La chaire d'économie militaire de l'ACAMIL se tourne ver la cyberdéfense

Autor(en): **Cuche, Kilian**

Objekttyp: **Article**

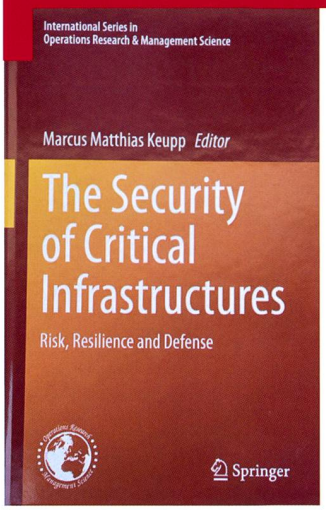
Zeitschrift: **Revue Militaire Suisse**

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

Heft 6

PDF erstellt am: **26.06.2024**

Persistenter Link: https://doi.org/10.5169/seals-913942



Le dernier livre édité par la chaire d'économie militaire publié chez Springer est consacré à la protection des infrastructures critiques de manière globale avec une approche scientifique.

Economie de défense

La chaire d'économie militaire de l'ACAMIL se tourne vers la cyberdéfense

MSc Kilian Cuche
Collaborateur de projet cyberdéfense à la chaire d'économie militaire de l'ACAMIL à l'EPF de Zurich.

La chaire d'économie militaire de l'ACAMIL à l'EPF de Zurich, sous la direction du professeur Marcus Keupp, étoffe son *portfolio* de recherche avec des thématiques liées à la cyberdéfense, à la guerre économique et à la protection des infrastructures critiques. En effet, au vu de l'augmentation des menaces hybrides, il est devenu primordial d'axer également la recherche en économie de défense sur ces thématiques afin de contribuer à la résilience des forces armées. Ces nouvelles recherches permettent d'apporter une vue économique et managériale sur des thématiques souvent abordées uniquement dans leur aspect technique. Nos homologues français produisent également des recherches économiques sur ces thématiques, notamment au sujet de l'industrie et l'innovation de défense comme présenté dans une publication récente de la *Revue Défense Nationale* (RDN).[1]

Méthodiquement, la chaire est tout d'abord focalisée sur l'économie institutionnelle ainsi que l'analyse économique des prescriptions légales et des règlements. Elle analyse l'organisation militaire d'un point de vue institutionnel afin d'examiner les possibilités et les limites de l'action économique au sein de ces organisations. Des analyses économiques et de gestion permettent de rattacher les problématiques économiques militaires à des aspects institutionnels et de performance. Ces dernières aboutissent dans des recommandations en matière de conception institutionnelle pour la pratique organisationnelle des organisations militaires.

La chaire se concentre aussi sur la recherche qui contribue à améliorer la sécurité de l'Etat et de la société. Elle analyse les techniques de la guerre économique moderne[2] ainsi que la gestion stratégique des technologies et de l'innovation. La résilience des infrastructures critiques est également évaluée par la simulation et l'analyse quantitative. De plus, deux recherches ont été menées dans le domaine de l'économie de la cybersécurité. L'analyse de ces différents domaines révèle des vulnérabilités stratégiques et contribue ainsi au développement des stratégies de défense contre les attaques hybrides. Finalement, des nouvelles publications ainsi que deux projets de recherches dans le domaine de la cyberdéfense sont en cours.

Economie militaire

Deux ouvrages phares ont été publiés par la chaire dans le domaine de l'économie de défense. Le premier concerne le passage stratégique de la Route de la Mer du Nord (publié en 2015 chez Springer[3]). Ce livre aborde les défis stratégiques, économiques, logistiques, judiciaires et militaires du futur grand jeu politico-stratégique dans la mer arctique. En effet, le changement climatique mondial a ouvert une nouvelle route maritime en Mer du Nord qui se propose comme une alternative stratégique à la route de Suez. Ajoutez à cela la découverte de nombreux produits de base et métaux facilement extractibles dans la région arctique et vous obtenez une attention toute particulière de la part des dirigeants d'entreprises et des leaders militaires sur cette nouvelle route maritime.

Le deuxième, Economie Militaire (publié en 2019 chez Springer[4]), était purement consacré à l'analyse institutionnelle de l'organisation militaire. Cet ouvrage analyse les problématiques d'efficacité et d'efficience des forces armées organisée dans une économie planifiée et propose des solutions afin d'améliorer la performance économique de l'organisation militaire par l'introduction d'une décentralisation des droits de propriétés au niveau des unités.

1 Rademacher, Benoît (dir.) et Malizard, Julien (dir.), 2020. Economie de défense : problématiques contemporaines. Revue Défense Nationale, 832.

2 https://www.vtg.admin.ch/de/organisation/kdo-ausb/hka/milak.detail.news.html/vtg-internet/verwaltung/2016/16-09/16-09-10-milak.html

3 https://www.springer.com/gp/book/9783658040802

4 https://www.springer.com/gp/book/9783658252878

Economie de la cybersécurité

Deux thèses de doctorat en systèmes d'information réalisée à HEC Lausanne ont débuté la réorientation stratégique de la chaire dans le domaine de la cyberdéfense. Ces travaux se concentrent sur les problématiques économiques de la cybersécurité. La première, réalisée par le Dr. Alain Mermoud porte sur l'économie comportementale appliquée à la sécurité des systèmes d'information.[5] Elle s'intéresse plus particulièrement au mécanisme incitatif permettant de favoriser le partage de l'information utile à la cybersécurité entre opérateurs d'infrastructures critiques. Cette thèse contient trois articles. Le premier présente un cadre théorique qui associe le comportement humain et les résultats du partage d'information. Le deuxième article développe et teste empiriquement ce modèle théorique. Le dernier article propose des recommandations politiques afin de réduire les coûts d'exécution du partage d'information cyber.

La deuxième thèse, réalisée par le Dr. Dimitri Percia David aborde l'économie et l'acquisition des ressources pour générer des capacités de cyberdéfense.[6] Elle est également réalisée en trois articles. Le premier est consacré aux ressources matérielles et démontre que les évolutions rapides dans le domaine technologique exigent de nouvelles hypothèses de modèle d'investissement. Cet article propose un modèle pour aider à anticiper l'effet des technologies de rupture sur le niveau optimal d'investissement en cyberdéfense. Il fournit également un cadre pour sélectionner et investir dans les technologies les plus efficaces. Le second est consacré aux ressources humaines et démontre qu'une organisation doit mettre l'accent sur le recrutement de fournisseurs de connaissances spécialisées afin de construire une capacité de cyberdéfense. Le dernier article est consacré aux ressources de connaissances et démontre que l'organisation doit encourager l'apprentissage continu de ses membres afin de construire une capacité de cyberdéfense efficace. Finalement, cette thèse propose des recommandations stratégiques à l'intention du gouvernement et des fournisseurs d'infrastructures critiques.

Sécurité des infrastructures critiques

La chaire d'économie de défense a également chapeauté la publication d'un livre consacré à la sécurité des infrastructures critiques publié en 2020 chez Springer Nature.[7] Ce livre analyse la sécurité des infrastructures critiques comme les réseaux routiers, ferroviaires, d'eau, de santé et d'électricité qui sont vitaux pour la société et l'économie d'une nation. Il évalue la résilience de ces réseaux face aux attaques intentionnelles. Des experts en recherche et gestion des opérations, en économie, en analyse des risques et en gestion de la défense ont contribué à ce livre en présentant des analyses théoriques, des graphiques, des statistiques avancées ainsi que des méthodes de modélisation appliquées. Finalement, ce livre identifie et discute des implications pour l'évaluation des risques, la politique et l'assurabilité des infrastructures critiques. Les conclusions présentées dans cet ouvrage sont applicables à l'échelle mondiale et ne se limitent pas à des lieux, des pays ou des contextes particuliers.

De plus, Sébastien Gillard, qui a également contribué à ce livre avec deux chapitres poursuit sa recherche dans ce domaine. Actuellement, il apporte sa contribution à un projet orienté sur la protection des infrastructures critiques et l'investissement dans la sécurité de l'information, en partenariat avec le Cyber-Defence Campus d'armasuisse basé à l'EPFL. En parallèle, il prépare une autre recherche pour sa thèse de doctorat consacrée à l'optimisation de la *Cyber Threat Intelligence (CTI)* au moyen de méthodes éconophysiques.[8]

Social Engineering

D'autres travaux dans le domaine de la cyberdéfense sont en cours d'élaboration. Une nouvelle thèse consacrée aux problématiques de *social engineering* (pratique de manipulation psychologique à des fins d'escroquerie en ligne) est également en cours de rédaction par Fabian Muhly en partenariat avec le département de criminologie de l'Université de Lausanne. Cette recherche vise à valider un instrument pour être plus à même de combattre les délits associés aux techniques de *social engineering*. Ce travail utilise le *Serious Gaming* comme un outil pour diminuer le risque d'être victime en sensibilisant les gens à propos des menaces de façon innovante et ludique. Cette recherche analyse la relation entre les facteurs individuels/situationnels et les perceptions d'être victime de *social engineering* au moyen d'un questionnaire. Le but final de cette recherche est d'obtenir un instrument efficace pour combattre les risques liés au *social engineering* en utilisant une méthode de sensibilisation par le *Serious Gaming* qui respecte les différences individuelles des participants.

Management de la cyberdéfense

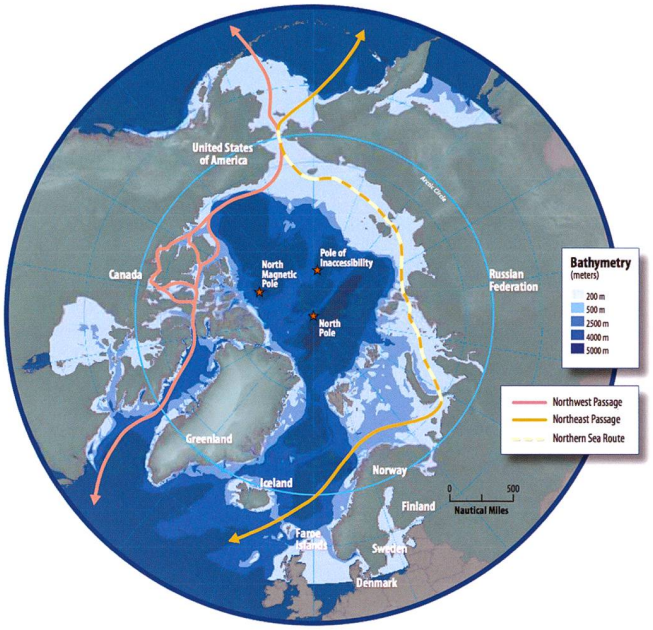
Deux projets de recherche consacrés au management de la cyberdéfense ont démarrés au début de l'année et devraient se terminer en 2023 par la publication d'un livre dédié à cette thématique. Comme dans les conflits conventionnels, l'armée doit d'abord être capable de se défendre dans le cyberespace avant de pouvoir remplir sa mission de défense nationale, de la population et des infrastructures critiques. La génération de cyber capacités, qui, à l'instar des services de renseignement, sont largement utilisées en temps de paix, diffère sensiblement de la génération de capacités militaires conventionnelles. Un problème de base commun, cependant, est que la puissance réelle requise est inconnue jusqu'à ce qu'un événement réel se produise. De plus, l'allocation de ressources financières ne suffit pas à elle seule à générer des prestations militaires.

5 https://serval.unil.ch/fr/notice/serval:BIB_5D54879D8F67

6 https://serval.unil.ch/fr/notice/serval:BIB_8A0DAC472C8F

7 https://www.springer.com/gp/book/9783030418250

8 L'éconophysique est un domaine de recherche scientifique qui propose de résoudre des problèmes économiques en appliquant des méthodes et des théories venant du domaine de la physique.



Carte de la région arctique montrant la route maritime du Nord, dans le contexte du passage du Nord-Est, et du passage du Nord-Ouest.

Le premier projet, chapeauté par Kilian Cuche, s'intéresse au management des ressources humaines pour la cyberdéfense et s'articule en trois parties. La première a pour but d'analyser les différents écosystèmes suisses impliqués dans la cyberdéfense (public, privé, et académique). La deuxième partie du projet s'intéresse aux capacités cyber et aura pour but de trouver des améliorations dans le transfert de connaissances et de compétences cyber entre ces trois écosystèmes. Finalement, la dernière partie sera consacrée à l'attractivité du secteur public, principalement l'armée, comme employeur cyber et aura pour but de donner des pistes pour améliorer le recrutement et la rétention du personnel dans le domaine cyber.

Le deuxième projet, réalisé par David Baschung, se penche sur les problématiques de gestion des ressources matérielles pour la cyberdéfense. Ce projet examine le processus global en ce qui concerne l'efficacité des capacités cyber de l'armée suisse. En effet, il ne suffit pas d'essayer uniquement d'optimiser le processus d'achat en termes de ressources matérielles cybernétiques, mais il faut plutôt avoir une vue globale du cycle, en commençant par la surveillance technologique, en passant par la planification des capacités, jusqu'à leur introduction dans le paysage des systèmes de production respectifs.

L'impact des politiques économiques sur la sécurité

Les futurs travaux s'orienteront naturellement vers les thématiques liées à l'économie de la cyberdéfense mais aussi à des sujets purement d'ordre de l'économie militaire afin de continuer dans le domaine de recherche historique de la chaire. Par exemple, le prochain livre envisagé aura pour thématique les différents modèles de politiques économiques et leurs impacts sur la sécurité. Il permettra une comparaison des modèles totalement autarciques ou isolationnistes avec des modèles totalement mondialisés ou libertaires et analysera leurs conséquences sur la sécurité. Finalement, il tirera des conclusions sur ces modèles de politiques économiques et démontrera leurs avantages et inconvénients.

K. C.

L'ACAMIL est un centre de compétences pour les sciences militaires reconnu en Suisse comme à l'étranger. Le centre mène des recherches et propose des enseignements au sein des départments suivants :
- Conduite et communication ;
- Histoire militaire ;
- Economie militaire ;
- Psychologie militaire et pédagogie militaire ;
- Sociologie militaire ;
- Etudes stratégiques.

Sélection bibliographique de la chaire d'économie militaire

Keupp, MM. (2015) *The Northern Sea Route*: A Comprehensive Analysis. Wiesbaden: Springer Gabler. ISBN 978-3-658-04081-9

Keupp, MM. (2017) *Der moderne Wirtschaftskrieg - Herausforderungen und Strategien*: MILAK-Herbsttagung vom 10. September 2016. Militärakademie an der ETH Zürich Schriftenreihe. MILAK Schrift Nr. 17

Keupp, MM. (2019) *Economie Militaire*. Wiesbaden: Springer Gabler. ISBN 978-3-658-25287-8

Mermoud, A. (2019) *Three Articles on the Behavioural Economics of Security Information Sharing*: A Theoretical Framework, an Empirical Test, and Policy Recommendations. PhD Thesis. Université de Lausanne. Faculté des hautes études commerciales (HEC)

Percia David, D. (2020) *Three Articles on the Economics of Information-Systems Defense Capability*: Material-, Human-, and Knowledge-Resources Acquisition for Critical Infrastructures. PhD Thesis. Université de Lausanne. Faculté des hautes études commerciales (HEC)

Cuche, K. (2019) Guerre de l'information et politique: quelles conséquences pour la sécurité de la Suisse ? *Revue Militaire Suisse*, numéro 6, 2019.

Keupp, MM. (2020) *The Security of Critical Infrastructures: Risk, Resilience and Defense*. International Series in Operations Research & Management Science, Cham: Springer Nature. ISBN 978-3-030 41826-7