché technologique lié à la cyberdéfense, mais également et surtout une capacité d'identification précoce des technologies impactant la cyberdéfense.

De manière plus large, le développement d'une capacité de cyberdéfense s'inscrit dans la politique et les procédures d'acquisition d'armement du DDPS, selon les recommandations du cabinet Deloitte rendues publiques en juin 2020.[3] *La démarche de poursuite de la mise en place de capacités de cyberdéfense s'inscrit dans la perspective des grands projets de ces quinze prochaines années, notamment le renouvellement des moyens de protection de l'espace aérien (Air2030), et la modernisation des Forces terrestres. Or, dans le contexte de développement d'une capacité de cyberdéfense – impliquant du matériel d'armement à fort contenu informatique –, il existe un risque lié à l'obsolescence prématurée des systèmes. Ainsi, les systèmes risquent d'être déjà obsolètes au moment de leur introduction auprès de la troupe alors qu'ils ne l'étaient pas encore lors de la décision d'acquisition. L'intervalle entre le temps nécessaire à l'acquisition du matériel (temps d'acquisition) et la décroissance de l'efficience technologique (temps technologique) est un problème propre à l'acquisition de matériel informatique et au développement d'une capacité de cyberdéfense. Une activité de veille technologique devrait alors permettre de réduire l'intervalle entre le temps d'acquisition et le temps technologique en sélectionnant les technologies les plus pertinentes à acquérir. En tant que commandant de compagnie, je suis particulièrement sensible à cet élément. Ainsi, la plateforme TMM sera également capable de suivre les développements technologiques relatifs au cyber-espace afin d'établir une image globale et en déduire des conséquences pour soutenir à la fois les développements stratégiques et la politique d'acquisition de matériel du DDPS, comme prévu dans le Plan d'Action Cyberdéfense (PACD).*

TM : *Jamais la technologie n'a évolué aussi vite qu'aujourd'hui. Du jour au lendemain, des technologies émergentes font leur apparition, et certaines changent radicalement le contexte et l'environnement de la cyberdéfense. De ce fait, il est critique de pouvoir anticiper les technologies qui vont faire la différence à court, moyen, et long terme. Il est important de bien modéliser les structures et dynamiques associées à une multitude de technologies en cours de développement, et ce afin de mieux pouvoir émettre des recommandations visant à adapter l'investissement et l'acquisition des technologies. Lors de la préparation de la première stratégie de cyberdéfense de la Suisse en 2011, j'avais été invité à donner un séminaire dans lequel je recommandais à la Confédération d'investir – via un fond spécial de capital-risque labellisé cyberdéfense – dans les technologies émergentes ayant un impact potentiel pour la cyber-défense. Le projet TMM 2.0 a clairement pour but d'opérationnaliser cette proposition formulée il y a maintenant presque 10 ans.*

3 https://www.admin.ch/gov/fr/accueil/documentation/communiques.msg-id-79450.html (consulté le 29.09.20)

Vous évoquez la SNPC. Dans le cadre de cette stratégie, comment est-ce que votre recherche contribue au développement d'une capacité de veille technologique pour la Confédération ?

DPD : *Afin de répondre à la mesure 1 (détection précoce des tendances ou technologies et acquisition des connaissances utiles) de la SNPC, le CYD Campus développe un « Tech Watch Program » avec sa propre plateforme de veille technologique inspirée de la base technologique et industrielle importante pour la sécurité (BTIS), qui constitue un élément important de la politique d'armement. La BTIS englobe 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 une « Surveillance des Technologies et des Marchés » (STM ; TMM en anglais) 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'entreprises 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, les experts, 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. En outre, nous effectuons des analyses sur mesure pour le compte du Secrétariat général du DDPS et le nouveau Centre national pour la cyber-sécurité (NCSC) qui est le centre de compétences de la Confédération en matière de cyber-sécurité et le premier interlocuteur pour les milieux économiques, l'administration, les établissements d'enseignement et la population pour toute question relative à la cyber-sécurité. Avec le NCSC, qu'il a placé sous la direction du délégué de la Confédération à la cyber-sécurité (ce dernier dépend directement du chef du Département fédéral des finances (DFF)), le Conseil fédéral entend renforcer le rôle actif de la Confédération dans la protection de la Suisse contre les cyber-risques. Notre objectif est donc d'alimenter la Confédération, via le CYD Campus, en produits (livrables) de veille technologique et pas uniquement le DDPS.*

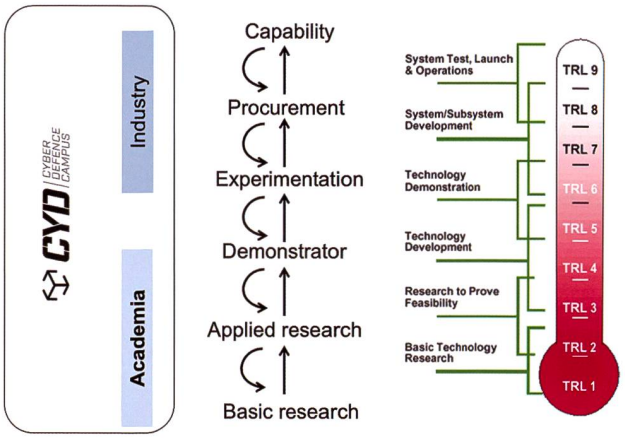
TM : *Du point de vue de la littérature scientifique, la veille technologique est une sous-discipline du « Technology Management ». Notre objectif est de contribuer à l'amélioration de la plateforme STM grâce à notre expertise scientifique. Pour cela, nous utilisons et développons des modèles scientifiques que nous validons empiriquement, dans le but d'automatiser :*
1. la ***surveillance*** *des développements technologiques en général et le suivi de leur évolution/adoption au sein du marché ; 2. la* ***prédiction*** *des tendances et des développements technologiques, incluant l'anticipation des technologies de rupture (disruptive) ; 3. l'****évaluation des risques et des opportunités*** *des développements technologiques pour la cyberdéfense.*

Ces trois buts permettent de : a. délivrer une identification précoce des tendances technologiques en distinguant et en cartographiant les acteurs (industrie : entreprises, fournisseurs, etc. ; recherche scientifique : chercheurs-clé, laboratoires, projets, etc.), les clusters technologiques et les hubs géographiques par cluster ; b. anticiper les tendances technologiques et évaluer les risques et les opportunités liés à ces mêmes tendances technologiques. Il sera alors possible d'identifier et de cartographier les organisations et les personnes associées à une technologie, d'établir des liens et d'éclairer les relations entre les différentes entités liées à une technologie donnée, d'identifier les changements de positionnement technologique des différentes entités liées à une technologie donnée, de délivrer une profilage des différentes communautés technologiques, de prédire les tendances technologiques et les futurs acteurs-clé , et d'observer le potentiel latent de synergies entre des disciplines scientifiques et des technologies.

De nombreux consultants – comme Gartner ou Forrester – offrent des services de veille technologique. En quoi votre approche est-elle différente ?

TM : *Notre objectif est de fournir des modèles quantitatifs de prévision technologique et des outils de surveillance du marché pour la cyberdéfense, basés sur les méthodes fournies par la science des données (data science). En partant d'une perspective socio-technique des systèmes d'information, nous appliquons certains principes de la physique appliquée à l'économie (econophysics), de l'apprentissage machine (machine learning), et de la microéconomie au domaine de la cyberdéfense. Une telle approche va permettre développer un tableau de bord quantitatif pour surveiller de quelle manière les technologies : (i) émergent, (ii) attirent une attention plus large (notamment en différenciant les bulles technologiques et le potentiel à long terme), (iii) se développent et mûrissent soudainement ou progressivement, et (iv) deviennent pertinentes en termes d'investissement, en particulier dans la perspective de la cyberdéfense. Pour ce faire, nous procédons en plusieurs étapes : Premièrement, nous analysons les réseaux de capacité de production, les structures et les dynamiques de l'innovation qui sous-tendent le cycle de vie de chaque technologie, en particulier son niveau de maturité technologique (« Technology Readiness Level », TRL). Puis nous développons des modèles prédictifs, grâce à l'intelligence artificielle, pour évaluer le potentiel de croissance de chaque technologie, et ses conséquences prédictibles pour la cyberdéfense. Enfin, nous modélisons des portefeuilles d'investissements par classes de technologies, afin de mieux diriger les investissements publics et privés, en particulier de manière à diversifier les risques extrêmes liés aux technologies émergentes.*

DPD : *La société Gartner propose une courbe de « maturité technologique » (parfois aussi appelée « hype curve »). Bien qu'elle semble intuitivement assez juste, cette courbe ne repose pas sur une analyse scientifique solide. Les techniques classiques de veille stratégique et d'identification précoce des tendances technologiques sont essentiellement basées sur des analyses qualitatives telles que : 1. des approches intuitives (jugement personnel, opinion d'expert, opinion de groupe d'experts, ou encore sur des méthodes structurées d'évaluation d'opinions de groupes d'experts, la méthode Delphi faisant référence dans ce domaine) ; 2. des approches mécanistiques comme la mise en réseau graphique, l'extrapolation de tendances ou encore des modèles de causalité ; 3. un mélange des deux premières méthodes. L'approche actuelle souffre de 2 problèmes : d'une part, elle n'est ni systématique ni quantitative et ne permet donc pas délivrer des prédictions solides. D'autre part, à l'heure de la multiplication d'inventions technologiques qui peuvent vraiment faire la différence (« game changer »), l'approche actuelle ne peut pas être appliquée à très large échelle. Les techniques de la science des données et de l'intelligence artificielle permettent de tester et valider un très grand nombre de scénarios au fur et à mesure que des données actualisées sont fournies à nos modèles.*



Infographique présentant le cycle de création d'une capacité de cyberdéfense : Par le biais d'un écosystème tripartite d'experts en cybersécurité – mêlant l'industrie (entreprises et « hubs » technologiques), le monde académique (laboratoires et chercheurs de référence) et armasuisse S+T –, une importante émulation d'idées et de projets voit le jour. Les besoins en termes de biens et services liés à la cybersécurité deviennent alors l'objet de recherches fondamentales et/ou appliquées, menant ainsi à des « proofs-of-concept » qui, lorsqu'ils s'implémentent de manière satisfaisante, deviennent intéressant pour les programmes d'acquisition et d'achats de matériel, contribuant à la création d'une capacité de cyberdéfense. A droite, le modèle de « Technology Readiness Level » (TRL) permet d'estimer le degré de maturité d'une technologie donnée, et peut donc être mis en parallèle avec le modèle de création de capacité en cyberdéfense. Source : armasuisse S+T.

Quels sont les technologies qui vont le plus influencer la cyberdéfense à court, moyen et long terme ?

DPD : *A court terme, on peut évidemment citer la technologie 5G. Pour rappel, en Suisse, deux groupes d'entreprises s'affrontent pour la 5G : d'un côté Sunrise et Huawei, de l'autre Swisscom et Ericsson. Les Etats-*

Unis affirment avoir trouvé la preuve que Huawei espionne pour le compte de la Chine. Ils font donc pression sur la Suisse, ainsi que sur l'Allemagne, pour qu'elles renoncent aux technologies chinoises pour le développement de la 5G. Pour l'instant, les autorités suisses voient le dossier Huawei davantage comme le théâtre d'une guerre commerciale que comme un problème de sécurité. Cependant, la polémique autour de ce dossier démontre que l'implémentation d'une nouvelle technologie échappe rarement à des logiques de guerre économique, mais aussi à des considérations géopolitiques.

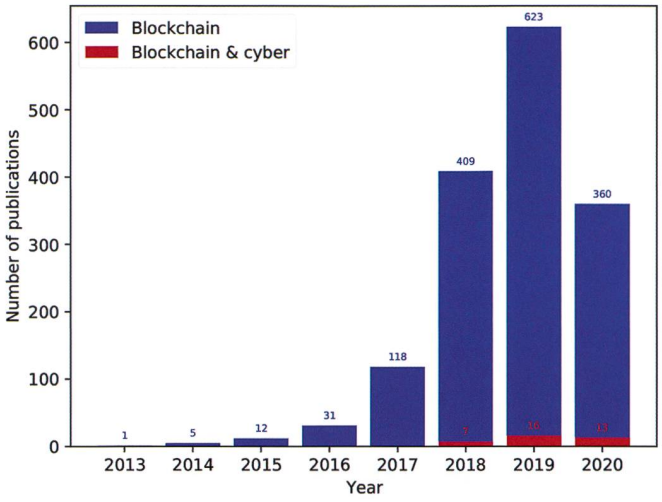
Aussi, lors d'un séminaire stratégique de deux jours, les experts du CYD Campus ont identifié un portfolio de technologies pouvant avoir un impact sur la cyberdéfense à moyen terme. Citons par exemple: les intelligences artificielle et collective («artificial intelligence» (AI), et «swarm intelligence»), les senseurs et la sécurité de l'Internet des objets («Internet of Things» (IoT) en anglais), le «edge computing», les mécanismes de préservation de la vie privée, l'apprentissage profond («deep learning»), le E-ID, le «graph analyse», etc. Au cours des deux prochaines années, nous allons analyser chaque technologie identifiée une par une afin de déterminer son impact potentiel sur la cyberdéfense.

Concernant la prospective à long terme, armasuisse S+T poursuit, sous la conduite du Dr Quentin Ladetto, le programme de recherche en veille technologique DEFTECH[4] dont le but est de détecter les technologies à caractère disruptif ainsi que d'anticiper leurs impacts pour le monde militaire en général, et l'Armée suisse en particulier. Le CYD Campus poursuite également une activité de «scouting» à l'international (ndlr: évoquée dans ce numéro de la RMS). Cette activité nous permet d'injecter du renseignement technologique d'origine humaine dans notre recherche.

TM: *A long terme, le calculateur quantique («quantum computing» en anglais) aura d'une manière quasi certaine un impact très important sur la cyberdéfense, en particulier sur la cryptographie, mais aussi sur la puissance de calcul. Cependant, il faut se méfier des modes. Le CYD Campus a récemment conduit une recherche sur les cas d'utilisation de la technologie Blockchain pour la cyberdéfense. Les résultats montrent que cette technologie (très à la mode dans la fintech) semble n'apporter qu'un gain marginal dans le domaine spécifique de la cyberdéfense. Nous espérons qu'une approche scientifique neutre permettra de rester en permanence concentré sur les innovations technologiques qui vont vraiment faire la différence.*

Est-il possible de s'informer, de contribuer, ou de collaborer à vos recherches?

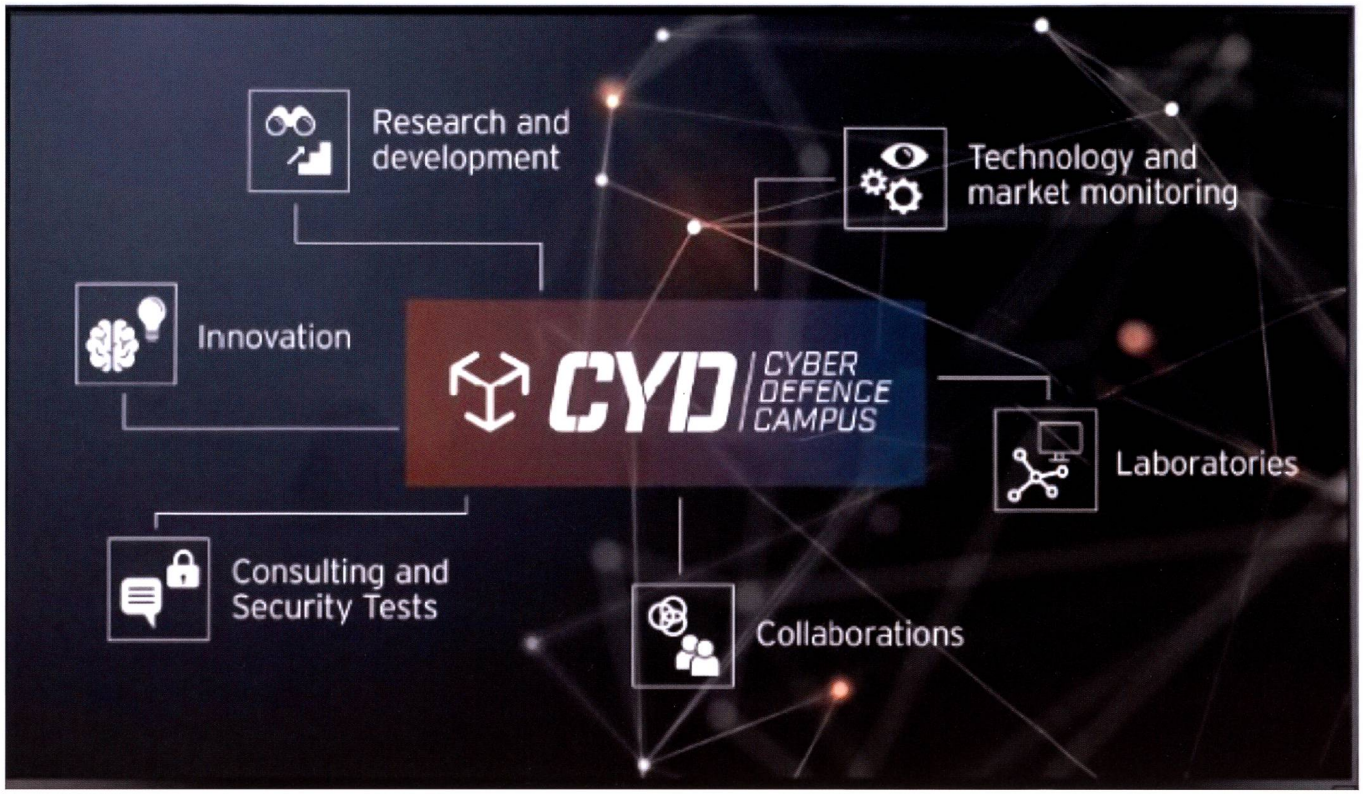
TM: *Outre sa rigueur d'exécution, une recherche scientifique de qualité doit nécessairement trouver sa source dans des problèmes concrets, si possible pour lesquels il existe des éléments empiriques (c'est-à-dire des données de qualité suffisante). De ce point de vue, il est absolument vital pour nous de dialoguer avec les organisations directement concernées par la cyberdéfense, telles que les autorités publiques, les entreprises spécialisées et les infrastructures critiques, afin d'affiner nos questions de recherche. Pour cela, le 3 novembre 2020, nous aurons l'honneur de présenter les éléments-clé de notre stratégie de recherche lors d'une grande conférence au SwissTech Convention Centre de l'EPFL sur le sujet «Cyber-Threat & Technology Intelligence». Il est aussi prévu que nous fassions un point d'avancement lors des «Swiss Cyber Security Days» (SCSD) qui auront lieu les 10 et 11 mars 2021 au Forum Fribourg. Enfin, nous organisons en septembre 2021, avec le Dr. Alain Mermoud et le Dr. Dimitri Percia David, la conférence internationale CRITIS («International Conference on Critical Information Infrastructures Security») à l'EPFL. Le sujet de cette année portera principalement sur le «technology forecasting, monitoring, foresight, and scouting» pour la protection des infrastructures et services critiques. Information et inscriptions sur: www.critis2021.org*



Cet histogramme indique le nombre de publications sur arXiv.org (une archive ouverte de pré-publications électroniques d'articles scientifiques) contenant les mots clés «blockchain» (en bleu) et «blockchain AND cyber*» (en rouge) dans le titre et le résumé. A partir de 2018, un engouement (hype) clair est visible, alors que seul un petit nombre de publications liées à la (cyber-) sécurité et à la blockchain apparaissent. Cela montre également que les préoccupations de sécurité d'une technologie émergente arrivent souvent dans une deuxième phase. Source: chiffres fournis par Sébastien Gillard, Dimitri Percia David, Thomas Maillart.

DPD: *Nous invitons tous les chercheurs intéressés à contribuer à nos recherches, à postuler pour un CYD fellowship. Par ailleurs, armasuisse peut, sous certaines conditions, établir un contrat de recherche avec un institut de recherche public ou privé. Pour les jeunes en formation, la Confédération offre également la possibilité d'effectuer un stage dans notre équipe de recherche ou d'exécuter une thèse de master (mémoire)*

4 https://deftech.ch/ (consulté le 29.08.20)



Le technology and market monitoring est une mission importante pour le CYD Campus.

au sein du CYD Campus. En cas d'intérêt, il convient d'envoyer une requête par e-mail (avec CV) directement à : cydcampus@armasuisse.ch. Par ailleurs, nous entretenons des contacts réguliers avec des scientifiques, lors de conférences internationales ou via des publications scientifiques de premier plan en physique, en économie, et en management. Grâce au réseau international du CYD Campus, nous avons des contacts réguliers avec nos homologues américains et israéliens qui se posent souvent les mêmes questions que nous. En France, nous suivons attentivement la recherche en Économie de Défense qui a récemment publié un document fondamental sur le rôle des technologies et de l'innovation dans l'autonomie et la défense d'un pays.[5] *Au niveau de l'UE, nous collaborons avec l'Agence européenne de défense qui poursuit également un programme de Tech Watch*[6] *et le projet de recherche PYTHIA*[7] *(« Predictive methodologY for TecHnology Intelligence Analysis »). Au niveau Suisse, nous collaborons avec le laboratoire de systèmes d'informations répartis du Prof. Karl Aberer de l'EPFL, ainsi que l'Académie suisse des sciences techniques (SATW) qui publie chaque année un « Technology Outlook »*[8] *dans lequel des experts évaluent le potentiel de 37 technologies prometteuses pour la Suisse et son économie. En outre, je garde un fort lien avec mon ancien employeur, à la chaire Economie de Défense à l'Académie militaire (ACAMIL) à l'EPF de Zurich.*

A. M.

* Plus d'information et inscription sur le site du CYD Campus : http://cydcampus.ch

5 Mlizard, J. & Rademacher, B. (2020). Économie de défense : problématiques contemporaines. *Revue Défense Nationale*, 832(7), 7-11. https://www.cairn.info/revue-defense-nationale-2020-7-page-7.htm.

6 https://techwatch.eda.europa.eu/ (consulté le 29.08.20)

7 http://www.pythia-padr.eu/ (consulté le 20.08.20)

8 https://www.satw.ch/fr/cybersecurite/technology-outlook-2019 (consulté le 29.08.20)

La 16ème édition de l'**International Conference on Critical Information Infrastructures Security (CRITIS 2021)** aura lieu du 27 au 29 septembre 2021 à l'EPFL SwissTech Convention Center. Cette conférence scientifique aura lien conjointement avec une conférence du CYD Campus réunissant des professionnels et des experts de la protection des infrastructures critiques.

Information et inscription: https://critis2021.org/