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

Artikel: Les fusion centers : le renseignement sous stéroïdes?
Autor: Percia David, Dimitri / Mermoud, Alain
DOI: https://doi.org/10.5169/seals-823423

La France veut augmenter sa souveraineté numérique. Ainsi, la Direction Générale de la Sécurité Intérieure (DGSI) a trouvé une alternative française à Palantir pour la gestion de ses données stratégiques. Palantir est une entreprise qui fournit principalement des logiciels et des analyses Big Data à la communauté du renseignement des Etats-Unis.

Renseignement

Les *fusion centers* : le renseignement sous stéroïdes ?

Cap Dimitri Percia David, cap Alain Mermoud

Doctorants en systèmes d'information à HEC Lausanne et collaborateurs scientifiques à l'ACAMIL à l'EPF de Zurich

Le renseignement nait de l'analyse de l'information. La production de renseignement intégré implique ainsi le partage d'information entre acteurs du renseignement. Cette activité humaine constitue la raison d'être des *fusion centers*, et permet de maximiser la production de sécurité.

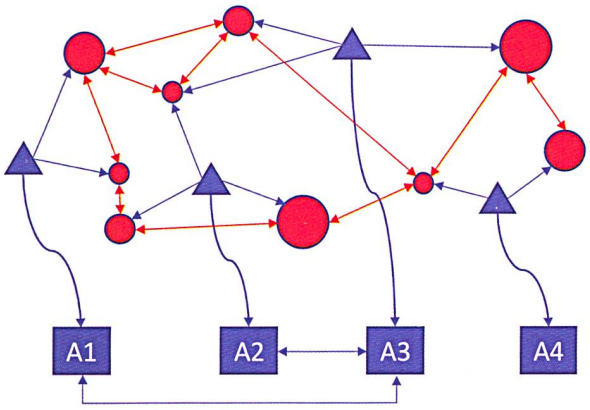
L'article précédent présentait notre recherche scientifique sur les incitations nécessaires à la production de cybersécurité grâce au partage d'information organisé par les *Information Sharing and Analysis Center* (ISACs). Dans cet article, qui suit nos précédentes publications dans l'ASMZ , nous étendons cette recherche aux *fusion centers* – une version améliorée et augmentée des ISACs – qui permettent de produire du renseignement, non seulement au service de la cybersécurité, mais également pour répondre à l'entier de l'éventail des menaces liées à la *société de l'information*.

L'inconvénient principal du partage d'information au sein des ISACs réside dans le fait qu'une transaction informationnelle entre plusieurs acteurs ne transcrit qu'une partie de l'ensemble des informations concernant les menaces pouvant être observées au sein d'un environnement donné. Ainsi, l'information est fragmentée et distribuée entre de nombreuses agences, rendant l'obtention d'une image complète de la situation longue et coûteuse. Par conséquent, une image incomplète de la situation est produite par les différentes agences de renseignement. La figure 1 illustre schématiquement ce problème d'asymétrie d'information.

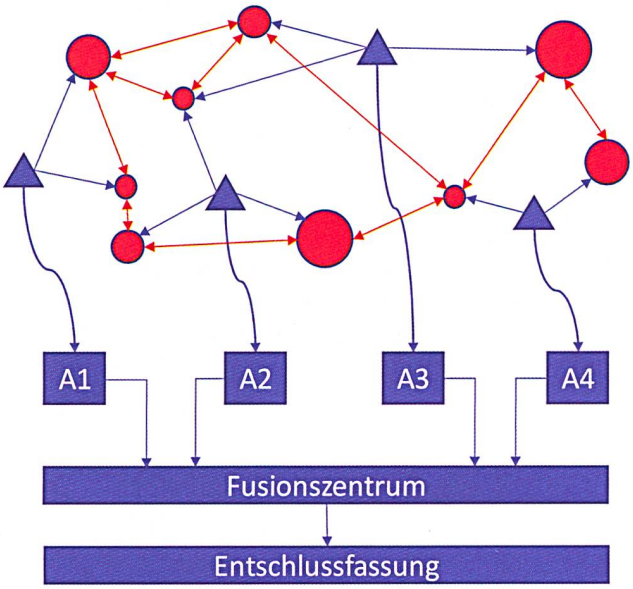
Les acteurs A1 à A4 ont chacun établi un senseur dans une structure hybride adverse. Chacune de ces sources fournit des informations à l'intention de chaque acteur. Bien que chaque élément structurel opposé soit observé par au moins une source, aucun acteur n'a une image correcte ou même complète de la situation. Au contraire, il ne reçoit que des informations fragmentées qui ne décrivent que de manière partielle la structure de l'adversaire. Cette situation est aggravée par le fait que les acteurs ne partagent pas nécessairement leurs informations fragmentées. L'acteur 3 échange des informations avec les acteurs 1 et 2, mais pas avec l'acteur 4. L'acteur 1 ne communique pas avec l'acteur 2, et l'acteur 4 ne partage aucune information (assimilé à un *passager clandestin*, ou *free-rider*). Cette fragmentation de l'information rend la prise de décision risquée, voire impossible.

L'idée d'un *fusion center* est de mettre fin à cette fragmentation en intégrant l'information de tous les acteurs. La figure 2 illustre l'état souhaité. Tous les acteurs alimentent le *fusion center* grâce aux informations acquises individuellement. En reliant les informations des différentes agences, il est maintenant possible de dresser un tableau complet de la situation et de prendre des décisions ciblées. Ainsi, les *fusion centers* aident à réduire les problèmes d'asymétrie d'information et de *passager clandestin*.

Les *fusion centers* permettent de lutter contre deux pratiques répandues dans les institutions: la rétention et le cloisonnement d'informations. Dû à l'absence de recoupement entre des informations de haute importance sécuritaire, ces pratiques génèrent un « manque à gagner » en termes de production de renseignement. La poursuite de ces pratiques est dommageable au développement d'un renseignement intégré, première ligne de défense contre les menaces contemporaines. La création de *fusion centers* adaptés aux structures institutionnelles de la Confédération pourrait apporter une solution pragmatique aux problèmes cités plus haut, et offrir un « guichet unique » (*one-stop-shop*) du renseignement suisse.



Cette illustration décrit la production de renseignement sans un fusion center. Chaque agence de renseignement reçoit des informations sur les menaces (cercles rouges) en provenance de ses senseurs respectifs (triangles bleus). Certaines agences communiquent entre elles, mais le partage d'information n'est pas systématique. Une forte présence d'asymétrie d'information est ainsi observée. Source : ASMZ.



Cette illustration décrit la production de renseignement avec un fusion center. Chaque agence de renseignement reçoit des informations sur les menaces (cercles rouges) en provenance de ses senseurs respectifs (triangles bleus). Ces informations sont cependant centralisées dans un fusion center. L'ensemble des informations est ainsi recoupé, rendant le partage d'information systématique. Une faible présence d'asymétrie d'information est ainsi observée. Source : ASMZ.

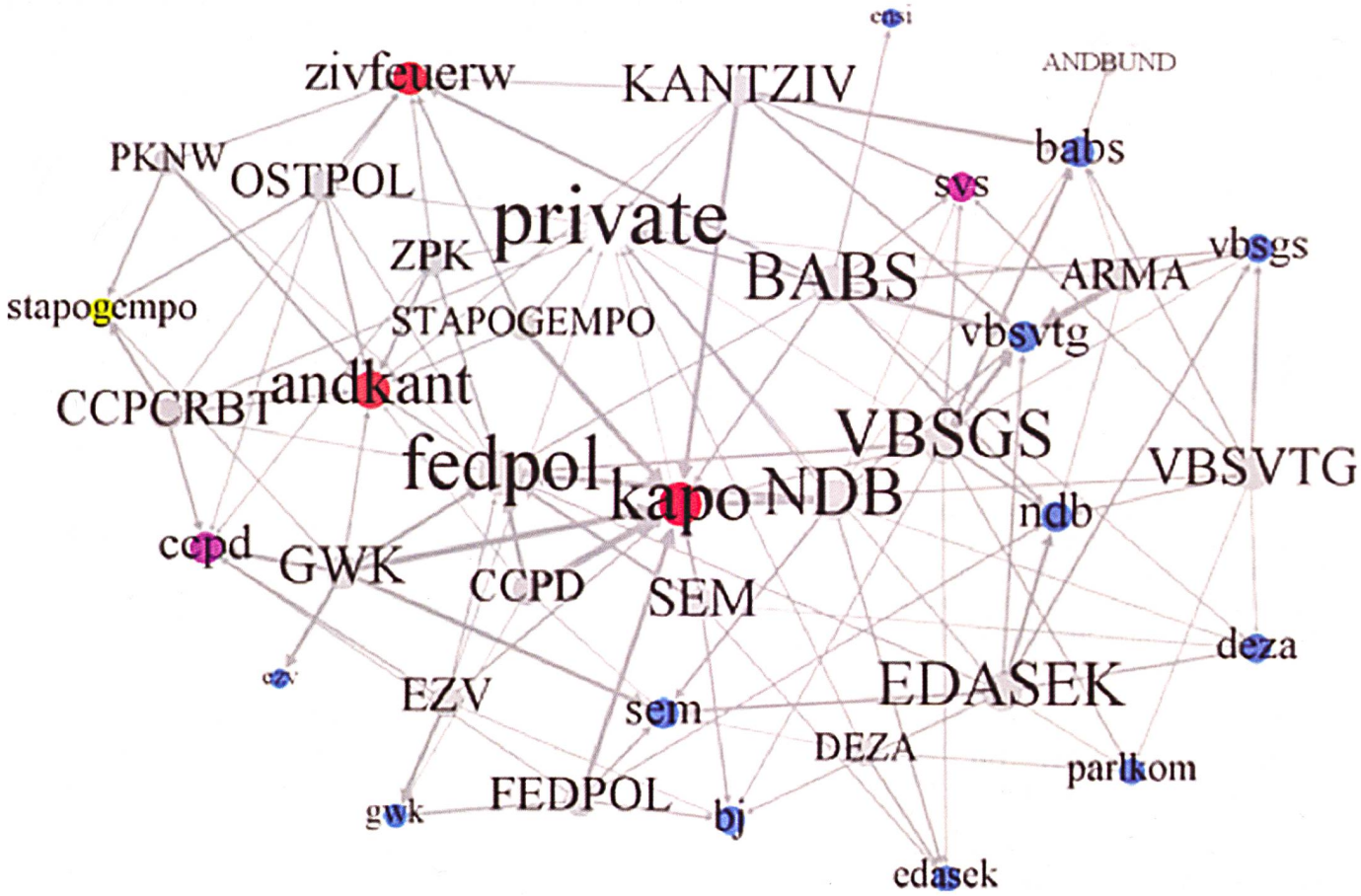
L'exemple américain : Un réseau national d'agences de renseignement

Afin d'assurer un partage d'information nécessaire à la production de renseignement intégré, le Département de la sécurité intérieure américain (*Department of Homeland Security*, DHS) a mis sur pied depuis 2003 un réseau national de *fusion centers*. Semblables aux historiques *Security Operation Centers* (SOC), les *fusion centers* agrègent les informations issues de diverses agences de renseignement (NSA, CIA, FBI, *military intelligence*, etc.), d'autres acteurs de la sécurité comme des agences fédérales (DEA, TSA, Garde nationale, etc.) et des polices locales, ainsi que des acteurs du secteur privé possédant des infrastructures permettant la collecte d'informations-clés (Google, Apple, Facebook, Amazon, Microsoft, etc.). Conçu comme une plateforme décentralisée – puisque généralement implémentée au niveau des Etats fédérés – de partage d'informations entre ces différents acteurs, les *fusion centers* constituent un réseau national de sources du renseignement.

Comme son nom l'indique, le but des *fusion centers* est de décloisonner les informations récoltées par les différentes agences de renseignement et acteurs-clés afin de lutter contre la rétention et le cloisonnement d'informations entre ces dernières. Mettre en réseau les différentes informations collectées permet alors de produire un renseignement intégré, recoupant, validant, et surtout complétant les informations manquantes que les agences isolées ne possèdent pas, rendant possible la détection de menaces complexes. C'est dans le contexte de l'échec d'anticipation des attentats du 11 septembre 2001 que le DHS envisagea la nécessité de décloisonner les informations propres aux différentes agences afin de favoriser un partage d'information nécessaire à la création de renseignement intégré. Réalisant que les différentes agences de renseignement américaines et les différents acteurs-clés à la production de renseignement avaient toutes les informations nécessaires afin de déjouer les attentats 9/11, mais qu'ils les cloisonnaient pour des raisons politiques, le DHS opta pour la création de *fusion centers*.

Le renseignement sous stéroïdes ?

Le processus opérationnel des *fusion centers* propose une méthode holistique de gestion du flux d'informations afin de produire un renseignement intégré, et ce à la fois à l'échelon régional et national. Le processus repose sur la participation active des organismes chargés de l'application de lois gouvernementales (nationales et régionales) et des acteurs du secteur privé afin d'intégrer les informations à des fins d'analyse propre à l'élaboration du renseignement. Au fur et à mesure que la diversité des sources d'information augmente, des analyses plus précises et plus solides peuvent être diffusées sous forme de renseignement ciblé. Les *fusion centers* permettent alors d'augmenter l'efficacité et l'efficience de la détection, la prévention, l'investigation et les réponses aux menaces ; le but final étant une recherche proactive d'identification et d'anticipation des menaces afin de les contrer avant qu'elles ne surviennent. Dans la *IV*e Révolution industrielle, de nombreux modèles d'affaires reposent sur le croisement de données hétérogènes provenant de sources variées. Le renseignement doit aujourd'hui poursuivre cette même logique afin d'anticiper les menaces et de détecter les opportunités.



Ce diagramme présente l'intensité (épaisseur des flèches) de collaboration entre les acteurs sécuritaires en Suisse. Un fusion center permettrait potentiellement d'augmenter la production du renseignement grâce à l'intensification du partage d'information existant entre ces acteurs.
Source : Hagmann, *et al.* 2018

Des *fusion centers* suisses ?

Fondé en 1971, le *Club de Berne* – comprenant les agences de renseignement des 28 Etats de l'UE ainsi que ceux de la Norvège et de la Suisse – est un forum informel de partage d'information entre directeurs du renseignement intérieur. Au sein de ce forum, le partage d'informations se fait de manière volontaire et non-contraignante. Notre modèle reposant sur cinq incitations-clés pour les ISACs (réciprocité, valeur de l'information, *design* institutionnel, réputation, et confiance), présenté dans notre précédent article, est donc généralisable au *Club de Berne*. Bien que manquant en intensité et en fréquence de partages, ce forum permet de produire du renseignement en capitalisant sur la neutralité et la stabilité politique et juridique de la Suisse. Le partage d'information entre nos différentes agences de renseignement et acteurs-clés de la sécurité – SRC, SRM, MPC, RNS, MELANI, FedPol, polices cantonales, douanes, entreprises stratégiques (RUAG) ou privées (ELCA, Kudelski, etc.) ne semble pas échapper aux enjeux de rétention et de cloisonnement d'information. Des *fusion centers* basés sur le principe volontaire de partage d'information, et adaptés à nos institutions (respectant les principes de subsidiarité et du fédéralisme) permettraient à la Confédération de maximiser sa sécurité nationale, tout en augmentant sa souveraineté dans le domaine du renseignement.

La production de renseignement permet d'une part de produire de la sécurité, et d'autre part de générer une « monnaie d'échange », tout comme l'introduction de la LRens[1] afin de « troquer » des produits du renseignement sur le marché international de ce dernier. Dans le but d'augmenter la fréquence et l'intensité du partage volontaire d'informations, les incitations citées dans notre article précédent fournissent les bases conceptuelles pour la création de *fusions centers* suisses, indispensables à la production de renseignement véritablement intégré. Assurer la production du renseignement par le partage d'information nécessite également de comprendre quels facteurs poussent les acteurs à participer à cet échange. Notre prochaine étude démontre l'importance de la perception positive du partage d'information pour la création de renseignement.[2] Comme dans le cas des ISACs, les (mauvais) comportements humains restent le maillon faible de la chaîne sécuritaire.

1 Mermoud, A., & Percia David, D. (2016). « La LRens: réduire le vide stratégique numérique suisse », in RMS+ N°4/2016,

2 La documentation complète concernant la méthodologie empirique et les résultats seront publiés in : Percia David, D., Keupp, M. M., & Mermoud, A. (2019). *Opportunism is not Enough: Understanding Performance Perception in Security Information Sharing. Computers in Human Behavior.*

De nombreux experts tirent un bilan mitigé de l'introduction de *fusion centers* aux Etats-Unis après le 11 septembre 2001. Comme dans le cas de certains ISACs, il semblerait que le *design* institutionnel joue un rôle majeur pour inciter les divers acteurs à partager la bonne information au bon moment. En particulier, il est important de laisser au secteur privé une grande marge de manœuvre et d'initiative pour organiser les partenariats publics-privés. Dans le cas américain, il semble qu'une place trop grande a été laissée aux Etats qui se sont rapidement enfermés dans des logiques de *rent-seeking* et de rétention d'information. Comme nous l'enseigne la nouvelle économie institutionnelle, il est essentiel que ces institutions (dans notre cas les *fusions centers*) reposent sur de saines règles incitatives permettant d'orienter (*nudger*) les acteurs vers des comportements maximisant la production de sécurité. A cet effet, il est essentiel de susciter une adhésion volontaire au système. En effet, si un acteur n'est pas intrinsèquement convaincu de l'utilité de sa contribution, il est fort probable que celui-ci partagera des informations incomplètes, voire fausses, et probablement pas dans les délais impartis. Dès lors, nous suggérons d'étendre notre modèle incitatif (décrit dans notre précédent article) aux *fusion centers*. Les résultats empiriques de cette étude scientifique seront présentés dans un futur numéro de la RMS.

D. P. D. et A. M.

Cyber

Les *fusion centers*, de quoi s'agit-il ?

Un *fusion center* est défini comme un espace physique et/ou virtuel dans lequel un effort de collaboration entre plusieurs agences de renseignement et acteurs-clés (senseurs) fournissent des ressources, expertises et informations. Le but d'un *fusion center* est de maximiser la capacité à détecter, prévenir, appréhender et répondre aux menaces. Les sources non-conventionnelles de collecte d'informations tels que les organisations du secteur privé peuvent être intégrées dans un *fusion center*. La mise en réseau de diverses informations collectées par les acteurs du *fusion center* permet, à la différence des agences de renseignement cloisonnées, de délivrer du renseignement intégré.

Les exemples actuels incluent le *Kudelski Cyber Fusion Center* (https://www.kudelskisecurity.com/services/managed-security) et les *fusion centers* de la *US National Fusion Center Association* (https://nfcausa.org/). En matière de défense, l'OTAN exploite le *Intelligence Fusion Center* depuis 2007, bien que l'analyse ne soit pas centrée sur la cybersécurité mais sur le terrorisme international.