Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

armasuisse
Science and Technology

Technology and Market Monitoring
Technology Intelligence for National Security

La veille technologique et scientifique pour la cyberdéfense

Dr. Alain Mermoud, MBA
jVeille 2022, Neuchâtel

CYD
CYBER DEFENCE CAMPUS

TMM is an important activity for anticipation and informed decision-making

“Aircrafts are interesting toys, but without military value”

- Marshal Ferdinand Foch, Ecole Supérieure de Guerre, 1904

TMM may reduce the gap with the technology growth

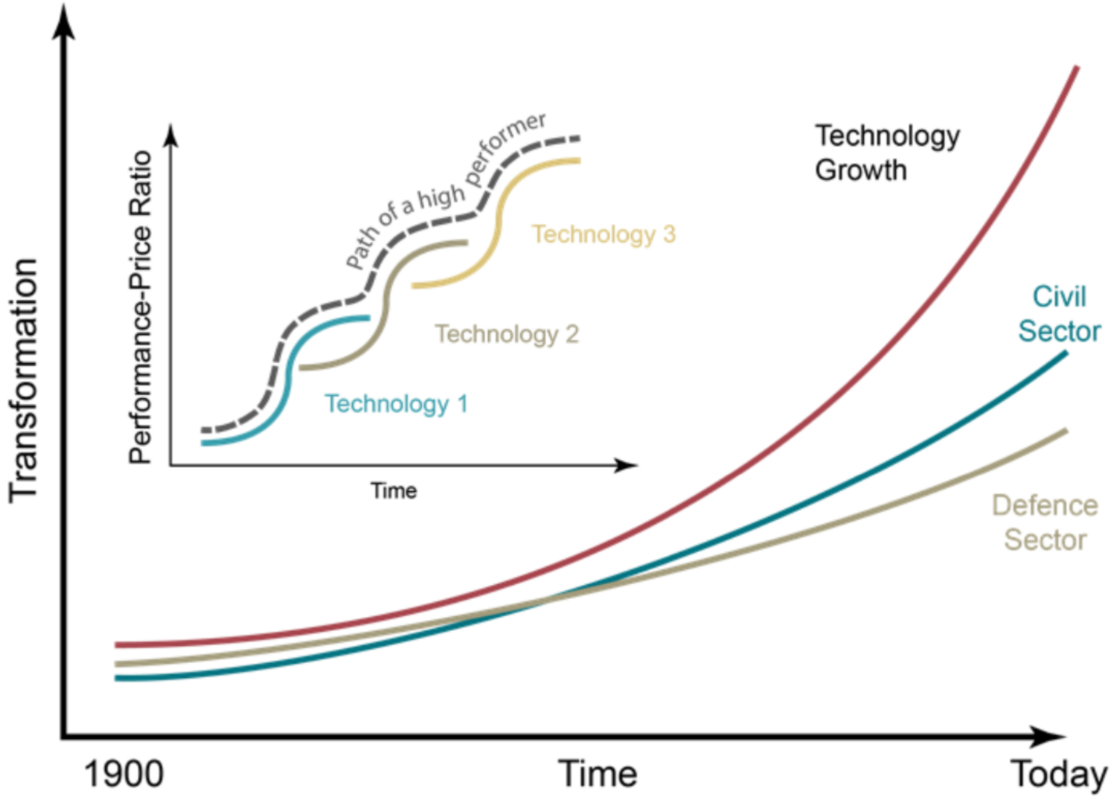
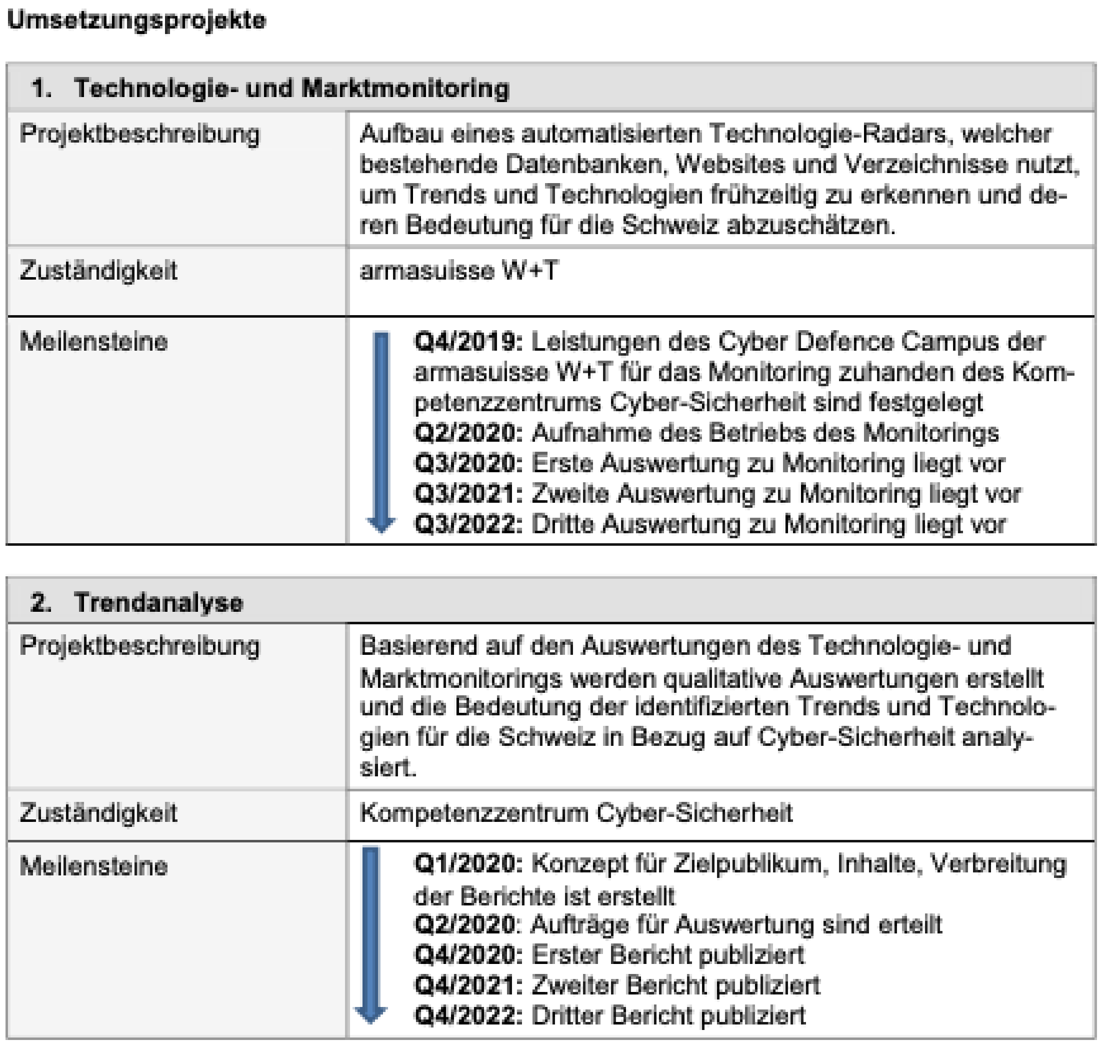


Figure 3: There exists a widening gap between the technology level in the civil sector compared to that in the defence sector. A technology market monitoring activity may reduce this gap by improving the defence sector's knowledge about the technology landscape.

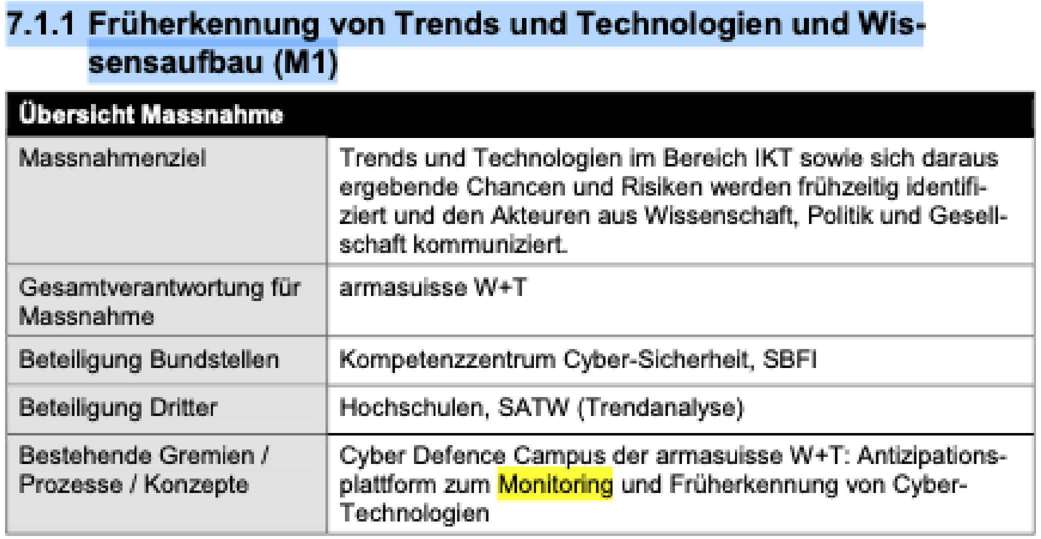
Policy Background: NCS 2018-2022



Umsetzungsprojekte

1. Technologie- und Marktmonitoring	
Projektbeschreibung	Aufbau eines automatisierten Technologie-Radars, welcher bestehende Datenbanken, Websites und Verzeichnisse nutzt, um Trends und Technologien frühzeitig zu erkennen und deren Bedeutung für die Schweiz abzuschätzen.
Zuständigkeit	armasuisse W+T
Meilensteine	**Q4/2019:** Leistungen des Cyber Defence Campus der armasuisse W+T für das Monitoring zuhanden des Kompetenzzentrums Cyber-Sicherheit sind festgelegt **Q2/2020:** Aufnahme des Betriebs des Monitorings **Q3/2020:** Erste Auswertung zu Monitoring liegt vor **Q3/2021:** Zweite Auswertung zu Monitoring liegt vor **Q3/2022:** Dritte Auswertung zu Monitoring liegt vor

2. Trendanalyse	
Projektbeschreibung	Basierend auf den Auswertungen des Technologie- und Marktmonitorings werden qualitative Auswertungen erstellt und die Bedeutung der identifizierten Trends und Technologien für die Schweiz in Bezug auf Cyber-Sicherheit analysiert.
Zuständigkeit	Kompetenzzentrum Cyber-Sicherheit
Meilensteine	**Q1/2020:** Konzept für Zielpublikum, Inhalte, Verbreitung der Berichte ist erstellt **Q2/2020**: Aufträge für Auswertung sind erteilt **Q4/2020:** Erster Bericht publiziert **Q4/2021:** Zweiter Bericht publiziert **Q4/2022:** Dritter Bericht publiziert



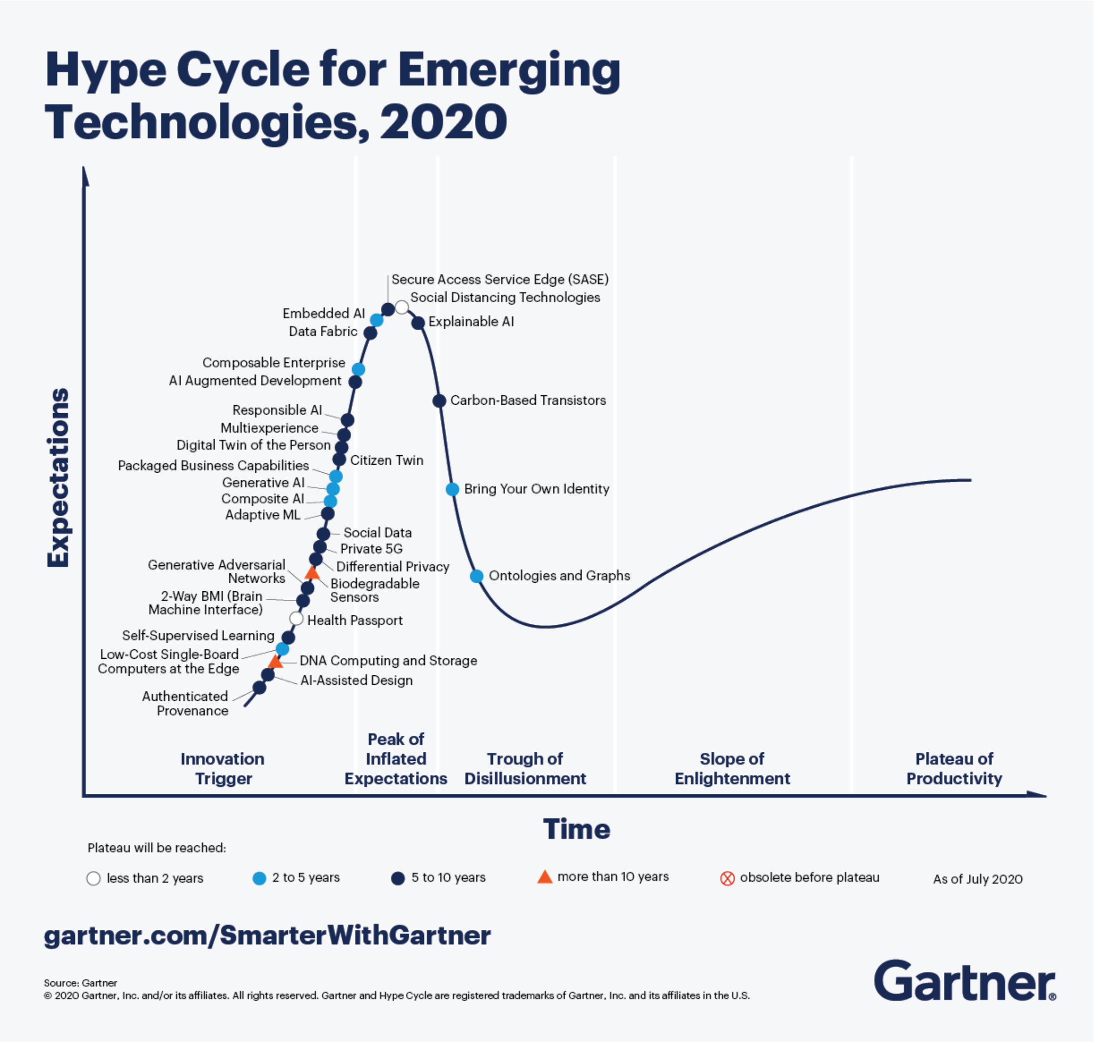
7.1.1 Früherkennung von Trends und Technologien und Wissensaufbau (M1)

Übersicht Massnahme	
Massnahmenziel	Trends und Technologien im Bereich IKT sowie sich daraus ergebende Chancen und Risiken werden frühzeitig identifiziert und den Akteuren aus Wissenschaft, Politik und Gesellschaft kommuniziert.
Gesamtverantwortung für Massnahme	armasuisse W+T
Beteiligung Bundstellen	Kompetenzzentrum Cyber-Sicherheit, SBFI
Beteiligung Dritter	Hochschulen, SATW (Trendanalyse)
Bestehende Gremien / Prozesse / Konzepte	Cyber Defence Campus der armasuisse W+T: Antizipationsplattform zum Monitoring und Früherkennung von Cyber-Technologien

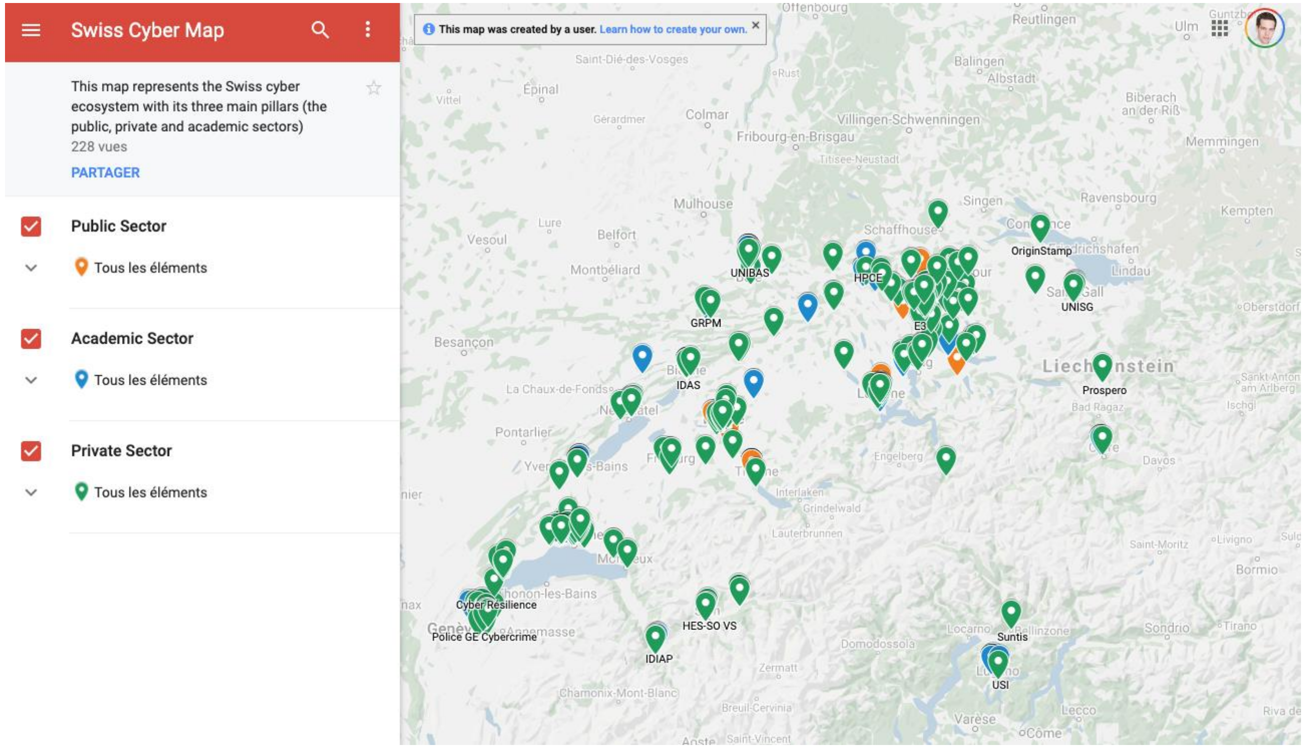
TMM Scientific Goal

- Identify, analyze and forecast trends related to cybersecurity technologies
  - How to find a ground truth / baseline for TMM?

Methods we should not discuss



Swiss Cyber Ecosystem Cartography



Swiss Cyber Map

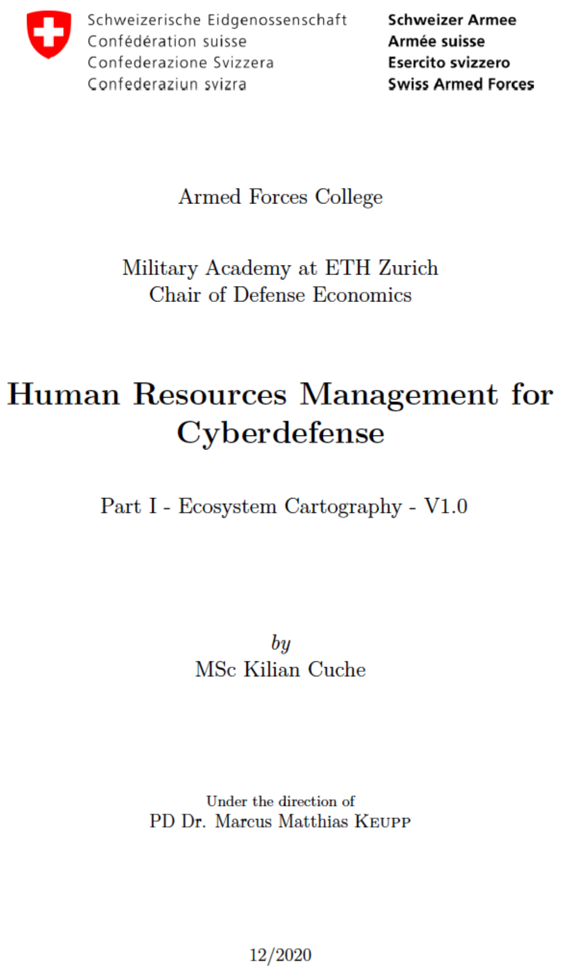
This map represents the Swiss cyber ecosystem with its three main pillars (the public, private and academic sectors)
228 vues
PARTAGER

☑ Public Sector
Tous les éléments

☑ Academic Sector
Tous les éléments

☑ Private Sector
Tous les éléments

This map was created by a user. Learn how to create your own.



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Schweizer Armee
Armée suisse
Esercito svizzero
Swiss Armed Forces

Armed Forces College

Military Academy at ETH Zurich
Chair of Defense Economics

Human Resources Management for Cyberdefense

Part I - Ecosystem Cartography - V1.0

by
MSc Kilian Cuche

Under the direction of
PD Dr. Marcus Matthias Keupp

12/2020

Link to a first version of the cyber cartography of Switzerland: https://bit.ly/3nVrkyX

CYD CYBER DEFENCE CAMPUS

TMM “Research Report” 2020

michael.tsesmelis@ar.admin.ch is looking for peer reviewers

Cybersecurity Technologies

An Overview of Trends in Switzerland and Abroad

Michael Tsesmelis, Dimitri Percia David, Thomas Maillart, Kilian Cuche, Giorgio Tresoldi, Colin Barschel, Quentin Ladetto, Sébastien Gillard, Loïc Maréchal, Claudia Schärer, Manuel Suter, Vincent Lenders, Alain Mermoud

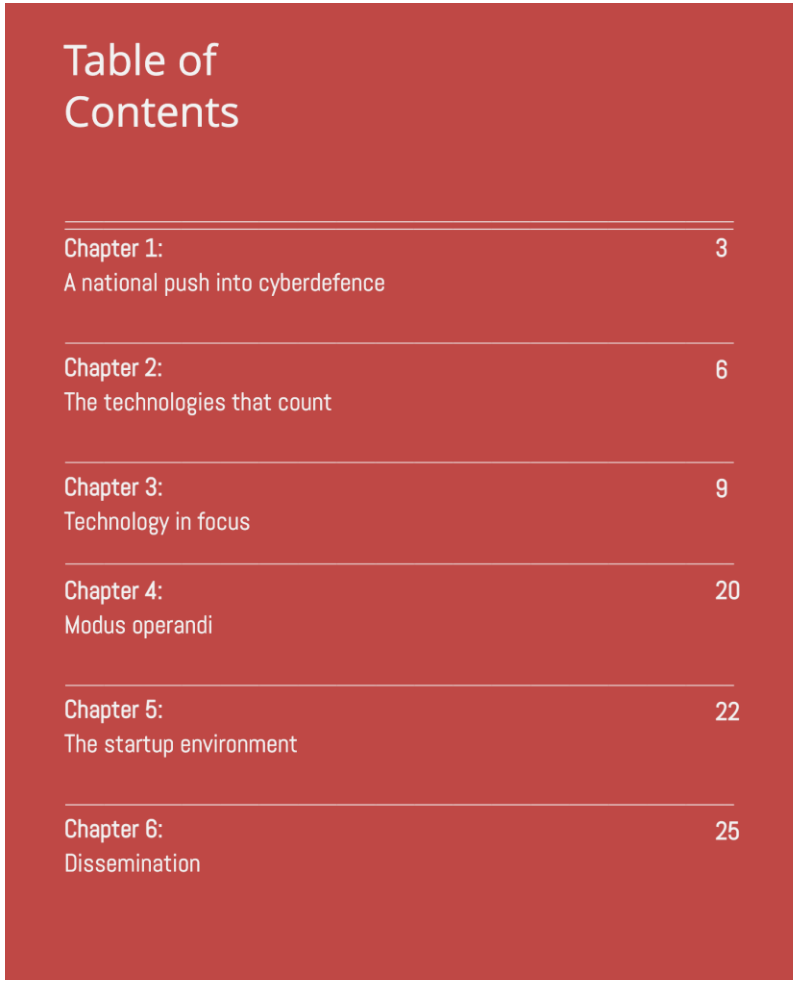
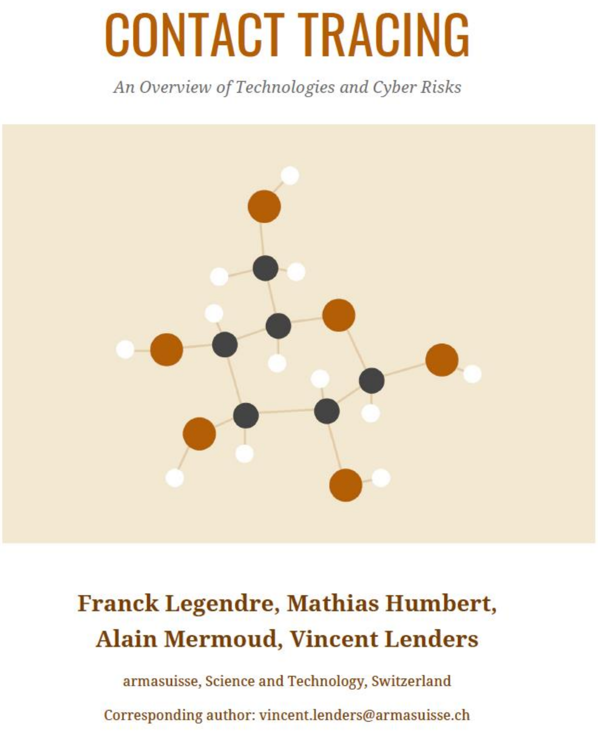


Table of Contents

Source:
https://my.visme.co/view/pv64g6pe-g1d5kovd3xv026m7

Scientific Publications



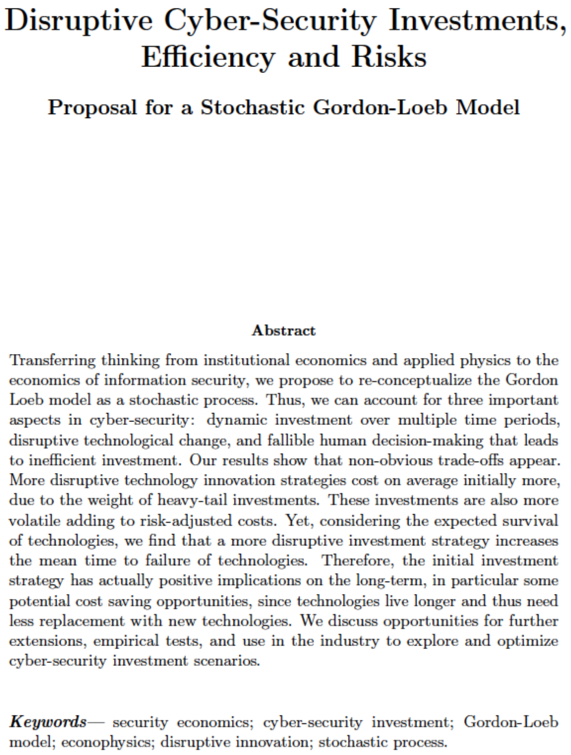
CONTACT TRACING

An Overview of Technologies and Cyber Risks

Franck Legendre, Mathias Humbert, Alain Mermoud, Vincent Lenders

armasuisse, Science and Technology, Switzerland

Corresponding author: vincent.lenders@armasuisse.ch



Disruptive Cyber-Security Investments, Efficiency and Risks

Proposal for a Stochastic Gordon-Loeb Model

Abstract

Transferring thinking from institutional economics and applied physics to the economics of information security, we propose to re-conceptualize the Gordon Loeb model as a stochastic process. Thus, we can account for three important aspects in cyber-security: dynamic investment over multiple time periods, disruptive technological change, and fallible human decision-making that leads to inefficient investment. Our results show that non-obvious trade-offs appear. More disruptive technology innovation strategies cost on average initially more, due to the weight of heavy-tail investments. These investments are also more volatile adding to risk-adjusted costs. Yet, considering the expected survival of technologies, we find that a more disruptive investment strategy increases the mean time to failure of technologies. Therefore, the initial investment strategy has actually positive implications on the long-term, in particular some potential cost saving opportunities, since technologies live longer and thus need less replacement with new technologies. We discuss opportunities for further extensions, empirical tests, and use in the industry to explore and optimize cyber-security investment scenarios.

Keywords— security economics; cyber-security investment; Gordon-Loeb model; econophysics; disruptive innovation; stochastic process.

Developing a Quantitative Risk-Adjusted Technology-Monitoring Indicator

Using Sentiment Analysis as a Risk Proxy for Cyber-Security Technologies

Percia David Dimitri[2,3]; Gillard Sébastien[1]; Mermoud Alain[2]; Maillart Thomas[3]; Keupp Marcus[1,4]; Maréchal Loïc[5]

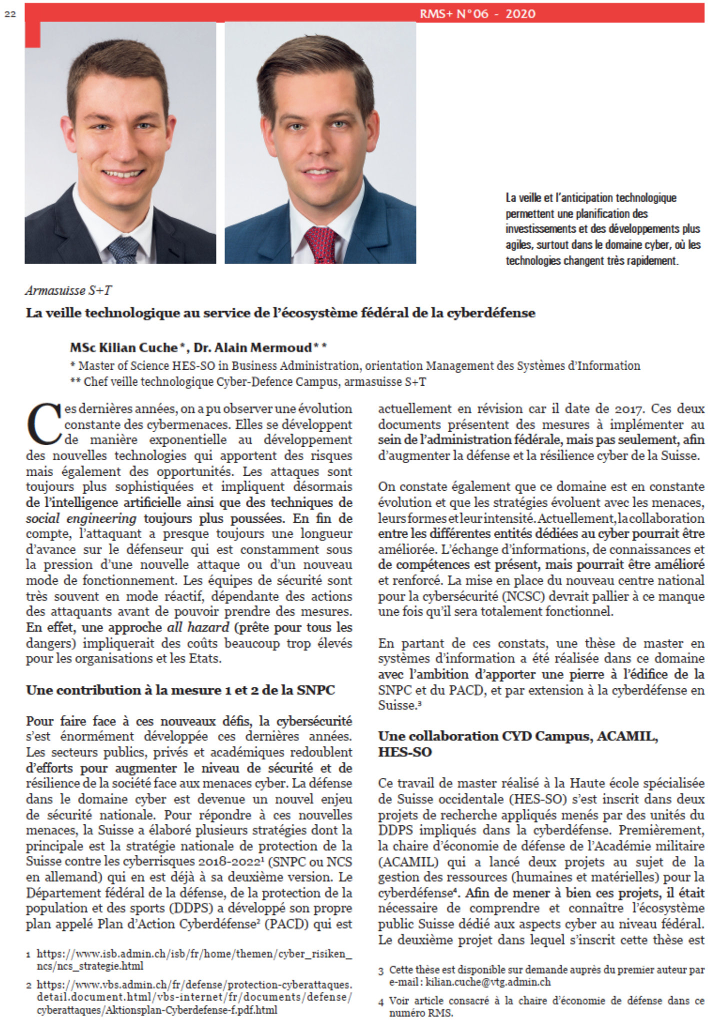
[1] ETH Zurich, Military Academy, Department of Defense Economics
[2] EPFL Cyber-Defence Campus, armasuisse Science and Technology
[3] University of Geneva, Geneva School of Economics and Management, Information Science Institute
[4] University of St. Gallen, School of Management, Institute of Technology Management
[5] University of Neuchatel, Faculty of Economics

Abstract

Technology monitoring is a central activity for developing a cyber-security capability as it helps organizations in anticipating cyber-threats and in assessing security products. However, extant technology-monitoring indicators are: (i) almost exclusively qualitative, (ii) barely scalable, (iii) lacking of scientific and measurement rigor, and (iv) not risk adjusted. In this work, we develop a scientifically-sound and scalable quantitative risk-adjusted technology-monitoring indicator and we apply it to cyber-security technologies. Our indicator aims to capture the risk-adjusted attention that a given community is giving to a specific technology. We build our technology-monitoring indicator by scrapping 1'820'561 scientific articles from the arXiv repository related to seven key security-related technologies, and then we adjust the indicator against a risk proxy captured by sentiment analysis (NLP). Our empirical measurements show that: (i) a specific technology-monitoring indicator is idiosyncratic, rather than following a common *hype cycle* pattern, (ii) security concerns systematically arrive at a later stage of technology development – an empirical evidence of the lack of *security by design*; and (iii) some broad attention – such as the blockchain hype – show very few use-cases in cyber-defence. To the best of our knowledge, our indicator offers the first quantitative assessment allowing the assessment and ranking of cybersecurity technologies.

Keywords— technology management, technometrics; technology forecasting; techwatch; hype cycle; technology lifecycle; NLP; sentiment analysis; security economics.

TMM Research Dissemination



22 RMS+ N°06 - 2020

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

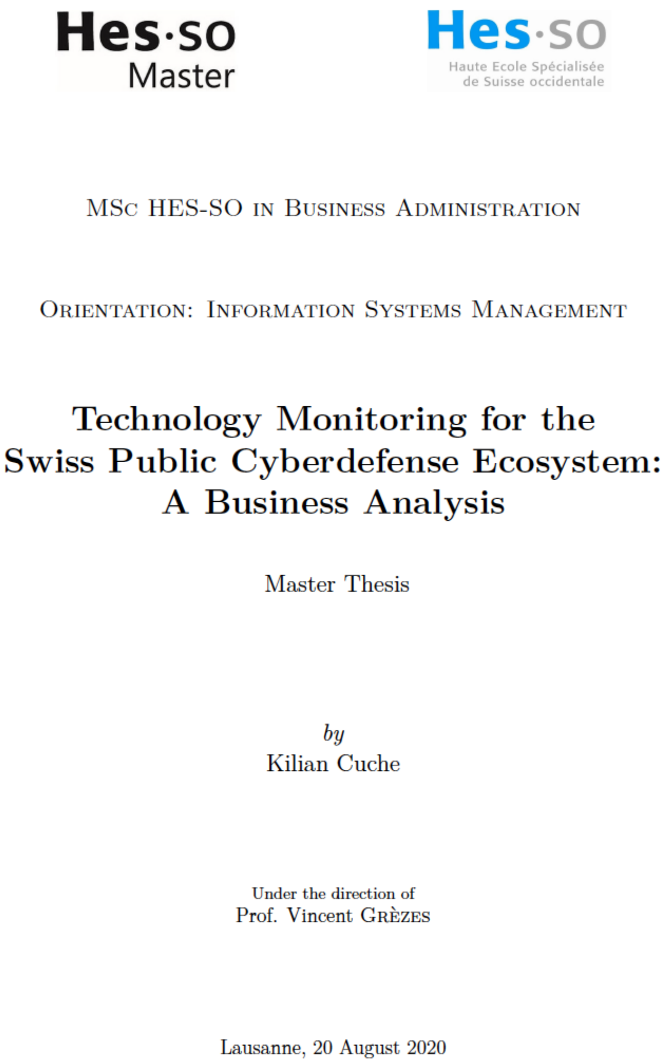
Ce travail de master réalisé à la Haute école spécialisée de Suisse occidentale (HES-SO) s'est inscrit dans deux projets de recherche appliqués menés par des unités du DDPS impliqués dans la cyberdéfense. Premièrement, la chaire d'économie de défense de l'Académie militaire (ACAMIL) qui a lancé deux 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.



Hes·so Master

Hes·so Haute Ecole Spécialisée de Suisse occidentale

MSc HES-SO in Business Administration

Orientation: Information Systems Management

Technology Monitoring for the Swiss Public Cyberdefense Ecosystem: A Business Analysis

Master Thesis

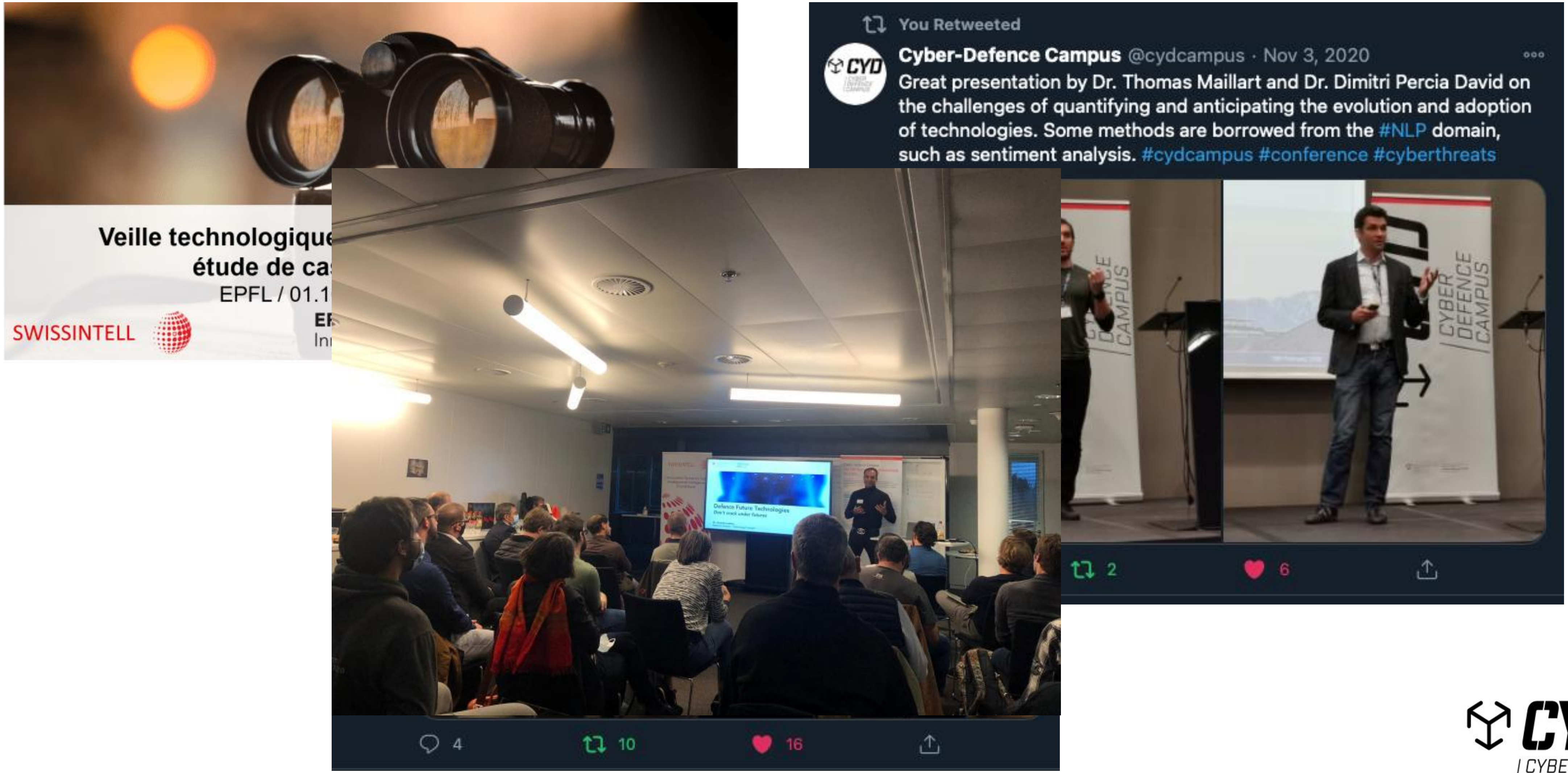
by
Kilian Cuche

Under the direction of
Prof. Vincent Grèzes

Lausanne, 20 August 2020

CYD CYBER DEFENCE CAMPUS

TMM Community Building with Swissintell



Veille technologique
étude de ca
EPFL / 01.1

SWISSINTELL

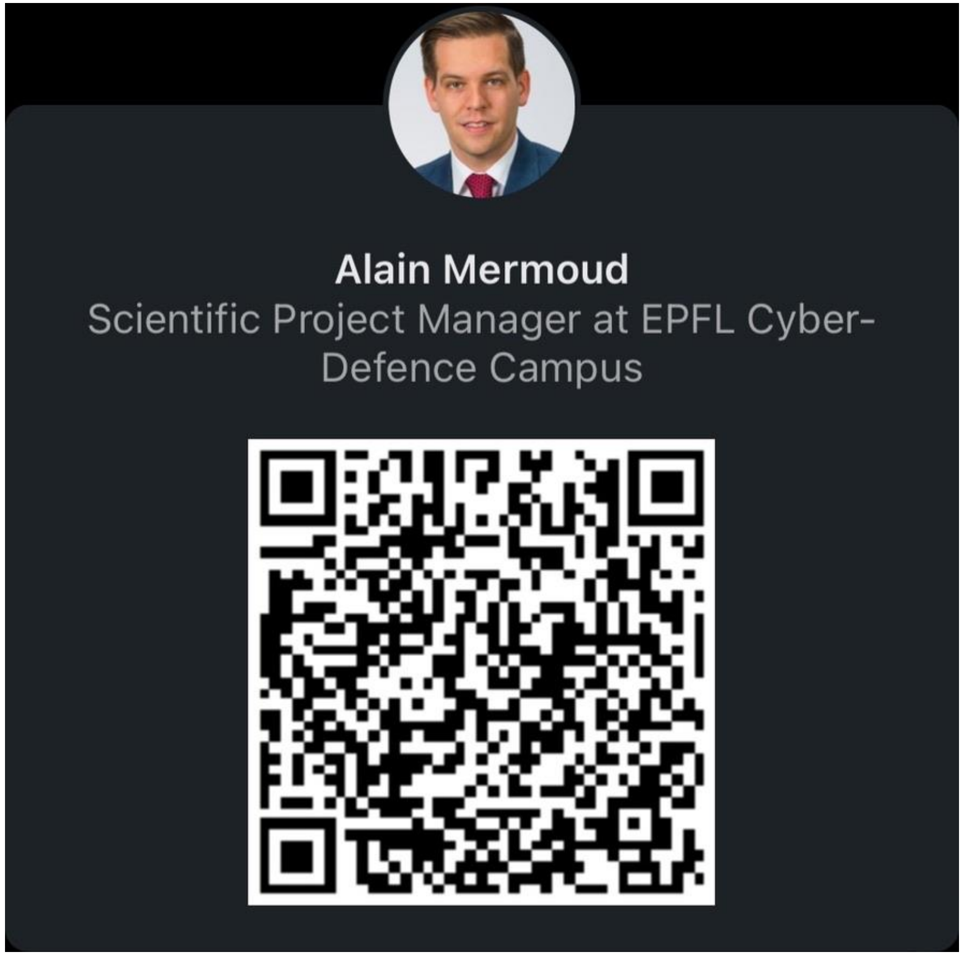
EF
In

You Retweeted

Cyber-Defence Campus @cydcampus · Nov 3, 2020

Great presentation by Dr. Thomas Maillart and Dr. Dimitri Percia David on the challenges of quantifying and anticipating the evolution and adoption of technologies. Some methods are borrowed from the #NLP domain, such as sentiment analysis. #cydcampus #conference #cyberthreats

Let's keep in touch!



Alain Mermoud

Scientific Project Manager at EPFL Cyber-Defence Campus

Twitter: @alainmermoud

LinkedIn: alain-mermoud.ch

References

- BABOK Guide - IIBA | International Institute of Business Analysis". www.iiba.org. Retrieved 2015-10-20.
- Fletcher, A.; Guthrie, J.; Steane, P.; et al. (2003). "Mapping stakeholder perceptions for a third sector organization". *Journal of Intellectual Capital*. 4 (4): 505–27.
- Humphrey, Albert (December 2005). "SWOT Analysis for Management Consulting" (PDF). *SRI Alumni Newsletter*. SRI International.
- Porter, Michael (January 1, 2008). "The Five Competitive Forces That Shape Strategy". *Harvard Business Review.*