DU RISQUE DE "SECURITE DE L'INFORMATION" AU "RISQUE CYBER"

Emilie Peneloux, Thomas Des Grottes, Philippe Lepinard, Cécile Godé

▶ **To cite this version:**

Emilie Peneloux, Thomas Des Grottes, Philippe Lepinard, Cécile Godé. DU RISQUE DE "SECURITE DE L'INFORMATION" AU "RISQUE CYBER". Management & Data Science, 2024, 10.36863/mds.a.31882 . hal-04885216

HAL Id: hal-04885216

https://hal.science/hal-04885216v1

Submitted on 17 Jan 2025

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Distributed under a Creative Commons Attribution - NoDerivatives 4.0 International License

DU RISQUE DE « SECURITE DE L'INFORMATION » AU « RISQUE CYBER »

Emilie Peneloux Thomas des Grottes Philippe Lépinard Cécile Godé

CITATION

., ., Lépinard, P., & Godé, C. (Juil 2024). DU RISQUE DE « SECURITE DE L'INFORMATION » AU « RISQUE CYBER ». *Management et Datascience*, Article 0031882. https://doi.org/10.36863/mds.a.31882.

LES AUTEURS

1. Emilie Peneloux (emilie.peneloux@outlook.fr) - CERGAM
2. Thomas des Grottes (desgrottesthomas@gmail.com) - (Pas d'affiliation)
3. Philippe Lépinard (philippe.lepinard@u-pec.fr) - Institut de Recherche en Gestion (IRG, EA 2354)
4. Cécile Godé (cecile.gode@univ-amu.fr) - Aix-Marseille Université CERGAM - ORCID : https://orcid.org/0000-0002-9148-2820

COPYRIGHT

© 2024 les auteurs. Publication sous licence Creative Commons CC BY-ND.

DÉCLARATION D'INTÉRÊTS

Le ou les auteurs déclarent ne pas avoir connaissance de conflit d'intérêts impliqués par l'écriture de cet article.

FINANCEMENTS

Le ou les auteurs déclarent ne pas avoir bénéficié de financement pour le travail mis en

jeu par cet article.

APERÇU

Une confusion sémantique réside entre « risques de sécurité de l'information » et « risques cyber » dans la littérature académique spécialisée. A partir d'une revue descriptive, nous interrogeons les terminologies employées afin de préciser l'état de l'art dans le champ. Nous montrons des différences de périmètre entre ces notions et un manque de définition unifiée, et aussi que l'emploi de la composante « cyber » semble rapprocher les mondes académique et professionnel. Forts de ces constats, nous émettons des recommandations pour de futures recherches.

CONTENU

Les cyberattaques exploitent les vulnérabilités d'un actif d'information ou d'un groupe d'actifs d'information pour causer des dommages à une organisation en termes de disponibilité, d'intégrité et de confidentialité. Selon le Baromètre Euler Ermes – Allianz Trade, près de 70% des entreprises ont essuyé une tentative de cyberattaque en 2022 et 55% d'entre elles ont subi une fraude avérée. En 2021, le préjudice des cyberattaques était supérieur à 10.000 euros pour 33% des entreprises victimes, et s'élevait à plus de 100.000 euros pour 14% d'entre elles.

La cybersécurité porte ainsi des enjeux majeurs, dont le monde professionnel s'est amplement emparé. De nouveaux métiers émergent ainsi pour assurer la gestion du risque cyber, allant du Responsable pour la Sécurité des Systèmes d'Information (RSSI) au responsable cybersécurité· Parallèlement, de nombreuses instances sont créées, menant à bien une mosaïque de missions au sein de cadres juridiques et de structures organisationnelles publiques, privées, civiles et militaires (Chaudhary et al., 2018 [https://doi.org/10.1093/cybsec/tyy005]). Face à ces initiatives, le monde académique n'est pas en reste. Débutées à la fin des années 1960, les recherches en cybersécurité évoluent depuis, discutant tout à la fois de risque de sécurité de l'information, de risque cyber ou de cybersécurité (Eling et al., 2021 [https://onlinelibrary.wiley.com/doi/epdf/10.1111/rmir.12169]).

Une confusion sémantique réside cependant entre ces types de risques (de Sagazan, 2020 [https://www.editions-ellipses.fr/accueil/10392-initiation-a-la-cybersecurite-9782340038011.html]) alors même que des auteurs insistent sur l'importance de les distinguer (von Solms et van Niekerk, 2013 [https://www.sciencedirect.com/science/article/abs/pii/S0167404813000801?via%3Dihub] ; Salomon, 2020 [https://www.editions-ellipses.fr/accueil/10762-cybersecurite-et-cyberdefense-enjeux-strategiques-9782340042414.html]) et que le marché, notamment de la cyber-assurance, le réclame également (Baldoni, 2022 [https://www.sciencedirect.com/science/article/pii/S1874548222000622?via%3Dihub]). Nous cherchons ici à identifier quelle terminologie est employée pour caractériser le risque de cybersécurité dans les revues académiques, pour quels objectifs et domaines d'application ?

Description de la littérature académique

Le risque pour la sécurité de l'information

Nous recensons 84 articles comportant « *Information security risk* » dans leur titre, répartis sur 59 revues majoritairement à destination d'un public académique, et publiés entre 1997 à 2023, selon la répartition suivante :

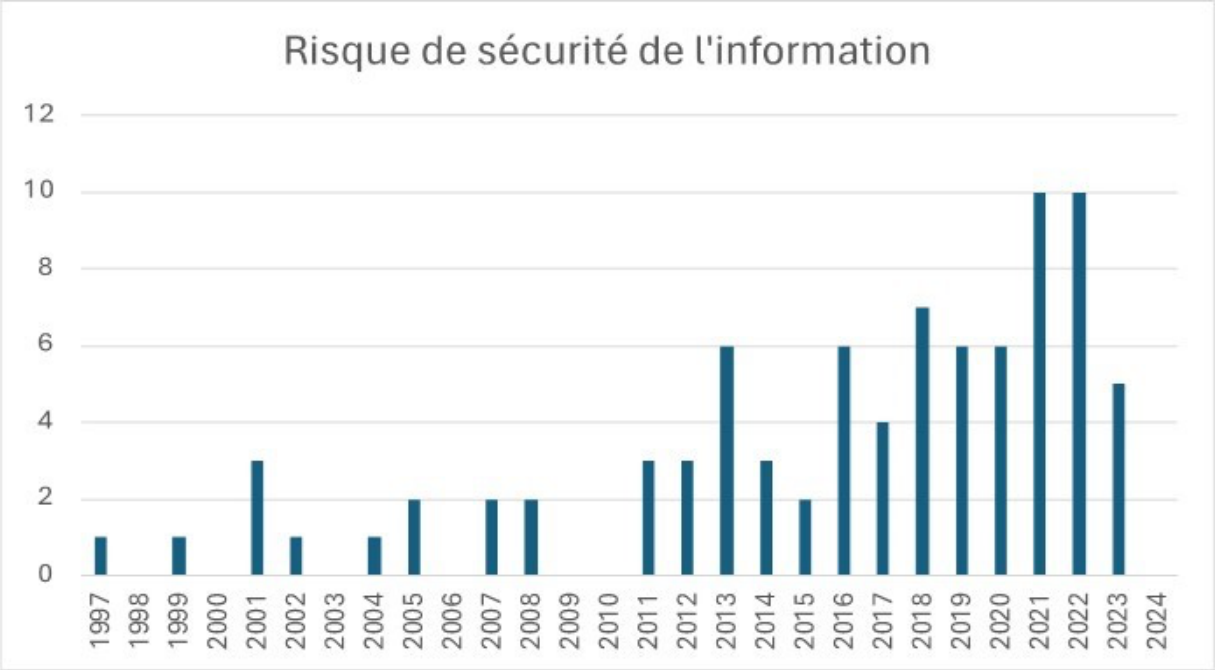

Figure 1. Évolution chronologique des articles sur le risque de sécurité de l'information

Les articles se penchant sur la notion de risque de sécurité de l'information peuvent être présentés selon 13 catégories (rassemblant au moins deux articles) indiquant les objectifs et domaines d'applications des travaux :

Catégories	Descriptions et sous-catégories	Nombre d'articles
Evaluation des cyber-risques	Méthodes d'évaluation quantitatives et/ ou qualitatives des risques	51
Gestion des cyber-risques	Management, bonnes pratiques, contrôles de sécurité, mitigations, aide à la décision	27
Système cyber-physique	Smart city, secteur de la santé, pipeline, objets connectés, secteur de l'énergie, usines de production chimique	21
Individus	Perception des risques ; comportements, sensibilisation, motivation	11
Nouvelles infrastructures	Environnement cloud, Big Data, digitalisation, intelligence artificielle	7
Modélisation	Facteurs de risques, impacts des risques	6
Revue de littérature	Revue de littérature académique sur des thématiques ou des méthodes	6
Direction	Concerne la direction d'une organisation	4
Assurance	Concerne la couverture d'assurance pour les incidents de sécurité	3
Gouvernement	Application au gouvernement, au cyberespionnage, organisations publiques	3
Ressources	Investissement	2
Conformité	Réglementaire	2
Approche globale	Mise en avant de la nécessité d'une approche globale	2

Tableau 1. Catégories associées aux articles sur le risque de sécurité de l'information et de ses systèmes

Les risques cyber et de cybersécurité

Nous recensons 193 articles de revues comportant « *Cyber risk* » dans leur titre. Ces articles sont répartis entre 128 revues à destination d'un public académique et professionnel, et publiés entre 2002 à 2024, selon la répartition suivante :

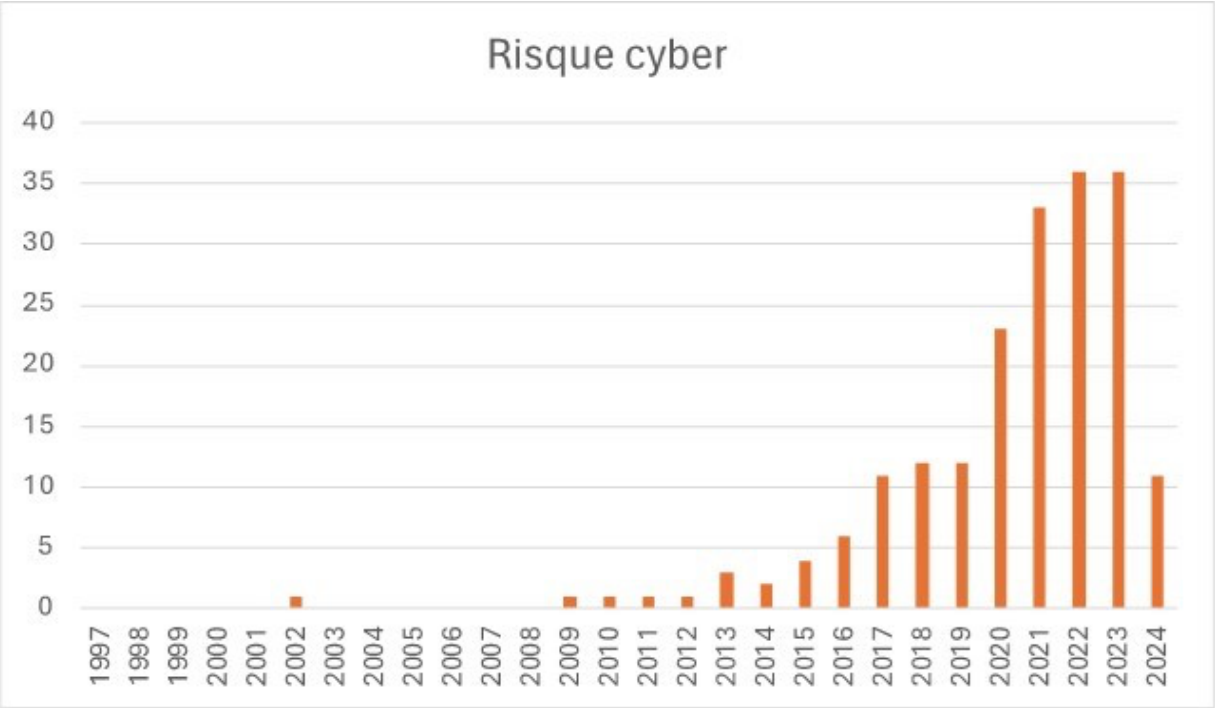

Figure 2 : Évolution chronologiques des articles sur le « risque cyber »

Seuls 50 des définissent le risque cyber, soit 26% d'entre eux, mais la plupart l'aborde comme synonyme de cyberattaque. Nous identifions 23 catégories (rassemblant au moins deux articles) indiquant les objectifs et domaines d'applications des travaux :

Catégories	Descriptions et sous-catégories	Nombre d'articles
Gestion des cyber-risques	Management, bonnes pratiques, contrôles de sécurité, mitigations	83
Evaluation des cyber-risques	Méthodes d'évaluation quantitatives et/ ou qualitatives des risques	74
Caractéristiques du risque	Dynamique, socio-technique, systémique, multi-dimensionnel, incertitude	52
Systèmes cyber-physique	Infrastructures critiques, secteur de l'énergie, eau, pipeline, objets connectés, secteur maritime, secteur de la santé, secteur du transport	72
Assurance	Couverture pour les incidents cyber, bonnes pratiques	36
Revue de littérature	Appliquées à un secteur en particulier, des méthodes ou des pratiques, revue académique, revue professionnelle	30
Individus	Comportements, acteurs, victimes, atteinte physique et morale, identité numérique, perception des risques, cyber-harcèlement, sensibilisation	23
Modélisation	Facteurs de risques, conséquences, scenarii d'attaque	20
Nouvelles infrastructures	Utilisation de l'intelligence artificielle, application à l'intelligence artificielle, blockchain, environnement cloud, digitalisation	19
Approche globale	Gouvernance globale, approche pluri-disciplinaire, approche inter-disciplinaire, multi-disciplinaire	19
Institutions financières	Application au domaine des institutions financières	17
Ressources	Investissement, allocation de ressources	17
Gouvernement	Appliqué au domaine du gouvernement, cyberdéfense, acteur, militaire, cyber-guerre, cyber-terrorisme	11
Direction	Concerne le comité de Direction d'une organisation	11
Conformité	Réglementaire, législation	7
Attaquant	Motivation, parcours	6
Contexte	Contexte socio-culturel, contexte géopolitique, contexte économique	5
Commerce	Application au domaine du commerce (dont e-commerce)	5
Supply chain	Application au domaine de la supply chain	4
Définition	Redéfinition des concepts	4
Finance	Impact financier	3
Juridique	Cabinet d'avocats	2
E-sport, jeux en ligne	Appliqué au domaine des jeux en ligne	2

Tableau 2 : Catégories associées aux articles sur le « risque cyber »

Concernant les articles de revues comportant « *Cybersecurity risk* » dans leur titre, nous en recensons 151, répartis sur 106 revues à destination d'un public académique et professionnel, et publiés entre 2004 à 2024, selon la répartition suivante :

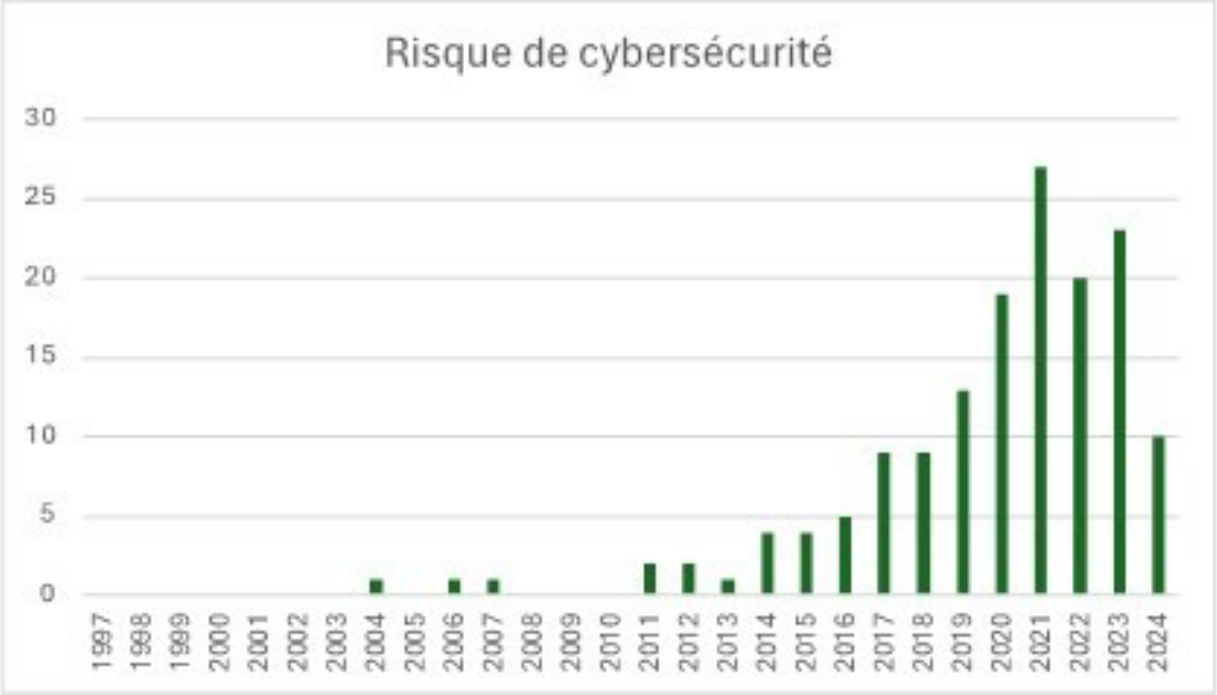

Figure 3 : Évolution chronologiques des articles sur le « risque cybersécurité »

Le risque de cybersécurité est seulement défini dans 28 des articles notre échantillon (soit 15%), renvoyant, comme pour le risque cyber, à la cyberattaque. Nous identifions 24 catégories (rassemblant au moins deux articles) indiquant les objectifs et domaines d'applications des travaux :

Catégories	Descriptions et sous-catégories	Nombre d'articles
Gestion des cyber-risques	Management, bonnes pratique, contrôles de sécurité, mitigations, aide à la décision	64
Evaluation des cyber-risques	Méthodes d'évaluation quantitative et/ ou qualitatives des risques	57
Systèmes cyber-physique	Infrastructures critiques, secteur de l'énergie, eau, pipeline, secteur de la santé, secteur du maritime, objets connectés, secteur du transport, secteur de l'aviation, smartphones, système de contrôle industriel, smart city	49
Individus	Comportements, acteurs, victimes, atteinte physique et morale, identité numérique, perception des risques, cyber-harcèlement, sensibilisation, réseaux sociaux	24
Revue de littérature	Appliqué à un secteur en particulier, des méthodes ou des pratiques, revue académique, revue professionnelle	17
Modélisation	Facteurs de risques, conséquences, scenarii d'attaque	15
Nouvelles infrastructures	Utilisation de l'intelligence artificielle, application à l'intelligence artificielle, blockchain , environnement cloud	14
Divulgation	Traite de l'obligation de divulgation ou de ses conséquences	14
Caractéristiques du risque	Dynamique, socio-technique, systémique, multi-dimensionnel, incertitude	13
Approche globale	Gouvernance globale, approche pluri-disciplinaire, approche inter-disciplinaire, multi-disciplinaire	11
Institutions financières	Application au domaine des institutions financières et plus largement au secteur de la finance	11
Ressources	Investissement, allocation de ressources	7
Gouvernement	Appliqué au domaine du gouvernement, cyberdéfense, acteur, militaire	6
Finance	Impact financier, coûts	6
Audit	Audit de sécurité cyber	6
Assurance	Couverture, bonnes pratiques	5
Direction	Concerne le comité de Direction d'une organisation ou la prise de décision de haut niveau	4
Conformité	Réglementaire, législation	4
Responsabilités	Responsabilités des dirigeants, des entreprises ou des managers	4
Commerce	Application au domaine du commerce (dont e-commerce)	2
Supply chain	Application au domaine de la supply chain	2
Enseignement supérieur	Application au domaine de l'enseignement supérieur	2
Stratégie	Stratégie, innovation, appropriation	2
Définition	Redéfinition des concepts	2

Tableau 3 : Catégories associées aux articles sur le « risque cybersécurité »

Analyse des résultats

Les articles comportant les termes « risque pour la sécurité de l'information », « risque de cybersécurité » et « risque cyber » poursuivent sensiblement les mêmes objectifs – à savoir de méthodologies de gestion du risque ou d'évaluation du risque – appliqués à des domaines tels que : les systèmes cyber-physiques (secteur de la santé, du maritime, de l'énergie, utilisation des objets connectés, etc.), les institutions financières

ou encore les nouvelles infrastructures (blockchain, intelligence artificielle, cloud).

Une première différence entre les contributions semble chronologique, les notions de cybersécurité et de risques cyber étant employées plus récemment que celle de risque de sécurité de l'information, comme le montre la Figure 4 :

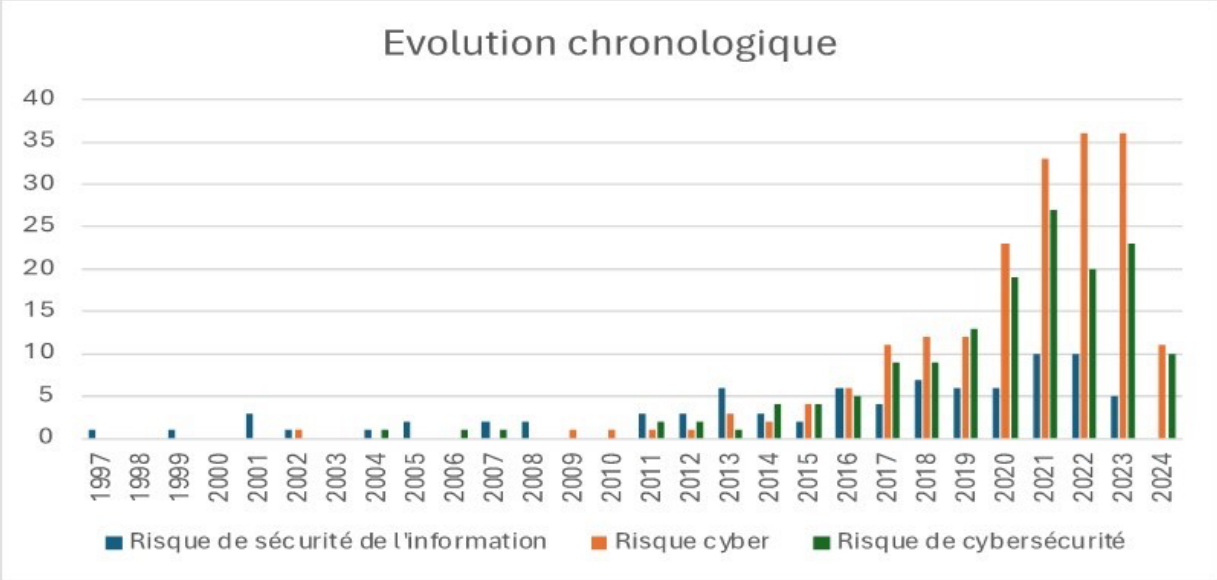

Figure 4 : Évolution chronologiques des terminologies employées

Les articles « cyber » soulignent la nécessité d'une approche globale et multidisciplinaire du risque en insistant sur ses aspects systémiques, multidimensionnels, sociotechniques et dynamiques. Cela se retrouve également dans les domaines d'application étudiés, qui sont nombreux et variés, là où les travaux portés sur le « risque de sécurité de l'information » sont plus génériques et moins ancrés dans les problématiques concrètes des professionnels. Ceci est certainement lié au fait que les articles « cyber » sont publiés dans des revues dont la cible est à la fois académique et professionnelle. Les thématiques vont alors se concentrer sur l'identification de bonnes pratiques de gestion du risque, de solution d'assurance, de gestion de divulgation d'incidents ou d'allocation des ressources. En cela, si l'absence de définition commune du risque cyber révèle une notion encore en construction autour de l'idée cyberattaque, la composante « cyber » semble rapprocher les mondes académique et professionnel.

Recommandations pour de futures recherches

Nos travaux révèlent l'importance d'une construire une définition unifiée et partagée du risque cyber, qui permettrait une meilleure appréhension de la notion par les différentes parties prenantes du paysage cyber. Cela implique de redéfinir les frontières entre les deux types de risque, « sécurité de l'information » et « cyber ». Des travaux adoptant le paradigme du *Design Science* (Simon, 2004 [https://www.amazon.fr/Sciences-lartificiel-Herbert-Simon/dp/2070301524]) et ancrés dans la transdisciplinarité (Romme, 2003 [https://pubsonline.informs.org/doi/10.1287/orsc.14.5.558.16769]) pourraient

être mobilisés pour produire des connaissances communes (Dresch et al., 2014 [https://books.google.fr/books/about/Design_Science_Research.html?id=pBtRBAAAQBAJ&redir_esc=y]) et favoriser la co-construction, par les monde académique et professionnel, d'une notion encore en devenir.

BIBLIOGRAPHIE

Baldoni, R. (2022). Managing the cyber risk in a multipolar world. *International Journal of Critical Infrastructure Protection*, 39(C), https://doi.org/10.1016/S1874-5482(22)00062-2 [https://doi.org/10.1016/S1874-5482(22)00062-2]

Chaudhary, T., Jordan, J., Salomone, M. D., et Baxter, P. (2018). Patchwork of Confusion: The Cybersecurity Coordination problem. *Journal of Cybersecurity*, 4(1). https://doi.org/10.1093/cybsec/tyy005 [https://doi.org/10.1093/cybsec/tyy005]

de Sagazan, C. (2020). *Introduction à la cybersécurité*. Ellipses.

Dresch, A., Pacheco Lacerda, D., et Valle Antunes, J. (2014). *Design Science Research*. Genève: Springer.

Eling, M., McShane, M., et Nguyen, T. (2021). Cyber risk management: History and future research directions. *Risk Management and Insurance Review*, 24(1), 93-125. https://doi.org/10.1111/rmir.12169 [https://doi.org/10.1111/rmir.12169]

Romme, A. G. L. (2003). Making a difference: Organization as design. *Organization Science*, 14(5), 558-573. https://doi.org/10.1287/orsc.14.5.558.16769 [https://doi.org/10.1287/orsc.14.5.558.16769]

Salomon. (2020). *Cybersécurité, cyberdéfense : Enjeux stratégiques*. Ellipses.

Simon, H. (2004). *Les sciences de l'artificiel*. Folio Essais : Paris.

Von Solms, R. et van Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, 38, 97-102. https://doi.org/10.1016/j.cose.2013.04.004 [https://doi.org/10.1016/j.cose.2013.04.004]

© 2025 - Management & Data Science - https://management-datascience.org - Tous droits réservés