Canvas pour le développement d'une capacité de cyberdéfense

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

Objekttyp: **Article**

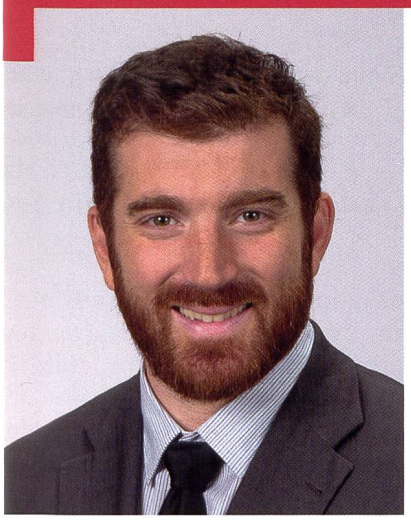
Zeitschrift: **Revue Militaire Suisse**

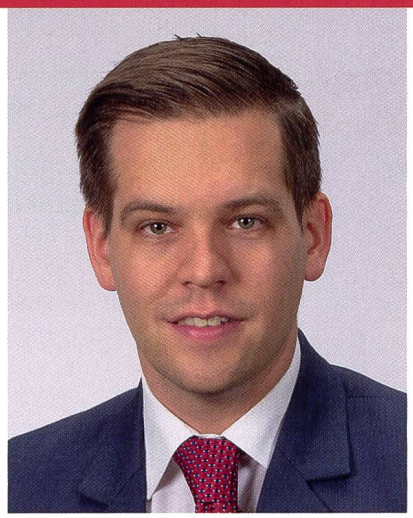
Band (Jahr): **- (2019)**

Heft 6

PDF erstellt am: **14.09.2024**

Persistenter Link: https://doi.org/10.5169/seals-977464





Un *Business Model Canvas* est un modèle de gestion stratégique, présenté sous la forme d'un *roadmap*. Un *canvas* est un guide pour les décideurs afin d'atteindre les buts fixés au préalable par l'organisation. Il s'agit d'un graphique visuel comportant des éléments-clés nécessaires à l'atteinte d'un objectif. Un tel *canvas* aide les organisations à procéder selon une systématique, définissant ainsi un *business model* adéquat.

Intelligence économique

Canvas pour le développement d'une capacité de cyberdéfense

Cap Dimitri Percia David*, cap Alain Mermoud**

* Doctorant en systèmes d'information à HEC Lausanne et collaborateur scientifique à l'ACAMIL à l'EPF de Zurich

** Docteur ès Sciences en systèmes d'information

Nous faisons suite à notre article « *produire du renseignement grâce au partage d'information* » publié dans la RMS N°6 / 2018.[1] En prenant davantage de recul stratégique, cet article vise à synthétiser les prérequis nécessaires à la création d'une capacité de cyberdéfense. Les considérations présentées dans cet article constituent les conclusions de la thèse de doctorat du premier auteur – recherche entreprise au sein de la chaire Economie de Défense de l'Académie militaire (ACAMIL) à l'EPF de Zurich, en partenariat avec le Département des Systèmes d'information de l'Université de Lausanne.

L'interdépendance engendre un risque (cyber)-systémique

Les besoins en ressources matérielles, ressources humaines et ressources de savoir nécessaires au développement d'une capacité de défense des systèmes d'information sont essentielles pour les fournisseurs d'infrastructures critiques. La continuité opérationnelle de ces dernières est vitale pour le fonctionnement des sociétés modernes. Or, ces infrastructures forment un écosystème interdépendant soumis au risque systémique de défaillances en cascade. Dans un tel contexte de risques extrêmes, aucun (re-)assureur - privé ou public - n'est capable de couvrir de telles défaillances. En conséquence, les fournisseurs d'infrastructures critiques sont contraints d'assurer eux-mêmes leur continuité opérationnelle face a de tels risques, qu'ils soient dus a des attaques délibérées ou a des catastrophes naturelles.

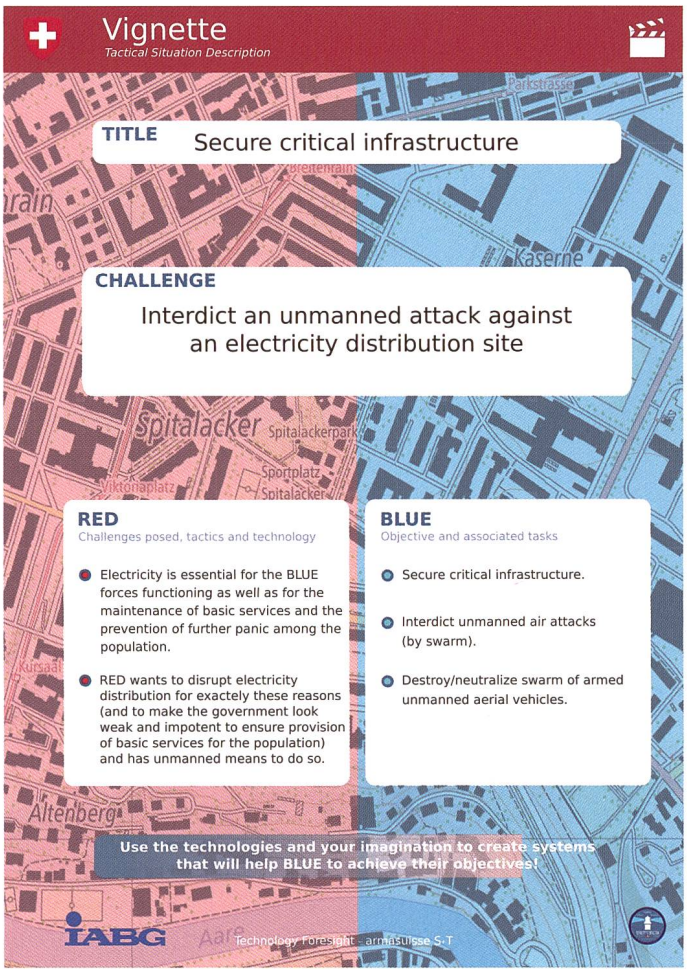
Développer une capacité de défense

Les systèmes d'information déterminent un tel écosystème interdépendant puisqu'ils constituent l'architecture interconnectée utilisée pour surveiller et gérer les infrastructures critiques. Ainsi, la continuité opérationnelle des systèmes d'information constitue un objectif crucial nécessitant une capacité de défense, c'est-à-dire la capacité d'anticiper et/ou de minimiser l'impact des incidents liés au risque d'un cyber-systémique. Afin d'assurer une telle capacité, les recherches en sécurité informatique (*computer & information security*) ont développé un ensemble de solutions techniques. Cependant, plusieurs universitaires et praticiens ont mis en exergue le fait que les solutions techniques adoptées pour résoudre les problèmes de défense des systèmes d'information sont nécessaires mais insuffisantes. Les incidents sont causés par une conception organisationnelle et/ou un comportement humain inappropriés, au moins aussi souvent que par une conception informatique inefficace.

Une approche socio-technique

Dans cette logique, les systèmes d'information sont appréhendés comme des systèmes socio-techniques constitués d'un ensemble de technologies (ressources matérielles) et d'agents humains (ressources humaines et ressources de savoir) qui utilisent ces mêmes technologies. En nous appuyant sur des recherches antérieures basées sur les compétences organisationnelles (*organizational capabilities*) et de l'économie de la sécurité informatique (*security economics*), nous explorons les aspects de la conception organisationnelle et du comportement humain nécessaires aux fournisseurs d'infrastructures critiques afin de construire une telle capacité de défense des systèmes d'informations. Cette capacité se décompose en ressources matérielles, humaines et de savoir, en explorant comment ces dernières devraient être développées pour construire une telle capacité.» par « nécessaires aux fournisseurs d'infrastructures critiques afin de construire une telle capacité de défense de leurs systèmes d'informations. Cette capacité se décompose en ressources matérielles, humaines et de savoir. En explorant comment ces dernières devraient

1 Mermoud, Alain & Percia David, Dimitri. *Produire du renseignement grâce au partage d'information*, in Revue Militaire Suisse (RMS+), No 6, 2018.



Sous la direction du Dr. Quentin Ladetto, armasuisse a récemment développé divers *canvas* et méthodologies pour la conduite de workshops créatifs. Ci-dessus un exemple avec un canvas développé pour la sécurité des infrastructures critiques. Source : https://deftech.ch/canvas/ (consulté le 14.09.19)

être développées pour construire une telle capacité, les auteurs proposent de développer un canvas pour la cyberdéfense.

Développer un *canvas* de cyberdéfense pour les forces armée

En économie de gestion, la matrice d'affaires (*business model canvas*) est une représentation des facettes essentielles d'une entreprise ou d'un nouveau produit.

Le plus célèbre est celui du Prof Yves Pigneur et du Dr. Alexander Osterwaler, développé à l'UNIL.[2] Notre idée consiste à adapter ce canvas au domaine de la cybersécurité, afin de favoriser le développement d'une capacité de cyberdéfense.

I. Ressources matérielles

Au travers d'une première recherche [1] consacré aux ressources matérielles, nous soutenons que l'évolution rapide du domaine technologique exige de nouvelles hypothèses de modèle d'investissement. Nous adoptons donc le fameux modèle de Gordon-Loeb pour que ce dernier puisse intégrer les développements dynamiques et discontinus du domaine technologique. Ce modèle économique de référence permet d'analyser le niveau d'investissement optimal en sécurité de l'information. Les résultats permettent d'aider les fournisseurs d'infrastructures critiques à anticiper l'impact des technologies de ruptures (*disruptive technologies*) sur l'efficacité des investissements de défense pour les systèmes d'information.

II. Ressources humaines

Dans une deuxième recherche [2] consacrée aux ressources humaines, nous soutenons qu'une organisation doit mettre l'accent sur le recrutement de

2 Osterwalder, Alexander & Pigneur, Yves. *Business model generation: a handbook for visionaries, game changers, and challengers*. John Wiley & Sons, 2010.

Ce nouveau *canvas* synthétise les résultats de la thèse de doctorat de Dimitri Percia David. La création d'une capacité de cyberdéfense avec une approche économique permet d'optimiser l'allocation des ressources et donc l'efficience et l'efficacité de la cyberdéfense d'une organisation [4].

Canvas pour la création d'une capacité de cyberdéfense

	Optimiser l'allocation des ressources nécessaires à la création d'une capacité de cyberdéfense		
Ressources	Matérielles (technologies)	Humaines (spécialistes)	Savoir (connaissances)
Transaction	Investissement	Recrutement	Transmission
Objectif	Sélectionner les technologies les plus effectives et ajuster l'investissement	Attirer les spécialistes (informaticiens et gestionnaires)	Absorber le savoir tacite aux travers des plateformes de transmission (ex. *Information Sharing and Analysis Center*)
Marche-à-suivre	1. Évaluer le montant à protéger 2. Évaluer la probabilité d'une fuite 3. Évaluer la perte attendue (1+2) 4. Sélectionner les technologies 5. Investir au niveau optimal	1. Évaluer le coût d'opportunité lié aux choix de carrière 2. Comparer ce coût avec celui des concurrents 3. Adapter le design organisationnel en fonction de (2)	1. Réduire au maximum les coûts de transaction liés au partage d'information 2. Aligner les incitations entre l'organisation et les employés

spécialistes pour construire une capacité de défense de ses systèmes d'information. Nous proposons alors une approche économique basée sur une analyse des coûts d'opportunité pour attirer de nouveaux employés dans le contexte de l'armée suisse, une infrastructure critique souffrant d'un déficit de personnel afin de surveiller et gérer leurs systèmes d'information.

III. Ressources de savoir

Dans une troisième recherche [3] consacrée aux ressources de savoir, nous soutenons qu'une organisation doit encourager l'apprentissage continu des membres actuels de l'organisation pour construire une capacité de défense des systèmes d'information. Prenant le cas du partage d'information (*cyber-risk / information sharing*) – un moyen de favoriser le partage des connaissances afin de construire une capacité de défense des systèmes d'information –, nous étudions les raisons pour lesquelles les individus s'engagent dans le partage d'information en se concentrant sur l'absorption des connaissances d'une telle activité. Nos résultats indiquent que la mesure dans laquelle un individu s'implique dans le partage des connaissances est fonction de ses attentes individuelles en matière d'absorption des connaissances, c'est-à-dire de l'avantage net qu'elle/il s'attend à tirer du partage d'information.

Applications sécuritaires concrètes

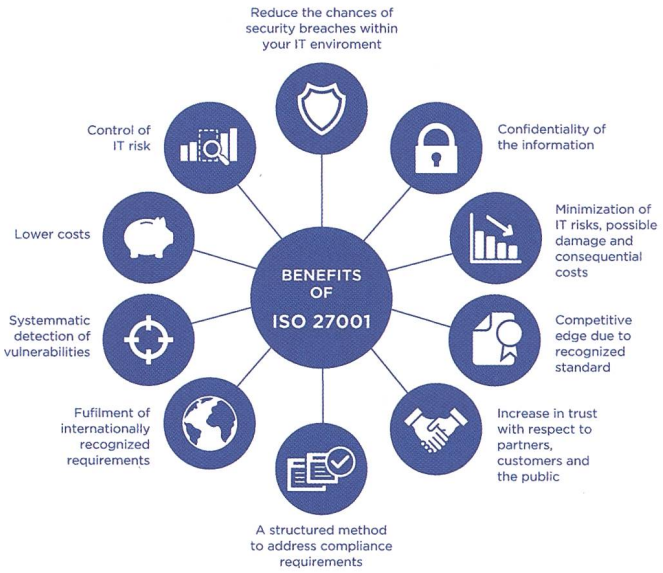
Pour les praticiens, ce *canvas* est également utile à la construction de *benchmark,* comme le *Global Cybersecurity Index* (GCI)[3] développé par l'Union Internationale des Communications (UIC). Cet indice mesure l'engagement des pays à l'égard de la cybersécurité à l'échelle mondiale, afin de les sensibiliser à l'importance et aux différentes dimensions du problème. Etant donné que la cybersécurité a un vaste champ d'application, englobant de nombreux secteurs et industries, le niveau de développement ou d'engagement de chaque pays est évalué selon cinq piliers (similaire à notre *canvas*) avant d'être agrégé en un score global: 1) Mesures juridiques, 2) Mesures techniques, 3) Mesures organisationnelles, 4) Renforcement des capacités, et 5) Coopération. A noter que la Suisse se classe à la 37ème place mondiale en 2018.

Des recommandations stratégiques à l'intention du gouvernement et des fournisseurs d'infrastructures critiques, ainsi qu'un agenda de recherche pour des travaux futurs sont présentés dans la conclusion de la thèse. Celle-ci sera téléchargeable d'ici quelques semaines sur SERVAL, le serveur institutionnel académique de l'UNIL.[4] Pour apporter une réelle plus-value au développement d'une capacité de cyberdéfense, ce canvas doit encore être amélioré au travers d'un processus itératif incluant une collaboration répétée entre praticiens et chercheurs. Ce canvas sera alors utile non seulement pour les forces armées, mais également pour toute organisation souhaitant développer une capacité de cyberdéfense.

D. P.D., A. M.

3 https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx (consulté le 21.08.19)

4 https://serval.unil.ch/ (consulté le 21.08.19)



Les *canvas* permettent également de développer des normes pour standardiser la sécurité de l'information. La suite ISO/CEI 27000 comprend par exemple les normes de sécurité de l'information publiées conjointement par l'Organisation internationale de normalisation (ISO) et la Commission électrotechnique internationale (CEI). La suite contient des recommandations des meilleures pratiques en management de la sécurité de l'information, pour l'initialisation, l'implémentation ou le maintien de systèmes de management de la sécurité de l'information (SMSI).

Bibliographie

[1] Dimitri Percia David, Marcus Keupp, Solange Ghernaouti, Alain Mermoud. *Cyber Security Investment in the Context of Disruptive Technologies: Extension of the Gordon-Loeb Model and Application to Critical Infrastructure Protection.* In Proceedings of the International Conference on Critical Information Infrastructures Security (CRITIS), Paris, 2016.

[2] Dimitri Percia David, Marcus Keupp, Ricardo Marino, Patrick Hofstetter. *The Persistent Deficit of Militia Officers in the Swiss Armed Forces: An Opportunity Cost Explanation. Defence and Peace Economics*, vol. 30, 2017.

[3] Dimitri Percia David, Marcus Keupp, Alain Mermoud. *Knowledge Absorption for Cyber-Security: The Role of Human Belief and Behavior.* In Journal of Computers in Human Behavior, 2019.

[4] Alain Mermoud, Marcus Keupp, Kévin Huguenin, Maximilian Palmié, Dimitri Percia David. *To share or not to share: A behavioral perspective on human participation in security information sharing.* In Journal of Cybersecurity, Oxford University Press, 2019.

[5] Alain Mermoud, Dimitri Percia David, Marcus Matthias Keup. *Pour une approche économique de la cybersécurité.* Military Power Revue, 36-49, 2017.