Observatoire Projet, Innovation, Conception (PIC)
Les échos de l'innovation

L'open innovation dans le secteur de la défense à propos de : Practicing secrecy in open innovation :

The case of a military firm

Victoire Charpy, Titouan Floquet & Titouan Lemaitre
Étudiants au Master PIC (promotion 2022-2023)

Résumé de l'article
L'article s'intéresse à la publication de l'article Langlois, J., BenMahmoud-Jouini, S., & Servajean-Hilst, R. : Practicing secrecy in open innovation – The case of a military firm paru dans la revue Research Policy en janvier 2023. Cet article est notamment issu des travaux de thèse de Langlois (2022), explorant les mécanismes qui permettent à l'open innovation d'exister dans le monde de la défense malgré les contradictions à première vue difficilement surmontables qui opposent ces deux mondes. L'article qui suit a pour objectif de vulgariser et de diffuser certains concepts abordés dans ces deux travaux de Langlois (2022).

Introduction

En 2014 un concours surprenant est apparu sur la plateforme Topcoder.com. L'objectif, développer un algorithme capable de surveiller les déplacements des populations de bisons des parcs naturels américains à partir d'images postées sur internet par des touristes.
Contrairement aux apparences, cet outil n'était en fait pas destiné à l'étude de la vie sauvage. C'était en fait un stratagème déployé par les services secrets américains pour faire développer une solution innovante leur permettant de suivre les déplacements des forces russes à la frontière avec la Crimée.
Cet exemple démontre que l'open innovation et le monde du secret ne sont pas incompatibles.

Pourquoi étudier le secret dans l'open innovation ?

Le but d'une entreprise innovante est de parvenir à extraire de la valeur des innovations qu'elle développe. Cette notion est appelée appropriabilité de l'innovation. Les solutions couramment utilisées pour s'approprier l'innovation reposent principalement sur des outils de protection de la connaissance qui s'appuient ou non sur l'appareil légal (brevets, propriété intellectuelle, copyrights vs norme sociale, moyens d'exclusion économique, etc.).
L'open innovation (OI) repose sur une diffusion vers des acteurs externes de la connaissance d'une entreprise et vient donc bousculer cette conception classique selon laquelle, la protection de cette connaissance est l'unique moyen générer un avantage compétitif à partir d'une innovation.
Le paradoxe repose dans le fait que le partage de connaissance est indispensable pour profiter de bénéfices de l'OI, mais la protection de cette connaissance est indispensable pour pouvoir s'approprier l'innovation et la convertir en avantage compétitif.

Si la littérature est vastement développée sur le sujet de la protection de la connaissance grâce aux outils de propriété intellectuelle, la protection de la connaissance par le secret est peu abordée alors même qu'elle est vastement déployée au sein des entreprises.

Comment est défini le secret dans la littérature ?

Pour comprendre sous quelle forme le secret est déployé au sein des entreprises, il est intéressant de revenir à la définition du secret.

Une définition managériale du secret est l'ensemble des règles qui restreignent le partage d'une information définie entre deux individus définis au sein d'une organisation. Ces règles peuvent être formelles comme un accord de non-divulgation ou informelles comme séparation physique des personnes qui permet le cloisonnement de l'information en limitant l'interaction sociale de ces personnes.

Une approche sociale du secret est l'ensemble des actions d'un individu donné pour dissimuler intentionnellement des informations à un autre individu au sein d'une organisation. Une façon de reformuler cette définition sous une forme éthiquement neutre est de définir le secret comme la limitation de connaissance réciproque dans les interactions sociales. Le secret peut alors être considéré comme une conséquence inévitable de toute interaction des individus avec le reste de la société.

On peut alors distinguer deux formes de secret. La forme passive consiste simplement à ne pas révéler certaines informations. Toute interaction sociale est par nature empreinte de cette forme passive de secret. La forme active du secret consiste à transformer la connaissance pour dissimuler les informations que l'on souhaite garder secrètes.

Enfin, le secret peut s'envisager sous différentes perspectives : la perspective dyadique et la perspective triangulaire. La perspective dyadique se définit comme la simple dissimulation d'une information par un individu à un groupe d'individus alors que la perspective triangulaire se définit comme le partage d'un secret avec un individu donné tout en dissimulant ce secret à un troisième groupe d'individus.

Ce retour à une définition sociale du secret nous invite à envisager comment l'ensemble de ces mécanismes sociaux peuvent participer au secret au sein d'un processus d'OI.

L'objectif est de comprendre comment ces formes sociales de secret peuvent permettre de dépasser le cadre traditionnel de management de la connaissance qui repose sur la contractualisation de la propriété intellectuelle. En particulier comment cette articulation sociale du secret à l'échelle micro des interactions entre les individus peut permettre d'être transparent en secret ou secret dans la transparence et ainsi aboutir à des interactions plus fructueuses.

Question de recherche

Trois limites de la littérature actuelle ont été mises en lumière, le rôle et les caractéristiques du secret dans le processus d'OI, au-delà du cadre traditionnel de la gestion du secret au niveau de l'entreprise (1), les formes de secret actives et passives et leur rôle dans le processus de partage de la connaissance (2) et l'évolution temporelle de mécanismes de dissimulation au cours du processus d'OI (3).

L'objectif de cet article est de répondre à ces limites de la littérature en répondant à la question suivante : comment les acteurs d'une firme font-ils individuellement usage des pratiques du secret pour naviguer le paradoxe de la transparence dans un processus d'OI ?

Méthodologie

Afin de tenter de répondre à la question de recherche énoncée ci-dessus, une série de 16 entretiens préliminaires avec des ingénieurs et des acheteurs directement impliqués dans le processus d'OI au sein de l'entreprise de défense européenne Globaldef a été réalisée. Les enjeux de l'OI identifiés lors de ces entretiens préliminaires ont suscité le besoin de réaliser 27 entretiens supplémentaires pour répondre aux quatre questions suivantes :

(1) Pourquoi certains acteurs pratiquent-ils le secret?
(2) Comment ce secret est-il pratiqué?
(3) Quelle est la nature des informations dissimulées?
(4) Qui sont les acteurs auxquels on dissimule ces informations?

À l'issue de ces entretiens ont été identifiés 235 unités de sens qui ont pu être regroupées en 20 catégories, qui ont elles-mêmes été regroupées en 7 aspects du secret comme décrit dans la figure ci-dessous.

***Figure 1** : Schéma présentant la structure des données récoltées lors des entretiens*

Résultats

Suite aux entretiens réalisés concernant la gestion du secret dans des projets d'Open Innovation, deux types de pratiques distinctes ressortent : les pratiques cognitives et les pratiques relationnelles.

Les pratiques cognitives du secret dans l'OI

Pour chercher des solutions innovantes externes à l'entreprise, les employés de GlobalDef commencent par *recadrer* les connaissances qu'ils vont partager à leur partenaire. Ce *recadrage* peut se distinguer en quatre catégories qui varient selon le degré d'altération de la connaissance d'origine (*secret actif*) et selon le degré de dissimulation de cette connaissance (*secret passif*) : offuscation, simplification, transposition et chiffrement.

En effet, le principal enjeu est de s'assurer qu'aucun élément secret concernant les produits de l'entreprise ne soit divulgué. Pour cela, les individus décontextualisent et généralisent les connaissances de l'entreprise. Ils doivent souvent déterminer eux-mêmes si la connaissance qu'ils détiennent est secrète et avec qui ils peuvent la partager. En effet, certaines catégories sont clairement identifiées comme secrètes (la dissuasion nucléaire par exemple), mais d'autres se situent dans une zone floue. En outre, certaines personnes interrogées se demandent parfois si l'information n'a pas été "surprotégée". Ainsi, l'ambiguïté concernant ce qui est secret ou non explique pourquoi les personnes interrogées ont très souvent employé l'adjectif "sensible" pour qualifier une connaissance potentiellement secrète. Cette tâche complexe de devoir *recadrer* l'information avant de pouvoir la partager constitue donc un *coût cognitif*.

L'offuscation consiste à brouiller les informations les plus critiques afin que le partenaire comprenne le sens global, mais pas les détails. Elle est particulièrement utile lorsque le secret concerne des informations quantitatives, car cela se traduit alors par le fait de donner des ordres de grandeur plutôt que des chiffres exacts.

La simplification consiste à supprimer les éléments sensibles et à *recadrer* le problème en quelque chose de plus simple. L'avantage de cette méthode est qu'elle permet de partager rapidement de l'information tout en limitant le coût cognitif et organisationnel lié au besoin de recadrage. Par exemple, un des experts interrogés explique : "Typiquement, si [dans la collaboration] on cherche à optimiser une trajectoire, on évite de choisir des contraintes révélant les caractéristiques de la zone à défendre, qui peut être sensible et confidentielle. On choisit un ensemble de contraintes suffisant, mais sélectionné avec soin".

La transposition consiste à transposer le problème dans un autre contexte que celui d'origine. Par exemple, pour dissimuler l'aspect militaire, un expert technique a "créé un scénario avec des voitures devant atteindre des stations de recharge et optimiser leurs trajectoires". L'avantage de la transposition dans un contexte civil est que cela permet d'attirer des entreprises innovantes pas forcément liées au monde de la défense.

Enfin, le chiffrement consiste à chiffrer les données sensibles tout en conservant le sens global. En effet, afin que les partenaires aient une idée suffisamment précise de la demande, les parties chiffrées ne doivent pas être essentielles à la compréhension du problème; autrement, cela pourrait générer chez les partenaires de la confusion et de la frustration. Le chiffrement est souvent utilisé pour les projets de *big data*, où il peut consister en une modification des noms des variables qui deviennent par exemple A, B, C, D, etc.

Cependant, le problème de toutes ces pratiques cognitives est qu'elles conduisent à une sur-codification de la connaissance. Soit trop d'informations sont cachées de peur qu'elles soient secrètes, soit les informations cachées rendent trop compliqué une bonne compréhension du problème. Face à ce problème, certains employés se demandent si cela vaut vraiment le coup de chercher à capter des connaissances externes à l'entreprise.

Les pratiques relationnelles du secret dans l'OI

Petitat (1998) distingue deux catégories de gestion du secret dans les relations sociales. La forme dyadique consiste à dissimuler des connaissances à d'autres acteurs, tandis que la forme triangulaire fait référence au fait de partager un secret avec un autre acteur tout en excluant un troisième ensemble d'acteurs.

L'étude de Langlois (2022) a révélé que, toujours dans le but de protéger les connaissances secrètes, les acteurs mettent en place deux types de limites dans les partenariats : des limites internes (entre eux et les partenaires, i.e. secret dyadique) et des limites externes à la structure du partenariat (i.e. secret triangulaire).

Les limites internes permettant de protéger les informations secrètes consistent à *recadrer* toutes les informations circulant entre l'entreprise et son partenaire. Ainsi, toute information qui sort de l'entreprise est *recadrée* avant d'arriver dans les mains du partenaire, qui travaille sans avoir accès aux informations secrètes.

Les limites externes, quant à elles, sont nécessaires lorsque le partenaire ne peut pas travailler efficacement sans avoir accès à la connaissance secrète. Il ne s'agit alors plus de mettre des mécanismes de contrôle sur l'information circulant entre l'entreprise et son partenaire, mais entre l'entreprise et son partenaire d'un côté, et le monde extérieur de l'autre. Pour un projet avec une entreprise partenaire, l'entreprise a par exemple aidé son partenaire à déménager dans des locaux plus sécurisés et a dépêché ses experts en cybersécurité afin de former les dirigeants aux risques encourus.

Combiner la profondeur contextuelle avec le degré de visibilité des connaissances partagées dans les partenariats d'OI

En ayant recours aux pratiques cognitives décrites précédemment, les acteurs décontextualisent les informations et modulent leur profondeur contextuelle afin de pouvoir partager leurs connaissances en dehors de l'entreprise.

En parallèle, les pratiques relationnelles modulent quant à elles le degré de visibilité des connaissances partagées. En effet, ces pratiques déterminent le nombre potentiel d'individus pouvant avoir accès à ces connaissances. Comme représenté par le "Secrecy mode I" sur le schéma ci-dessous, les limites internes de protection du secret (secret dyadique) entraînent une large diffusion des connaissances, car l'entreprise s'est préalablement assurée que toutes les connaissances partagées au partenaire ne contenaient aucune information secrète, donc l'entreprise partenaire n'a pas besoin de faire attention aux connaissances qu'elle divulgue. À l'inverse, comme représenté par le "Secrecy mode II" sur le schéma, les limites externes de protection du secret (secret triangulaire) engendrent une diffusion des connaissances beaucoup plus réduites, car l'entreprise a préalablement cherché à s'assurer que seules les personnes habilitées et ayant le droit d'en connaître pourraient avoir accès aux connaissances partagées. Ainsi, afin de combiner ouverture et protection du secret, les entreprises combinent la profondeur contextuelle (qui permet le partage de connaissance) avec le degré de visibilité (qui permet la protection des connaissances).

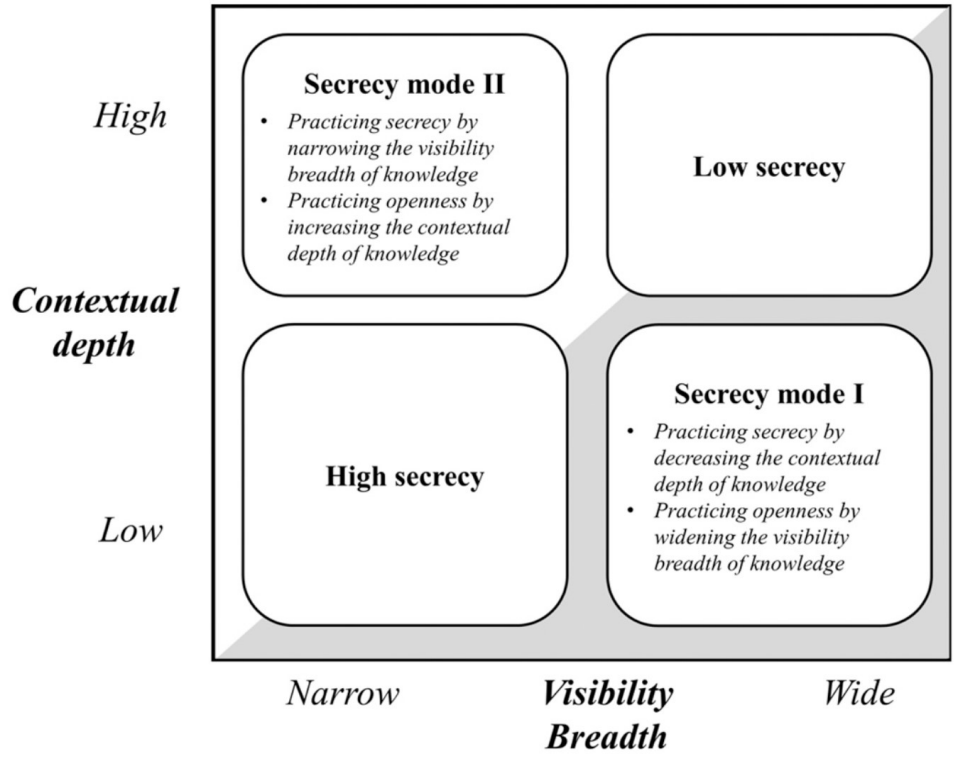

***Figure 2** : Schéma présentant les différents modes de gestion du secret*

La dynamique des pratiques de secret dans l'évolution temporelle des partenariats OI

En analysant de près les modes de secret déployés dans les six partenariats OI, les chercheurs ont découvert que les acteurs de Globaldef ont modifié la profondeur contextuelle et l'étendue de la visibilité des connaissances échangées avec leurs partenaires en fonction de la phase du cycle de vie du partenariat (recherche, initialisation du partenariat et intégration des connaissances).

Lors de la phase de recherche, les acteurs de Globaldef ont déployé divers processus pour trouver des sources externes de connaissances, tels que le crowdsourcing, les salons professionnels, ou le scouting. Pour activer ces processus de recherche, les acteurs doivent révéler des connaissances internes afin d'accroître la spécificité de la recherche. Cependant, au début de la recherche, les partenaires ne sont pas encore connus, et leur statut d'ami ou d'ennemi n'a pas encore été établi. Par conséquent, les participants à la recherche ont vécu une tension entre le partage et la protection des connaissances.

Pour surmonter ces tensions, les acteurs ont combiné l'élargissement de l'étendue et la réduction de la profondeur tout en renonçant à un certain degré de précision. À l'inverse, les chercheurs ont combiné une faible étendue et une grande profondeur pour tirer parti d'interactions plus profondes concernant le problème sous-jacent, mais avec un éventail limité de résolveurs potentiels.

Une fois que les acteurs ont identifié un partenaire correspondant aux exigences de la recherche, il faut initier le partenariat en définissant la profondeur contextuelle des connaissances partagées et le niveau de contrôle de la connaissance au-delà du partenariat.

Deux approches sont possibles :

- L'approche peu approfondie/étendue : avantageuse en termes de temps et de coût d'initialisation du partenariat, parce que les acteurs ont évité le long processus d'obtention d'accréditation. Cependant, cette approche était désavantageuse en raison de l'écart créé

entre les connaissances originales et les connaissances recadrées, et cet écart pouvait limiter l'ambition de la recherche en termes de création de connaissances et d'innovation.

- L'approche très approfondie/étroite : permet aux acteurs de partager des connaissances beaucoup plus approfondies, mais le cadre formel requis est plus coûteux et plus long à mettre en œuvre.

Une fois que les partenariats OI sont lancés, trois types de trajectoires sont possibles dans l'évolution des partenariats.

- Les acteurs continuent à maintenir une approche peu approfondie/étendue des pratiques de secret. Cette approche offrant un bon rapport coût-efficacité dans la phase d'initialisation peut devenir difficile et coûteuse, en particulier lorsque les acteurs bénéficiaires cherchent à générer des connaissances de plus en plus spécifiques.
- Les acteurs passent d'une approche peu approfondie/étendue à une approche très approfondie/étroite à un moment donné du partenariat OI. Cela implique de changer la pratique relationnelle du secret précédemment adoptée, c'est-à-dire le passage d'une frontière interne à une frontière externe.
- Les acteurs peuvent maintenir l'approche très approfondie/étroite qui a été mise en œuvre dans la deuxième phase.

Les objectifs peuvent évoluer au cours du partenariat. Par exemple, si les acteurs bénéficiaires travaillent sur des sujets plus spécifiques, après avoir travaillé sur des sujets plus génériques alors, ils compensent l'augmentation de la profondeur contextuelle par une diminution de l'étendue de la visibilité, en sécurisant le flux de connaissances.

De plus, dans certains cas, les acteurs bénéficiaires ont cherché à influencer la stratégie de croissance de leur partenaire vers les marchés de la défense. Du point de vue des acteurs bénéficiaires, cette approche " high depth/low breadth " encourage l'assimilation des codes de défense, qui est indispensable pour prospérer dans cette industrie.

Discussion

D'une perspective statique à une approche plus dynamique du secret dans les partenariats de l'OI

Cette recherche apporte de nouvelles perspectives par lesquelles les acteurs organisationnels peuvent modifier le format des connaissances qu'ils échangent. Par exemple, si dans un contexte organisationnel les acteurs échangent ouvertement des connaissances basées sur une formulation très explicite, mais transposée ou simplifiée, un observateur distant pourrait conclure à tort que les connaissances circulent de manière très ouverte entre les partenaires, passant ainsi à côté de la pratique cognitive de la dissimulation.

Cette étude met également en évidence les pratiques relationnelles que les acteurs de l'OI déploient en mettant en place des frontières internes au partenariat afin de contrôler la visibilité et l'exposition des connaissances et les efforts significatifs déployés par les acteurs focaux afin d'aider leurs partenaires à construire leurs propres pratiques de secret au niveau organisationnel, par la transmission d'une culture du secret.

D'une vision institutionnelle à une vision stratégique du secret dans l'IO

Pour le moment, dans la littérature sur la stratégie, le secret a été essentiellement abordé comme un mécanisme statique d'isolement au niveau de l'entreprise appliqué par des règles institutionnelles. L'approche du secret développée dans cette étude aborde le secret comme une pratique de niveau

micro-encadrée dans un espace à deux dimensions. Les acteurs individuels s'efforcent de naviguer dans la combinaison entre profondeur contextuelle et ampleur de la visibilité des connaissances qu'ils partagent. Ainsi, les règles institutionnelles de secret ne sont pas considérées comme une fin en soi, mais comme un moyen de soutenir une stratégie particulière et sont sujettes à modification dans l'évolution des projets d'innovation.

Une telle vision du secret ouvre de nouvelles perspectives de recherche sur les compromis auxquels sont confrontés les décideurs dans les processus d'OI et de partage des connaissances. À cet égard, le cadre de la profondeur contextuelle et de la largeur de la visibilité peut servir d'analyse de base menant à la découverte de stratégies de secret.

Conclusion

L'objectif de cette recherche est de mieux comprendre comment les acteurs individuels pratiquent le secret lorsqu'ils participent à des initiatives d'OI entrantes visant l'acquisition de connaissances externes. En se basant sur une étude qualitative d'une seule entreprise, cette étude montre que les acteurs de l'OI ont déployé des pratiques cognitives et relationnelles du secret afin d'acquérir des connaissances externes. Ainsi, cette étude montre qu'être "ouvert" ne signifie pas renoncer à ses secrets, mais déployer une stratégie concernant la profondeur contextuelle et l'étendue de la visibilité des connaissances à échanger avec les partenaires de l'IO. De plus, cette étude propose un cadre comme modèle pour construire des stratégies de secret dans les partenariats d'innovation. En outre, ces stratégies peuvent contribuer à faire passer le secret d'une activité purement juridique et contractuelle à un effort plus stratégique.

Cette recherche présente cependant certaines limites. Tout d'abord, des travaux antérieurs soulignent que l'étude du secret dans les organisations soulève des questions évidentes et méthodologiques. En effet, la recherche de données sur un tel sujet est une tâche délicate pour les chercheurs. Même si une relation de confiance a été établie entre chercheurs et informateurs, il est inévitable que les données aient été elles-mêmes sujettes à un recadrage des connaissances de la part des informateurs. Une autre limite de cette étude est l'absence d'une explication exhaustive du changement entre les pratiques de secret dans l'OI, bien que certaines variables clés ont été évoquées. Une troisième et importante limite de cette étude concerne le secteur militaire auquel appartiennent l'étude de cas et les informateurs. Ce n'est pas que les autres secteurs sont moins secrets que l'industrie de la défense, mais de nombreuses pratiques de secret sont déterminées par un système de règles spécifiques au secteur de la défense. Cette forte spécificité sectorielle pourrait limiter le caractère généralisable des résultats.

BIBLIOGRAPHIE

Langlois, J. (2022). The dynamics of secrecy management in open innovation: The case of the defense industry. *Thèse de doctorat*, Institut Polytechnique de Paris

Langlois, J., BenMahmoud-Jouini, S., & Servajean-Hilst, R. (2023). Practicing secrecy in open innovation–The case of a military firm. *Research Policy*, *52*(1), 104626.

Petitat, A. (1998). *Secret et formes sociales*. Presses universitaires de France.

Pour citer cet article :
Charpy V., Floquet T., & Lemaitre T., (2023) « L'open innovation dans le secteur de la défense à propos de Practicing secrecy in open innovation The case of a military firm », *Les échos de l'innovation, Observatoire Projet, Innovation, Conception (PIC),* mis en ligne le 20 février 2023.

L'Observatoire PIC regroupe les publications diverses que les enseignants et les étudiants produisent à partir de leurs travaux et réflexions : publications (livres, articles ou communications à des colloques du domaine), cahiers du master PIC (support de valorisation des mémoires de recherche, coécrit entre les étudiants et les tuteurs), les échos de l'innovation, et vidéos (issues des soutenances publiques)

www.masterpic.fr/observatoire