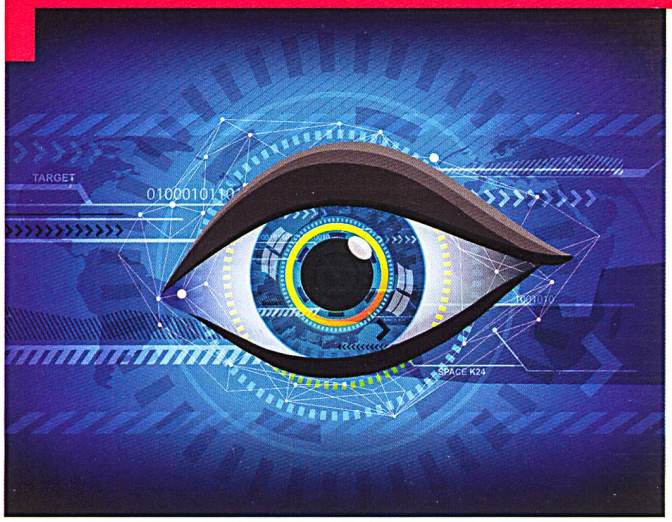
Zeitschrift: Revue Militaire Suisse
Herausgeber: Association de la Revue Militaire Suisse
Band: - (2018)
Heft: 6

Artikel: Produire du renseignement grâce au partage d'information
Autor: Mermoud, Alain / David, Dimitri Percia
DOI: https://doi.org/10.5169/seals-823422



Après l'adoption de la Stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC) 2018-2022, le Conseil fédéral a commencé les travaux concernant l'obligation de déclarer les cyberattaques. L'objectif est de préparer les bases d'ici l'été 2019 afin de pouvoir prendre une décision de principe sur l'introduction d'une déclaration obligatoire.

Renseignement

Produire du renseignement grâce au partage d'information

Cap Alain Mermoud, cap Dimitri Percia David
Doctorants en systèmes d'information à HEC Lausanne et collaborateurs scientifiques à l'ACAMIL à l'EPF de Zurich

Cet article présente les résultats vulgarisés d'une recherche scientifique menée par la chaire Economie de Défense de l'Académie militaire (ACAMIL) à l'EPF de Zurich, en partenariat avec la Centrale d'enregistrement et d'analyse pour la sûreté de l'information (MELANI). Cette recherche empirique constitue le cœur de la thèse de doctorat par articles du premier auteur. Cet article scientifique a été accepté et présenté en juin 2018 au prestigieux *Workshop on the Economics of Information Security* (WEIS). Une extension de cet article évalué par les pairs est en cours de publication dans la revue scientifique de référence *Journal of Cybersecurity*.

Une approche économique de la cybersécurité et du renseignement

Cette recherche part du constat que la cybersécurité ne peut plus se limiter aux seuls aspects techniques de l'informatique. Une approche holistique alliant plusieurs disciplines est nécessaire afin de comprendre et de résoudre l'ensemble des problèmes. En l'espèce, notre démarche consiste à appliquer un cadre théorique issu de l'économie comportementale pour mieux comprendre le rôle du mécanisme incitatif favorisant le partage d'information sur les cybermenaces.

L'échange d'information sur les cybermenaces consiste à partager de l'information pertinente pour la cybersécurité entre agents économiques. Ces informations peuvent porter sur une faille, une vulnérabilité, un maliciel, des techniques de hameçonnage (*phishing*), une fuite de données, etc. Un agent peut également partager de l'information à propos des bonnes pratiques (résolution d'un incident), une compétence particulière, des avis et conseils d'experts, ou encore des renseignements existants.

Produire du *Threat Intelligence* grâce au partage d'information

Le renseignement sur et depuis le cyberespace est la première ligne de défense contre les cyberattaques. Il permet d'anticiper les attaques et de contribuer à l'attribution d'une cyberattaque en identifiant son origine ou son auteur, ou en détectant des tendances sur les méthodes utilisées et les secteurs touchés. Ces exemples illustrent le lien grandissant entre le renseignement et la cybersécurité. Du point de vue du renseignement, le partage d'information sur les cybermenaces permet également de produire du *Cyber Threat Intelligence* (CTI).

La CTI est une discipline basée sur le cycle du renseignement (analyse des besoins, collecte, analyse et diffusion d'information) qui est bien connu des militaires. Elle a pour finalité la production de renseignement lié aux cybermenaces, par exemple dans le but d'alimenter les systèmes de détections précoces ou les CERTs. Dans ce but, la CTI agrège également du renseignement en sources ouvertes (OSINT), en provenance des réseaux sociaux (SOCMINT), ou encore d'origine humaine (HUMINT), sans oublier l'information grise (difficile d'accès) située dans le web profond (*deep web*) ou le web invisible (*dark web*). La CTI se nourrit également du partage d'information entre agences de renseignement et autres acteurs de la sécurité.

Les avantages du partage d'information

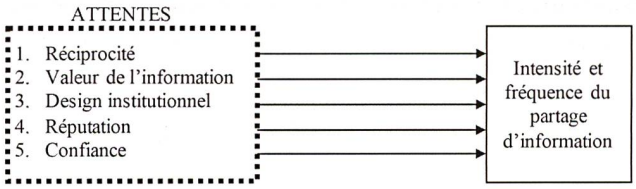
D'un point de vue pratique, le partage d'information permet de produire du renseignement pour assurer le suivi de la situation, et ce faisant d'anticiper et de prévenir les cyberrisques. De l'autre côté de la tranchée, les cybercriminels et autres *black hat hackers* ont une longue tradition du partage d'information pour coordonner des cyberattaques, échanger des expériences ou exploiter l'asymétrie d'information offerte par les vulnérabilités *zero-day*. D'un point de vue économique, le partage d'information sur les cybermenaces a de nombreux avantages. Citons par exemple :

Depuis 1998, les ***Information Sharing and Analysis Centers*** **(ISACs)** organisent le partage d'information (d'une manière centralisée) entre opérateurs d'infrastructures critiques aux USA. Interconnectées de par leur nature systémique, ces infrastructures vitales offrent un contexte particulièrement favorable pour étudier le partage d'informations pertinentes pour produire de la cybersécurité. En général, les ISACs sont des organismes sans but lucratif organisés par secteur d'activité économique. Le *Financial Services Information Sharing and Analysis* (FS-ISAC : https://www.fsisac.com) regroupe par exemple plus de 7'000 membres de l'industrie bancaire. Avec la généralisation des véhicules connectés, l'industrie automobile s'est dotée d'un *Automotive Information Sharing and Analysis Center* (AUTO-ISAC : https://www.automotiveisac.com). En Suisse, la plateforme MELANI-Net organise ce partage d'information depuis 2004 au sein d'un partenariat public-privé (PPP) regroupant les principales infrastructures critiques du pays.

- La réduction d'asymétrie d'information entre l'attaquant et le défenseur ;
- L'abaissement du coût d'investissement optimal en cybersécurité, car le partage d'information est une activité qui demande peu de ressources ;
- La création d'un jeu à somme positive ;
- La prévention de l'effet domino entre infrastructures critiques interconnectées (scénario du type *cyber subprime*) ;
- La création d'*externalités*[1] positives qui augmentent le niveau total de sécurité.

Le problème du passager clandestin : Une lacune scientifique et pratique

Dans cette étude, nous définissons le partage d'information comme une activité humaine affectée par le problème du *passager clandestin*.[2] Dans la pratique, de nombreuses personnes physiques ou morales profitent des bénéfices du partage d'information, mais sans vouloir y participer. La rétention d'information ou le problème du *principal-agent*[3] peuvent expliquer ce comportement humain inadéquat. Cette problématique d'*aléa moral*[4] dans la cybersécurité est reconnue comme une importante lacune dans la littérature scientifique par de nombreux praticiens, le régulateur, l'industrie et le monde académique.



Notre modèle (ci-dessus dans une version vulgarisée) a permis d'identifier cinq variables permettant d'expliquer le mécanisme incitatif du partage d'information. Celui-ci est mesuré avec une approche multidimensionnelle (intensité et fréquence) et régressé sur ces cinq variables, toutes mesurées sur une échelle psychométrique.

Le développement et le test d'un nouveau modèle incitatif Afin de comprendre et de réduire ce problème, la chaire Economie de Défense de l'ACAMIL a développé un modèle incitatif permettant de mieux comprendre ce qui motive les humains à partager de l'information sur les cybermenaces. Ce modèle a été testé empiriquement grâce à notre partenariat avec MELANI, qui a diffusé un questionnaire psychométrique[5] (validé au préalable par un *focus group*) à son cercle fermé regroupant 424 opérateurs d'infrastructures critiques. Grâce au précieux soutien de la direction de MELANI, ce questionnaire en ligne a obtenu un taux de réponse exceptionnel de 63%. Les variables et le modèle ont été validés au préalable par un comité scientifique international en 2016[6] , qui a confirmé que ces cinq « effets » sont des éléments précurseurs au partage d'information.[7]

L'efficience réside dans un *design* institutionnel sain

Nos résultats empiriques[8] soulignent l'importance du comportement (inadéquat) humain dans la cybersécurité. Le *design* institutionnel de l'ISAC est le facteur influençant le plus l'intensité et la fréquence du partage d'information. Pour les institutions organisant le partage d'information, ces résultats permettent d'identifier et de mettre en place les bonnes incitations pour augmenter

1 En sciences économiques, le concept d'*externalité* décrit le fait qu›un agent économique crée, par son activité, un effet externe en procurant à autrui, sans contrepartie monétaire, une utilité ou un avantage de façon gratuite, ou au contraire une nuisance, un dommage sans compensation.

2 Le problème du *passager clandestin* (*free-rider*) désigne le comportement d'un agent qui profite d'un avantage sans y avoir investi autant d'efforts (en argent ou en temps) que les autres agents d'un groupe.

3 La *théorie de l'agence* est une branche de l'économie qui étudie les conséquences du problème *principal-agent*. Ce problème apparaît lorsque l'action d'un acteur économique (le principal) dépend de l'action ou de la nature d'un autre acteur (l'agent) sur lequel le principal est imparfaitement informé.

4 Un aléa moral (*moral hazard*) peut apparaître dans certaines situations à risque lorsqu'un agent se comporte différemment selon son degré d'exposition au risque. L'aléa moral est, par exemple, observable dans le domaine des assurances, lorsqu'un assuré augmente sa prise de risque, par rapport à la situation où il supporterait seul les coûts d'un sinistre.

5 La psychométrie est la science qui étudie l'ensemble des techniques de mesure pratiquées en psychologie, ainsi que les techniques de validation et d'élaboration de ces mesures.

6 Mermoud, A., Keupp M.M., Ghernaouti, S., Percia David, D., 2016. *Using incentives to foster security information sharing and cooperation : a general theory and application to critical infrastructure protection*. The 11th International Conference on Critical Information Infrastructures Security, Paris. http://www. critis2016.org/

7 ENISA technical report (2010). *Incentives and challenges for information sharing in the context of network and information security*. https://www.enisa.europa.eu.

8 Les résultats empiriques complets sont disponibles à l'adresse : https://weis2018.econinfosec.org/wp-content/uploads/sites/5/2018/05/WEIS_2018_paper_7.pdf (consulté le 07.10.2018).

l'intensité et la fréquence du partage d'information. Pour le législateur, l'élaboration d'institutions efficientes pour le partage d'information devrait donc être prioritaire. Sur le plan de l'individu, la *théorie du Nudge* de Richard Thaler (prix Nobel d'économie 2017) a démontré que des suggestions indirectes peuvent, sans forcer, influencer les motivations et la prise de décision des individus vers plus de partage d'information. Sur le plan des institutions, la nouvelle économie institutionnelle offre de nombreuses pistes pour implémenter de « bonnes » règles, permettant d'inciter les individus à adopter de « bons » comportements. Enfin, le partenariat public-privé semble être le modèle de gouvernance préféré parmi la population interrogée pour pratiquer cette activité. Notre dernier article scientifique détaille précisément les aspects de la gouvernance du partage d'information.[9] En détaillant le mécanisme incitatif permettant d'orienter les comportements humains vers l'échange volontaire d'information, notre modèle permet également d'optimiser l'efficience de la cybersécurité.

Créer des conditions favorables pour le partage volontaire d'information

Notre modèle incitatif est compatible avec une vision libérale et décentralisée de la cybersécurité. Cette vision se base sur l'idée que, pour bien fonctionner, un système doit reposer sur la responsabilité individuelle, une adhésion volontaire et la motivation intrinsèque de ses membres, plutôt que sur la contrainte juridique. Cette vision, en accord avec celle du système de milice, repose donc fondamentalement sur la confiance et une collaboration forte entre le secteur public et le secteur privé. Nos recommandations politiques soutiennent l'idée qu'un partage volontaire d'information (reposant sur le modèle incitatif susmentionné) est plus efficient qu'un partage obligatoire, comme c'est le cas dans certaines juridictions.[10]

Les deux auteurs de l'étude à l'Université d'Innsbruck, juste après la présentation de leurs résultats au 17e Workshop on the Economics of Information Security (WEIS).

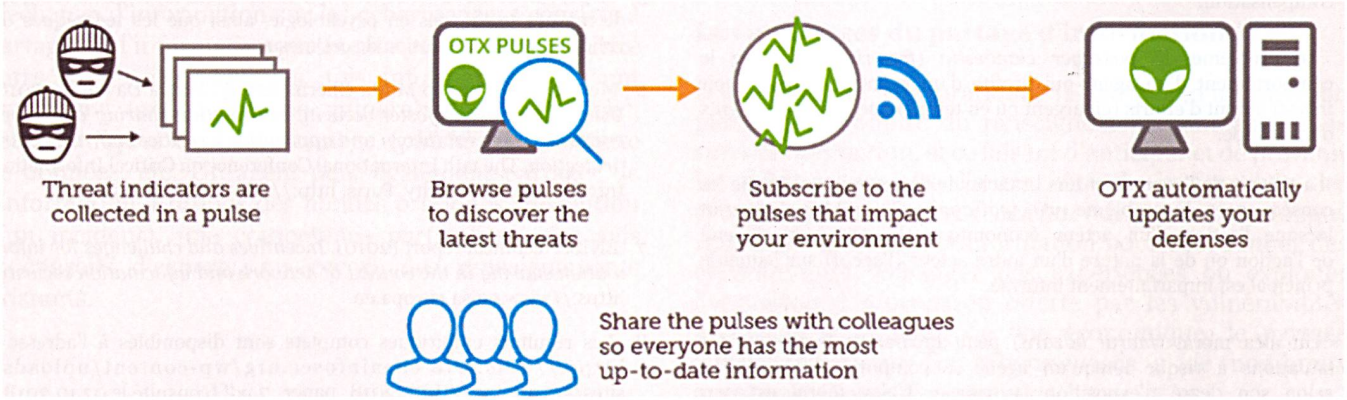
Vers un modèle automatisé en code source ouvert ?

Ces dernières années, certaines initiatives privées sont venues combler les défaillances des ISACs souvent considérés comme trop bureaucratiques. Ainsi, Facebook et IBM ont lancé en 2015 des plateformes

9 Mermoud A., Keupp M.M., Percia David, D. *Governance Models Preferences for Security Information Sharing : An Institutional Economics Perspective for Critical Infrastructure Protection*. In Proceedings of the International Conference on Critical Information Infrastructures Security (CRITIS), Kaunas, Lithuania, sep 2018. http://www.lei.lt/critis2018/

10 L'article 33 du nouveau règlement général de l'UE sur la protection des données crée par exemple un système de notification des violations de données à caractère personnel (*data breaches*). En cas de violation susceptible d'engendrer un risque pour les droits et libertés des personnes physiques, le responsable du traitement devra la notifier à l'autorité de contrôle dans les meilleurs délais et, si possible, 72 heures au plus tard (cf. art. 33 § 1).

La plateforme Open Threat Exchange permet à chacun de partager de l'information sur les cybermenaces. Les organisations peuvent créer gratuitement de « petits ISACs », c'est-à-dire des groupes par secteur d'activité en s'épargnant les coûts, les lenteurs et les infrastructures associées à un ISAC.
Source : https://www.alienvault.com



de CTI permettant le partage d'information sur les cybermenaces entre leurs utilisateurs. Aujourd'hui, la plus grande plateforme participative est *Open Threat Exchange* dont le code source est ouvert. Elle regroupe 80'000 participants de 140 pays qui partagent jusqu'à 19 millions de menaces potentielles par jour.

Cette plateforme, rachetée en août 2018 par AT&T, est partiellement automatisée et permet une grande interopérabilité, ainsi que l'intégration de technologies de rupture comme le *big data analytics* ou l'apprentissage automatique (*machine learning*). L'automatisation a par ailleurs l'avantage de supprimer ou diminuer les comportements humains inadéquats. Notre prochain projet de recherche compte exploiter les métadonnées disponibles sur cette plateforme afin d'affiner notre modèle incitatif qui se marie, à priori, parfaitement avec les pratiques de partage volontaire observées sur cette plateforme.

Le partage d'information, une activité-clé pour produire du renseignement

En conclusion, cette recherche apporte de multiples contributions. Sur le plan scientifique, elle permet de mieux comprendre le mécanisme incitatif qui sous-tend le partage volontaire d'information entre infrastructures critiques. Notre modèle a été développé dans le cadre de la protection des infrastructures critiques, mais il peut aussi être appliqué à d'autres domaines, tel que le partage d'information entre agences de renseignement. Il permet également de lutter contre les phénomènes de rétention d'information entre les différents acteurs de la chaîne sécuritaire. La Suisse offre un cadre idéal au déploiement de ce modèle grâce à sa stabilité politique et son haut degré de confiance entre et envers les institutions. Par ailleurs, cette recherche scientifique contribue à renforcer notre souveraineté numérique et la résilience des infrastructures critiques moyennant des coûts réalistes. En ce sens, nos résultats répondent également aux besoins stratégiques de la défense, de l'industrie et de la recherche académique.

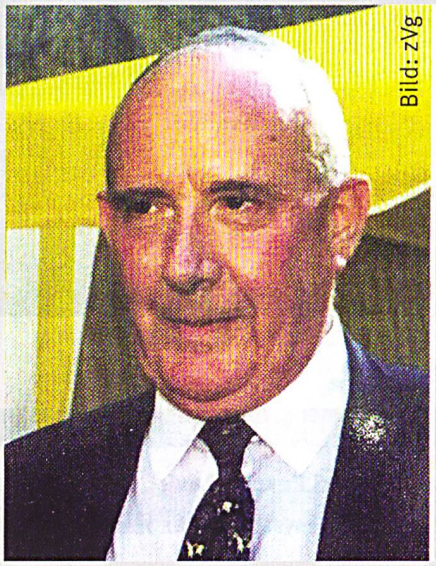
Sur le plan pratique, cette étude offre de nombreuses pistes aux praticiens pour améliorer l'efficience du partage d'information, notamment au sein des ISACs. Par ailleurs, les régulateurs y trouveront de nombreux conseils, notamment en matière de gouvernance, pour accompagner et soutenir le partage d'information sur le plan législatif. Enfin, sur le plan sociétal, ce travail contribue à un équilibre général en concurrence parfaite (*optimum de Pareto*) et donc à la réalisation du premier théorème du bien-être dans le domaine de la cybersécurité.

A. M. et D. P. D.

P.S.: Le DFAE a récemment crée un « Bureau de l'Envoyé spécial pour la politique étrangère et de sécurité relative au cyberspace » afin d'institutionnaliser la participation de la Suisse au partage d'information international.

Nécrologie

Colonel EMG Dominique Brunner



Le 30 septembre 2018, le colonel EMG Dominique Brunner (23.01.1938 – 30.09.2018) nous a quitté. Officier d'état-major général passionné, il a commandé le régiment d'infanterie bâlois (22).

Ce juriste de formation a travaillé de 1963 à 2008 pour l'entreprise de communication Rudolf Farner Public Relations AG. Il a été tour à tour associé, directeur puis président du Conseil d'administration (1980-1996). Il a rédigé durant ce temps plus de 500 articles de journaux et brochures. Son premier article pleine page date du 3 septembre 1961, où il offrait un plaidoyer pour la neutralité et une politique de sécurité et militaires modernes. Homme de débat, il a œuvré de manière constructive à de nombreuses votations sur l'armée.

Dominique Brunner est un nom connu des lecteurs de la RMS, qui regretteront ses traductions ainsi que ses articles d'opinion. La rédaction, émue, adresse ses meilleurs messages et ses remerciements sincères aux proches du colonel EMG Dominique Brunner.

Rédaction RMS+