APPEL À COMMUNICATIONS

Journée d'études du Groupe Thématique « Risque, Incertitude et Organisation »
de l'AIMS

Hyper-digitalisation et "(dé)risquification" des organisations : quels enjeux pour la résilience organisationnelle ?

5 mai 2026
Paris (lieu précisé ultérieurement)

Devenu incontournable, le numérique façonne profondément nos sociétés occidentales et en trace la trajectoire. Régissant un nombre croissant d'aspects de la vie quotidienne (e-commerce, plateformes de divertissement, dématérialisation des procédures administratives, objets connectés, réseaux sociaux, etc.), il s'impose comme un pilier de l'organisation des infrastructures et des acteurs qui les gouvernent. États, entreprises, citoyens et consommateurs redéfinissent en permanence leur "champ des possibles", au rythme des innovations qui ouvrent la voie à de nouvelles technologies, services et usages. L'avènement de l'intelligence artificielle pousse cette « ère de la digitalisation » à son paroxysme, renforçant l'idée d'une société largement dominée par la technique (Ellul, 1988).

Comme d'autres technologies avant elles, ces mutations reflètent autant qu'elles transforment notre rapport aux risques et à leur gestion (Beck, 1992). Fidèle à la promesse d'un accès plus ouvert et direct à l'information, ainsi qu'au décuplement de nos capacités, l'hyper-digitalisation offre de nombreuses opportunités pour améliorer la gestion des risques. Pour les experts (gestionnaires de risque, auditeurs, ingénieurs, régulateurs, etc.), le big data et les algorithmes pourraient permettre d'affiner les prévisions, de repérer les signaux faibles et d'adopter une vision plus systémique, mieux à même d'appréhender la complexité des risques (Marsden & Steyer, 2025). L'anticipation et le pilotage des risques "connus" n'ont ainsi jamais été aussi robustes. Mais au-delà de cet affinage des expertises, le numérique peut aussi constituer un outil d' "encapacitement" pour le grand public : il horizontalise les rapports entre citoyens, usagers et consommateurs, et ouvre la voie à des formes de coordination émergente en situation de crise. Les réseaux sociaux ont ainsi parfois permis de structurer une solidarité entre habitants sur des territoires touchés par des catastrophes naturelles (Alexander, 2014). De plus, mise à la disposition du grand public, l'intelligence artificielle peut contribuer à réduire certaines barrières entre experts et profanes.

Mais ces "progrès" s'accompagnent aussi de nombreuses controverses. Tout en simplifiant la vie des individus, l'hyper-digitalisation introduit un niveau d'hyper-surveillance et d'hyper-contrôle de masse, atteignant - voire dépassant - les scénarios anticipés par la science-fiction. Les technologies numériques génèrent également de nouvelles incertitudes : usages détournés (e.g., cyberattaques), addictions, perte de compétences, dévalorisation du travail humain, déshumanisation des relations sociales, bouleversement de secteurs et métiers, fracture numérique. Dans un contexte de gestion des risques, le numérique exacerbe des formes de perte de vigilance, de surcharge cognitive, de dépendance excessive à l'IA, de dilution de la responsabilité humaine, etc. (Endsley, 2023; Gmyrek, Berg & Bescond, 2023; Pasquale, 2015; Vuarin & Steyer, 2025; Waardenburg, 2024). De nouveaux risques (Hardy & Maguire, 2020) émergent ainsi inexorablement à mesure que la digitalisation s'immisce dans tous les aspects du fonctionnement des organisations. Par ailleurs, la transition vers le "tout-numérique" plonge la société et ses institutions dans un état de vulnérabilité inédit, lié à la complexité des systèmes (e.g., difficulté à maîtriser intégralement la "boîte noire" technologique), à

la dépendance aux ressources énergétiques (e.g., risque de coupure électrique prolongée ou généralisée), et aux impacts environnementaux considérables induits par l'augmentation structurelle des besoins numériques (Marsden & Steyer, 2025). Enfin, l'apparition de nouveaux "objets à risque" (Hilgartner, 1992) - tels que les robots humanoïdes, les plateformes d'accès à l'IA générative ou les véhicules autonomes - soulève des questions inédites de responsabilité et d'éthique (e.g., à qui incombe la responsabilité d'une défaillance ou d'un dommage causé par une IA ?). La régulation de ces enjeux demeure encore largement embryonnaire.

L'objectif de cette journée d'étude du GT AIMS RIM (Risque Incertitude et Management) est ainsi d'explorer cet impact ambivalent de l'hyper-digitalisation sur les risques et leur gestion au sein des organisations. Nous invitons ainsi des travaux souhaitant explorer plus largement l'articulation entre digitalisation, risque et résilience. Les travaux présentés lors de cette journée pourront par exemple s'articuler autour des thématiques suivantes (non exhaustives) :

Thème 1. Le rôle de la digitalisation et des technologies "intelligentes" dans l'anticipation et le pilotage des risques en organisation

- En quoi et sous quelles conditions les technologies de digitalisation et l'IA favorisent-elles l'anticipation et le pilotage des risques ?
- Comment la matérialité des dispositifs numériques (capteurs, IA, plateformes collaboratives, dashboards, etc.) influe-t-elle sur la manière dont les risques sont identifiés, hiérarchisés et traités ?
- Comment la multiplication des données génère paradoxalement des zones d'ignorance ou d'invisibilisation des risques (biais algorithmiques, données manquantes, opacité des modèles) ?
- Comment se structurent les rapports humain-machine dans la gestion des risques "augmentée" par l'IA ? Comment reconfigurent-ils les dynamiques organisationnelles ?
- Quelles sont les nouvelles formes de désorganisation liées à la « surcharge attentionnelle » dans des environnements hyper-digitalisés ? Peut-on concevoir des dispositifs de gouvernance de l'attention organisationnelle à l'ère de l'hyper-digitalisation ?
- Quelles sont les nouvelles méthodes pour appréhender les risques très incertains (e.g., risques environnementaux, risques géopolitiques, risques à très long terme,...) induites par les avancées technologiques ?

Thème 2. Gestion de crise, résilience des organisations et outils digitaux

- Quels rôles jouent les technologies digitales dans l'anticipation et la réponse aux crises ?
- Dans quelle mesure la digitalisation constitue-t-elle un vecteur de démocratisation de la gestion de crise ?
- Comment l'abondance d'informations générées par les outils numériques reconfigure-t-elle les processus de *sensemaking* en situation de crise ? Dans quelle mesure les technologies numériques facilitent ou brouillent la construction de sens partagé au sein des organisations ?
- En quoi l'IA transforme-t-elle les formes de coordination et les rapports de force dans les processus de gestion de crise ?
- Quel lien entre hyper-digitalisation et résilience des organisations, aux échelles individuelles, organisationnelles et territoriales ?

Thème 3. Hyper-digitalisation des organisations et nouvelles incertitudes

- Quelles vulnérabilités et incertitudes l'IA et l'hyper-digitalisation introduisent-elles ?
- Comment les acteurs ajustent leurs pratiques face à des incertitudes numériques (cyberattaques, défaillances algorithmiques, biais des IA) ?

- Comment les acteurs ajustent leurs pratiques face à des incertitudes numériques (cyberattaques, défaillances algorithmiques, biais des IA) ?
- Comment appréhender les mécanismes de surveillance, de contrôle ou de dépendance introduits par l'omni-présence accrue des algorithmes ?
- Quels enjeux éthiques et de régulation les nouvelles technologies introduisent-elles ? Quels processus de construction sociale du risque les sous-tendent ?
- Comment la numérisation transforme-t-elle les dispositifs de valorisation et de mesure du risque (indicateurs, scoring, rating, tableaux de bord automatisés) ? Dans quelle mesure ces instruments participent-ils à une illusion de maîtrise, masquant certaines incertitudes radicales ?
- Quels formats de justification et d'épreuves de légitimité sont mobilisés pour arbitrer les choix de gestion des risques en contexte hyper-digitalisé ?

Objectifs de la journée

Le groupe thématique encourage les travaux à forte dimension théorique, méthodologique ou empirique, qui proposent de renouveler les approches classiques des formes d'action collective organisée à l'aune des risques et des incertitudes contemporains, en considérant les apports de travaux plus récents. On pourra notamment penser aux travaux s'inscrivant dans les perspectives suivantes (liste non exhaustive) : sensemaking, attention-based view, sociologie pragmatique, valuation studies, approches « practice » variées (avec un intérêt certain pour l'étude de la matérialité), approches discursives/CCO, sociologie des controverses, agnotologie.

Plusieurs types de contribution sont ainsi attendus, qu'ils soient théoriques, méthodologiques, épistémologiques et / ou empiriques, et dès lors qu'ils adressent de manière explicite les notions de risque, de résilience en lien avec les technologies.

Afin de permettre une réelle discussion des papiers, le nombre de places, incluant les contributeurs, est limité.

Procédure de soumission

La sélection des communications se fera sur la base d'un résumé étendu, d'une longueur de 3000 mots maximum (bibliographie comprise). Il présentera l'intérêt du sujet, décrira le contenu de l'article et résumera la contribution. Les résumés étendus en anglais sont possibles. Cependant les présentations et les discussions de la journée se feront en français.

Calendrier

- Date limite de soumission des résumés étendus : **13 février 2026**
- Retour des avis aux communicants : **16 mars 2026**
- Envoi de la version finale de la communication : **17 avril 2026**

Les résumés et les versions finales sont à envoyer par courriel à :
veronique.steyer@polytechnique.edu ; julie.mayer@univ-rennes.fr ;
geoffrey.leuridan@imt-atlantique.fr ; nour.kanaan@univ-lille.fr

Frais d'inscription

La journée ne comporte pas de frais d'inscription. Les frais de transport et de restauration sur place (déjeuner) seront à la charge des participants. Pour les non-adhérents à l'AIMS, il faut y ajouter l'adhésion à l'association (30€, 15€ pour les doctorants) voir https://www.strategie-aims.com/adherents

Comité d'organisation de la journée

Véronique Steyer (i3-CRG, Ecole polytechnique), Julie Mayer (CREM, Université de Rennes), Geoffrey Leuridan (IMT Atlantique), Nour Kanaan (Université de Lille).

Références

Alexander, D. E. (2014). Social media in disaster risk reduction and crisis management. *Science and engineering* ethics, 20(3), 717-733.

Beck, U. (1992). *Risk society: Towards a new modernity. Sage Publications, Londres.*

Ellul, J. (1988). Le bluff technologique. Hachette, Paris.

Endsley, M. R. (2023). *Ironies of artificial intelligence.* Ergonomics, 66(11), 1656-1668.

Gmyrek, P., Berg, J. et Bescond, D. (2023). *Generative AI and jobs: A global analysis of potential effects on job quantity and quality*. Rapport technique, ILO. doi: 10.54394/FHEM8239.

Hardy, C., Maguire, S., Power, M., & Tsoukas, H. (2020). Organizing risk: Organization and management theory for the risk society. *Academy of management annals*, 14(2), 1032-1066.

Hilgartner, S. 1992. *The social construction of risk objects: Or, how to pry open networks of risk. In Organizations, uncertainties, and risk*, ed. J.F. Short and L. Clarke, 39–53. Boulder, CO: Westview Press.

Marsden E. & Steyer V. (2025), *Artificial intelligence and safety management: an overview of key challenges.* Number 2025-03 of the Cahiers de la Sécurité Industrielle, Foundation for an Industrial Safety Culture, Toulouse, France

Pasquale, F. (2015). *The Black Box Society: The Secret Algorithms That Control Money and Information*. Harvard University Press. isbn: 978-0674970847, 260 pages.

Vuarin, L. & Steyer, V. (2025). La résilience organisationnelle face à l'intelligence artificielle: Examen critique du concept de human in the loop en action. *Innovations*, 76(1), 239-276.

Waardenburg, L. (2024). Human-AI collaboration: A blessing or a curse for safety at work? Tecnoscienza – *Italian Journal of Science & Technology Studies*, 15(1):133–146.