Sécurité, défense et l'Internet des objets: entendons ce que 1000 étudiants suisses ont à dire à ce sujet

L'intelligence ambiante permet d'imaginer un très grand nombre d'innovations mais elle comporte aussi des risques. Au-delà des experts, les citoyens ont un véritable rôle à jouer. Connaître leurs comportements et leurs pratiques est essentiel. Pendant cinq mois, de septembre 2016 à janvier 2017, une étude a été menée en Suisse occidentale auprès de 1000 étudiants pour explorer les futurs possibles de l'intelligence ambiante en Suisse. L'utilisation de Futurescaper, une plateforme à destination d'organisations engagées avec leurs parties prenantes dans des activités de prospective participative, a permis de dégager plusieurs éléments de discussion autour des questions suivantes: quels sont les futurs possibles de l'intelligence ambiante en Suisse et comment entreprises, administrations publiques et individus peuvent-ils agir dès à présent pour saisir les opportunités et faire face aux menaces qui lui sont liées?

Mots clés: **Intelligence ambiante, prospective, Suisse occidentale, production collaborative**

Auteurs: **Prof. Thomas Gauthier**, HEG-Genève & emlyon; **Dr. Sylvaine Mercuri Chapuis**, ESDES, The Business School of Ucly

Introduction

L'«intelligence ambiante», le système constitué par l'ensemble des objets connectés (ordinateurs, tablettes, montres et bracelets connectés etc.) et capables d'analyser rapidement les données qu'ils enregistrent, permet aux individus d'accéder à l'information plus simplement, «la proactivité de l'environnement venant alléger la charge cognitive que l'usager doit actuellement mobiliser pour accéder à cette information via des ordinateurs» (Entretien, 2009; p. 482). L'intelligence ambiante permet d'imaginer un très grand nombre de nouvelles applications et de nouveaux services mais elle comporte aussi des risques, en particulier dans le domaine de la sécurité et de la défense informatique. Face à des hackers de tous horizons, la protection des données sensibles est indispensable et elle doit faire l'objet d'une attention permanente autant d'un point de vue individuel que collectif. Les derniers scandales en date, celui de la cyberattaque du 12 mai 2017 via le virus «Wannacry» qui a touché plus de 150 pays dans le monde, infectant plus de 200 000 ordinateurs (seulement 200 en Suisse) (Le Temps, 2017) ou celui de la cyberattaque du 27 juin 2017, impliquant plusieurs multinationales européennes et américaines ainsi que des structures gouvernementales ne sont qu'une illustration de ce qui pourrait se multiplier à l'avenir. Pour assurer la protection de leur vie privée, les individus doivent redoubler de vigilance et ils sont les premiers à jouer un rôle. En 2016, dans son rapport semestriel sur la sureté de l'information, la Confédération Suisse, réalisant un état des lieux sur le plan international, indiquait que la barre des 20 milliards d'objets connectés (contre 6 milliards à cette époque) devrait être franchie d'ici 2020 [1] . Elle indiquait également que la vulnérabilité de l'Internet des objets tenait «surtout à la culture de sécurité» (p. 8) des fabricants et des utilisateurs des objets communicants. A la lecture de ce rapport, on comprend qu'il s'agit alors d'agir sur les cultures qui coexistent aujourd'hui afin de définir de bonnes pratiques individuelles et collectives qui permettraient de développer une «bonne» culture de la sécurité (Chevreau et Wybo, 2007). En s'intéressant aux valeurs, aux normes ou aux symboles partagés et qui sont supposés être liés à la sécurité, il s'agit de mobiliser au-delà des experts, un collectif plus large, l'ensemble des citoyens, premiers vecteurs de risque, qui ont ici un véritable rôle à jouer.

Une réflexion autour de leurs comportements et de leurs pratiques est alors indispensable. Elle permet notamment une sensibilisation voire une prise de conscience, permettant de stimuler des comportements plus vigilants. De manière à faciliter ce changement, le recours à des activités de prospective est intéressant car celles-ci consistent pour n'importe quel individu, compte tenu de tendances lourdes et de signaux faibles perceptibles dans son environnement et qui sont d'ordres politique, économique, socioculturel, technologique, écologique ou encore légal, à imaginer des scénarios d'avenir plausibles pour faciliter sa prise de décision et son action. Ainsi, plutôt que d'anticiper des changements prévisibles pour mieux s'y préparer et en tirer parti (notion de préactivité), l'individu cherchera à provoquer les changements souhaités par des actions spécifiques (notion de proactivité) (Godet et Durance, 2011). Cette différence est notable car l'action individuelle et collective change de statut : elle est perçue de manière plus positive par les individus car ils sont responsables de l'avenir qu'ils contribuent à façonner à travers les actions qu'ils entreprennent.

Pour mener une réflexion plus large, la question suivante peut être posée : quels sont les futurs possibles de l'intelligence ambiante en Suisse et comment entreprises, administrations publiques et individus peuvent-ils agir dès à présent pour saisir les opportunités et faire face aux menaces qui lui sont liées ? De manière à répondre à cette question, une étude a été menée entre septembre 2016 et janvier 2017 auprès de près de 1000 étudiants en Suisse occidentale. A cette occasion, Futurescaper, une plateforme créée en 2011 à Londres par Noah Raford et Nathan Koren, a été utilisée.

Futurescaper, animer la réflexion collective et prospective

Depuis 2011, la plateforme Futurescaper est utilisée pour animer de nombreuses réflexions prospectives. Il s'agit d'imaginer des solutions futures avec plusieurs participants à même d'apporter des contributions et des éclairages significatifs sur des situations précises. Il s'agit aussi de rendre l'action individuelle plus qualitative en favorisant une dynamique intellectuelle permanente.

Développée par deux diplômés du MIT et de l'Université d'Oxford, la plateforme Futurescaper propose de suivre une série de quatre étapes: la préparation du projet (étape 1), l'engagement des parties prenantes (étape 2), l'interprétation et l'analyse (étape 3) et la restitution et la présentation des résultats (étape 4). Les réflexions autour de l'environnement correspondent au point de départ pour définir des scénarios plausibles, qui sont non figés et qui permettent de prendre des décisions immédiates (Godet, 2004). Cette manière de fonctionner permet de caractériser la plateforme Futurescaper comme une véritable innovation incrémentale car son ingénierie permet d'aller au-delà de raisonnements causaux en créant une réticulation de la pensée entre plusieurs participants.

Les contributions vers lesquelles la plateforme Futurescaper oriente sont quant à elles d'ordre qualitatif (Figure 1) car il s'agit d'imaginer collectivement des tendances, les conséquences de ces tendances, et les conséquences de ces conséquences. Elle facilite une réflexion collective qui permettra ensuite aux participants de proposer des combinaisons nouvelles, des scénarios, dans lesquels figureront des opportunités et des

menaces à saisir ou à éviter. Compte tenu de ces opportunités et menaces, les participants pourront alors s'exprimer sur les attitudes à avoir pour changer ou pour poursuivre le scénario qu'ils imaginent. Les participants sont force de proposition car ils verbalisent des pistes d'actions compte tenu de tendances qu'ils n'auraient peut-être pas identifiées individuellement.

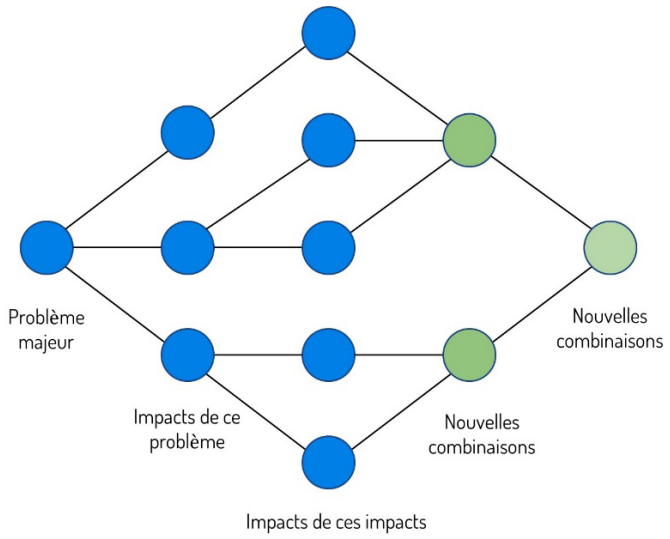

Figure 1: Contributions obtenues en utilisant la plateforme Futurescaper

Déterminer les futurs possibles de l'intelligence ambiante en Suisse

Entre septembre 2016 et janvier 2017, près de 1000 étudiants de Suisse occidentale ont été sollicités pour participer à une démarche de production collaborative (crowdsourcing). Les étudiants préparant un Bachelor ou un Master étaient issus de filières économiques et de gestion mais aussi de filières d'ingénierie, d'art et de design [3] . Lors d'une séance de 45 minutes environ, dans leur classe habituelle (de 10 à 80 étudiants), une intervenante préalablement identifiée par le directeur de l'étude commençait par diffuser une vidéo de présentation de l'intelligence ambiante. Les participants étaient ensuite interrogés de manière ouverte sur leur connaissance du sujet puis trois exemples leur étaient proposés : les véhicules autonomes, les drones et la montre connectée d'Apple, l'Apple Watch. L'intervenante indiquait ensuite une adresse Internet à laquelle les participants étaient invités à se rendre afin de participer à l'étude. Elle les informait que d'autres classes avaient été interrogées en amont et que les réponses d'autres étudiants étaient déjà enregistrées et visibles sur la plateforme. A partir de là, les participants étaient invités à répondre à cinq questions:

- quelles tendances associez-vous à l'intelligence ambiante? (question 1), les tendances peuvent être politiques, économiques, sociales, technologiques, écologiques ou juridiques, veuillez choisir de 1 à 3 éléments (consigne 1);
- quelles pourraient être les conséquences directes de la/des tendance(s) lambda (il y a ici une personnalisation de la/des tendance(s) compte tenu de la réponse faite à la question 1)? (question 2), veuillez choisir de 1 à 3 tendances (consigne 2);
- quelles pourraient être les conséquences directes de votre réponse ci-dessus? (question 3), vous devez entrer de 1 à 3 réponses pour chaque tendance (consigne 3);
- quelle opportunité ou menace vous paraît la plus importante? (question 4), vous devez ajouter un élément (consigne 4);
- afin de saisir cette opportunité ou faire face à cette menace, que devraient faire dès à présent... Les entreprises?... Les administrations publiques?... Les individus? (question 5).

Au moment de la préparation de l'étude (étape 1), 52 tendances tirées de documents identifiés sur le web ont été préenregistrées sur la plateforme Futurescaper. Des articles de presse, des études scientifiques ou professionnelles, des articles de blogs, et d'autres documents ont été identifiés puis analysés pour alimenter cette étape. C'est uniquement lorsque l'information contenue dans ces documents est arrivée à saturation [4] que le directeur de l'étude a consenti à passer à l'étape d'engagement (étape 2). À l'issue des étapes 2 et 3, les tendances étaient au nombre de 337.

La tendance «baisse de la protection de la vie privée» est celle qui a suscité le plus de recommandations (43 précisément). Trois autres tendances sont également à relever: la tendance «baisse de l'intelligence humaine» a suscité 25 recommandations, la tendance «hausse de l'addiction et de la dépendance aux objets connectés» en a suscité 21 et la tendance «hausse des cyberattaques et des piratages» en a suscité 15.

Sécurité et défense à la rencontre de l'Internet des objets, explorer les futurs possibles pour agir aujourd'hui

Le travail de production collaborative a permis d'identifier de nombreuses tendances originales (Tableau 1) qui sont venues compléter celles qui avaient été pré-enregistrées sur la plateforme Futurescaper (Tableau 2) avant le début de l'étude.

Politique	Chômage
Economique	Flux d'information, télétravail, nombre d'emplois, interactions machine/machine, performance logistique, automatisation, décisions prises directement par les machines et les objets, qualité du travail
Social	Interactions humaines, temps libre disponible, maintien et suivi à domicile des personnes âgées
Technologique	Hyper connectivité, télésurveillance, géolocalisation, confort, sécurité, traçabilité, identification des objets, observation de l'environnement, capacité d'action à distance, assistance à l'humain, brevets, autonomie des machines et des objets
Ecologique	Pollution, fluidité du trafic, consommation d'énergie, ondes électromagnétiques
Légal	Cyberattaques, protection des données, protection de la vie privée, échanges d'information, normes de sécurité, collecte de données, transparence

Tableau 1: tendances initiales

Exemples	Accidents de la route, activités en extérieur, addiction et dépendance aux objets connectés, apocalypse, bien-être, collaboration et entraide, confiance aveugle envers la technologie, méfiance vis-à-vis de l'État, conflits et guerres, création de nouvelles énergies, variété des emplois, exigence, fainéantise, médicalisation, société de contrôle, manipulation, spectateurs, individualisme, incompréhension, intelligence humaine et artificielle, isolement, dépression, paranoïa, insécurité, justice, perte de libertés individuelles, agilité, capitalisme, pauvreté, prévention, pression étatique, profits, substitution de l'homme par la machine, réalité virtuelle, sécurité, savoir, totalitarisme, humanoïde, violence, valeurs superficielles, équilibre vie privée/vie professionnelle, stupidité humaine, chantage, éducation, ennui, déqualification, disparition des entreprises, éthique, permanence, dépendance, sens de la vie, espérance de vie, ressources, créativité…

Tableau 2: quelques exemples de tendances finales originales

Ces tendances sont à la source d'une réflexion autour de futurs possibles pour la sécurité et la défense informatique et elles permettent d'établir quatre scénarios qui peuvent ainsi être proposés au débat (Figure 2). Ces scénarios sont construits autour des deux variables jugées les plus incertaines et dont on pense que l'évolution aura l'impact le plus élevé: la datafication [5] des individus et leur intérêt pour les objets connectés.

Scénario «défendre»

Un fort intérêt pour les objets connectés combiné avec une forte datafication des individus constitue la base du scénario «défendre» pour la sécurité et la défense informatique.

Dans ce scénario, les individus portent un regard enthousiaste sur les nouvelles technologies. Pour la plupart, ils sont devenus des utilisateurs experts des objets connectés et ils sont en mesure d'exploiter pleinement leur potentiel de véritables assistants personnels.

Les individus sont proactifs et transmettent volontiers les données qu'ils génèrent aux fabricants d'objets connectés, si possible en temps réel. Ils sont convaincus qu'il s'agit là du

meilleur moyen de contribuer à l'amélioration continue de l'expérience utilisateur.

Dans le scénario "défendre", l'objet connecté est devenu le prolongement naturel du corps humain. Dans le même temps, les individus ont développé une sorte de sympathie sincère vis-à-vis de l'intelligence ambiante que rend possible le déploiement des objets connectés. Cette intelligence ambiante rassure, accompagne et soutient.

Dans le scénario "défendre", les experts de la défense et de la sécurité font face à une question surprenante: que leur reste-t-il à faire? Qu'est-ce que la société attend d'eux?

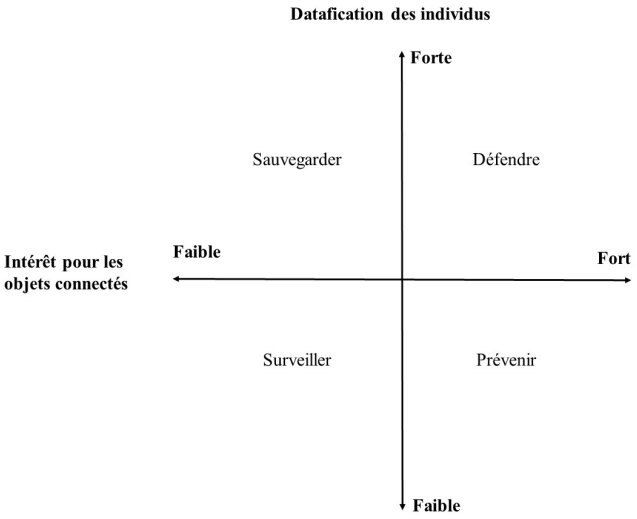

Figure 2: scénarios pour l'intelligence ambiante, la sécurité et la défense informatique

Scénario: «prévenir»

Un fort intérêt pour les objets connectés combiné avec une faible datafication des individus sont les deux piliers du deuxième scénario: «prévenir».

Tandis que les objets connectés s'accumulent, ils ne semblent apparemment ni offrir beaucoup de nouvelles opportunités, ni présenter de nouveaux risques. La raison? Personne ne semble être en mesure de transformer systématiquement les données collectées en informations et en connaissances actionnables.

Dans le scénario «prévenir», la question clé que se posent les experts de la défense et de la sécurité est la suivante: quand est-ce que les objets connectés réaliseront pleinement leur potentiel de transformation?

En conséquence, lesdits experts se doivent d'agir en utilisateurs précoces afin de se donner les moyens d'estimer le plus tôt possible les menaces et opportunités potentielles que véhiculent chaque nouvel objet ou nouvelle classe d'objets connectés.

Scénario «sauvegarder»

Un faible intérêt pour les objets connectés combiné avec une forte datafication des individus constitue la base du scénario «sauvegarder».

Dans ce scénario, les individus ne sont que modérément intéressés par les objets connectés, bien qu'ils continuent de contribuer individuellement et collectivement à générer des quantités sans cesse croissantes de données au travers de leurs nombreuses transactions quotidiennes qui n'impliquent pas nécessairement le recours à des objets connectés personnels.

Ces données ont le potentiel d'être converties en informations et en connaissances à haute valeur ajoutée.

Dans le scénario «sauvegarder», les données ainsi produites sont versées dans un "commun de connaissances" (knowledge commons), qui, à son tour, est mis à disposition des innovateurs afin de leur permettre d'accélérer le développement de leurs prototypes et de raccourcir les délais d'accès au marché. Les individus contribuent de manière consciente aux dynamiques d'innovation ouverte, lesquelles ont été adoptées largement par la plupart des acteurs dont les experts de la défense et de la sécurité informatique.

Dans le scénario «sauvegarder», c'est finalement une plus grande proximité entre individus et experts de la défense et de la sécurité informatique qui permet l'amélioration continue de la sécurité des données et des infrastructures ainsi que la conscience collective des enjeux liés au cyberespace. Ensemble, experts et individus se sentent concernés par le besoin d'établir et de maintenir des standards élevés en matière de cybersécurité à travers tout le territoire.

Scénario: «surveiller»

Un faible intérêt pour les objets connectés combiné avec un faible niveau de datafication des individus sont les deux piliers du quatrième et dernier scénario: «surveiller».

Dans ce scénario, les objets connectés en sont toujours au stade de gadgets.

La plupart des individus ont peur: ils craignent que tôt ou tard, une catastrophe surviendra. Ils se demandent: quand est-ce qu'un véhicule autonome et connecté sera hacké et causera la mort d'un ou plusieurs passants?

Dans le même temps, les personnes sont méfiantes à l'égard de grandes entreprises qui collectent, analysent et peut-être même revendent leurs données personnelles.

Du point de vue des experts de la défense et de la sécurité informatique, le scénario «surveiller» ne présente pas de difficultés particulières: personne ne remet en cause l'importance et la nécessité de surveiller en continu le trafic des données de sorte à détecter le plus rapidement possible les attaques et autres comportements frauduleux aux conséquences potentiellement catastrophiques.

Conclusion

Grâce à un travail collaboratif auquel ont participé un millier d'étudiant-e-s de toute la Suisse romande, nous disposons désormais de quatre scénarios prospectifs contrastés, riches des intuitions, des craintes et des espérances que portent les participant-e-s à la démarche.

Ces quatre scénarios ont vocation à servir de véritable "banc d'essai" sur lequel professionnels de la sécurité et de la défense, administrations publiques, associations etc. peuvent désormais tester un certain nombre d'options stratégiques, de choix politiques, d'arbitrages, etc.

Il s'agit, pour les organisations qui le souhaiteront, de répondre à quelques questions: mon choix stratégique est-il pertinent dans chacun des scénarios? Est-il efficient? Souhaitable?

Fortes des enseignements tirés de ce questionnement, les organisations pourront, au besoin, ajuster leurs choix stratégiques voire même repartir à zéro et envisager des options alternatives, jusqu'alors impensées.

En résumé, bâtir des scénarios prospectifs puis y tester des options stratégiques ou politiques, c'est se donner l'opportunité, à moindre frais, d'anticiper les impacts directs et indirects de décisions qui pourraient s'avérer capitales pour l'avenir de son organisation. Dans le secteur clé de la sécurité et de la défense, marqué par d'innombrables turbulences, incertitudes, contradictions, etc., il paraît fort sage d'institutionnaliser une telle démarche qui se révèle, dans la pratique, peu coûteuse au regard des gains stratégiques qu'elle procure.

S'il est nécessaire de citer un exemple, rappelons-nous l'épisode de la crise pétrolière de 1973 et la remarquable résilience dont l'entreprise Royal Dutch Shell a fait preuve ; une entreprise qui, depuis de nombreuses années déjà, avait inscrit dans son ADN le recours systématique aux scénarios prospectifs pour challenger les orientations stratégiques actuelles et envisagées.

Prof. Thomas Gauthier
est Professeur à la Haute école de gestion de Genève et à emlyon business school. Il débute sa carrière en tant qu'assistant de recherche à l'université Harvard. Il rejoint ensuite la société Philips où il occupe successivement les fonctions d'ingénieur, directeur de recherche clinique puis chercheur. Il est titulaire d'un doctorat en médecine expérimentale de l'Imperial College London et est également diplômé du Massachusetts Institute of Technology et de l'École Supérieure de Physique et Chimie Industrielles de Paris.

Dr. Sylvaine Mercuri Chapuis
est Enseignant-Chercheur en Sciences de Gestion à l'ESDES, The Business School of UCLy. Partenaire de la Haute école de gestion de Genève, ses travaux portent sur la Responsabilité Sociale des Organisations, la prospective stratégique et le management des ressources humaines. Elle est titulaire d'un doctorat de l'Université Jean Moulin Lyon 3 et elle est également diplômée de HEC Paris, de l'Helsinki Business Polytechnics School, de l'Université Savoie Mont-Blanc et l'École Nationale d'Assurance de Paris.

Liens & Explications

[1] https://www.newsd.admin.ch/newsd/message/attachments/47967.pdf, consulté en mai 2017.

[2] http://www.futurescaper.com, consulté en mai 2017.

[3] Au sein de la Haute Ecole Spécialisée de Suisse occidentale, la Haute Ecole de Gestion de Genève (HEG), la Haute École Arc (HE-Arc), la Haute Ecole du Paysage, d'Ingénierie et d'architecture de Genève (HEPIA), la Haute Ecole d'Art et de Design de Genève (HEAD), la Haute Ecole de Santé de Vaud (HESAV) ont été mobilisées. Des étudiants de l'école Changins, Haute Ecole de Viticulture et Œnologie ainsi que de l'Ecole Polytechnique Fédérale de Lausanne ont aussi participé à l'étude.

[4] La saturation des données est atteinte lorsqu'il n'y a plus d'information nouvelle dans les documents analysés.

[5] Étape qui consiste à passer de la donnée à l'information utile: «les assurances peuvent par exemple exploiter les données relatives aux déplacements des véhicules de leurs assurés afin d'établir des contrats qui soient le plus proche possible des risques réellement présentés par leurs clients (et non plus des contrats tenant compte de leur âge, de leur sexe et de l'historique de leur conduite)» (Chamaret, 2014; p. 95).

Bibliographie

- Von Bertalanffy, L. (1973), Théorie générale des systèmes, Paris: Dunod
- Chamaret, C. (2014), «La révolution big data», Annales des Mines - Gérer et comprendre, vol. 116, n°2, p. 94-96.
- Chevreau, F.-R., Wybo, J.-L. (2007), « Approche pratique de la culture de sécurité. Pour une maîtrise des risques industriels plus efficace », Revue française de gestion, vol. 5, n° 174, p. 171-189.
- Courrier international (2016), Automobile. Premier accident mortel pour la voiture autonome Tesla, 01 juillet, disponible sur http://www.courrierinternational.com/article/automobile-premier-accident-mortel-pour-la-voiture-autonome-tesla.
- David, A., Hatchuel, A. (2007) « Des connaissances actionnables aux théories universelles en sciences de gestion », AIMS, XVIème Conférence Internationale de Management Stratégique, Montréal.
- «Entretien», Distances et savoirs, vol. 7, n°3, p. 479-500.
- Freeman, R. E. (1984), Strategic management: a stakeholder approach, Boston: Pitman series in business and public policy.
- Frenchweb.fr (2011), 600 000 comptes Facebook victimes de tentatives de hacking chaque jour, 31 octobre, disponible sur http://www.frenchweb.fr/infographie-600-000-comptes-facebook-victimes-de-tentatives-hacking-chaque-jour-50227/32364.
- Godet, M. (2004), Manuel de prospective stratégique, tome 2: L'art et la méthode, Paris: Dunod.
- Godet, M., Durance, P. (2011), La prospective stratégique pour les entreprises et les territoires, Paris: Dunod.
- Johnson, G., Whittington, R., Scholes, K., Angwin, D., Regner, P., Fréry, F. (2017), Stratégique, 11ème édition, Paris: Pearson Education.
- Le Temps (2017), Le rançongiciel Wannacry a peu touché la Suisse, 15 mai, disponible sur https://www.letemps.ch/economie/2017/05/15/rancongiciel-wannacry-touche-suisse.