AIDES
A LA REFLEXION

Penser la complémentarité humains-technologies en contexte

Futurs défis pour la sécurité dans les organisations à risque

Corinne Bieder

Rédaction coordonnée par Caroline Kamaté

n° 2024-03

THÉMATIQUE

Opérateur du futur

Les Cahiers de la sécurité industrielle

FONCSI
Fondation pour une culture de sécurité industrielle

La Fondation pour une Culture de Sécurité Industrielle (Foncsi) est une Fondation de recherche reconnue d'utilité publique par décret en date du 18 avril 2005. Elle a pour ambitions de :

- contribuer à l'amélioration de la sécurité dans les entreprises industrielles de toutes tailles, de tous secteurs d'activité ;
- rechercher, pour une meilleure compréhension mutuelle et en vue de l'élaboration d'un compromis durable entre les entreprises à risques et la société civile, les conditions et la pratique d'un débat ouvert prenant en compte les différentes dimensions du risque ;
- favoriser l'acculturation de l'ensemble des acteurs de la société aux problèmes des risques et de la sécurité.

Pour atteindre ces objectifs, la Fondation favorise le rapprochement entre les chercheurs de toutes disciplines et les différents partenaires autour de la question de la sécurité industrielle : entreprises, collectivités, organisations syndicales, associations. Elle incite également à dépasser les clivages disciplinaires habituels et à favoriser, pour l'ensemble des questions, les croisements entre les sciences de l'ingénieur et les sciences humaines et sociales.

FONCSI
Fondation pour une culture de sécurité industrielle

Fondation pour une culture de sécurité industrielle
Fondation de recherche reconnue d'utilité publique

http://www.foncsi.org/

6 allée Émile Monso – CS 22760
31077 Toulouse Cedex 4
France

Téléphone : +33 (0) 532 093 770
X : @LaFonCSI
Email : contact@foncsi.org

Ce document

Titre	Penser la complémentarité humains-technologies en contexte
Sous-titre	Futurs défis pour la sécurité dans les organisations à risques
Mots clés	Sécurité ; numérique ; intelligence artificielle ; humain ; technologie ; incertitude
Auteur	Corinne Bieder
Date de publication	Avril 2024

Ce *Cahier de la sécurité industrielle* est issu de l'analyse stratégique de la Foncsi « Opérateur du futur-Génération des travailleurs à venir 2030-2040 ». Ce projet a rassemblé un noyau de chercheurs académiques qui participe aux travaux de la Foncsi de longue date, ainsi que des experts scientifiques issus des organisations qui soutiennent la fondation. Ils se sont réunis une quinzaine de fois avec pour objectif d'explorer les impacts qu'ont les mégatendances qui traversent notre monde et nos sociétés sur la sécurité des organisations à risque. Ce cahier se focalise sur le rôle des humains et sur leur relation aux technologies.

À propos de l'auteure

Corinne Bieder est docteure en sociologie et sciences de gestion. Ingénieure de formation, elle détient également un mastère spécialisé en management du risque et un DESS en ergonomie. Après avoir travaillé chez EDF, Dédale et Airbus, elle a rejoint l'ENAC où elle est responsable du programme de recherche en management de la sécurité. Elle a été membre académique du groupe scientifique d'analyse stratégique (GSAS) de la Foncsi, et en est depuis 2024 la directrice scientifique.

Pour citer ce document

Corinne Bieder (2024). *Penser la complémentarité humains-technologies en contexte – Futurs défis pour la sécurité dans les organisations à risque*. Numéro 2024-03 de la collection Les *Cahiers de la sécurité industrielle*, Fondation pour une culture de sécurité industrielle, Toulouse, France.

Librement téléchargeable sur : www.foncsi.org

Résumé

La rapidité d'évolution des technologies numériques bouleverse le paysage de l'industrie à risques conventionnelle, introduisant de nouveaux défis pour la sécurité. Ce document se focalise sur le rôle joué par l'homme à l'horizon 2030-2040 dans la gestion et la gouvernance de la sécurité. Il met en évidence l'impact du cadre implicite adopté pour appréhender les contributions respectives des humains et des technologies numériques à la sécurité des industries à risques. Alors qu'un cadre centré sur l'humain souligne comme essentielles à la sécurité des capacités spécifiquement humaines telles que l'empathie, la compréhension, le jugement…, un cadre centré sur la technologie met en avant la puissance et la vitesse de calcul comme atouts pour la sécurité industrielle de demain. Aucun de ces cadres opposant humains et technologies numériques ne semble approprié pour rendre compte de situations réelles où les deux coexistent et interagissent de manière plus complexe que via les seules interfaces humains-machines. De plus, ces situations s'inscrivent dans un contexte plus global, social, politique, organisationnel et culturel, appelant à nuancer des affirmations absolues sur la Technologie et l'Humanité. Plus généralement, le fonctionnement des industries à risques est complexe. Penser en termes de dichotomies (par exemple, technologie vs humain ; numérique vs non numérique) se révèle trop simpliste pour anticiper les défis qui nous attendent en matière de sécurité. Explorer les interrelations entre les humains et les technologies numériques implique d'étudier le contexte dans lequel les deux catégories évoluent pour cadrer de manière pertinente les potentiels futurs défis de sécurité. Cela implique que, pour refléter une réalité complexe, il faille convoquer diverses perspectives et disciplines pour rapprocher humains et technologies et les envisager dans leur contexte.

Mots-clés : sécurité ; numérique ; intelligence artificielle ; humain ; technologie ; incertitude ; risque

Avant-propos

Lorsque cette analyse stratégique a débuté en 2019, nous, à la Foncsi, l'avons surnommée en interne « L'opérateur du futur ». Elle visait en effet principalement l'impact des évolutions technologiques et sociétales anticipées sur le rôle futur des opérateurs de première ligne dans la sécurité des opérations industrielles. Ce sujet a effectivement été traité. Mais il a été largement dépassé.

Cela était dû, évidemment, à de profonds changements dans le monde lui-même. En 2019, le SRAS-COV-2 était encore l'apanage obscur de quelques chauves-souris exotiques (sinon le captif secret d'un labo de « haute sécurité »…). L'Ukraine n'était pas en guerre. Et la « crise énergétique » n'avait pas encore soufflé sur le grand public la petite brise prémonitoire du cataclysme écologique que l'humanité a réussi à fabriquer. Et bien sûr : Chat-GPT n'existait pas encore.

Mais une deuxième raison est que les analyses stratégiques de la Foncsi partagent avec d'autres activités de recherche une caractéristique bien connue : lorsqu'elles réussissent, elles suivent rarement le chemin prévu. Et cette analyse a été particulièrement féconde. Dans la présente synthèse, Corinne Bieder le capte remarquablement. Elle élargit le regard bien au-delà de la dichotomie traditionnelle, inspirée de la liste de Fitts, entre les humains et la technologie. Et même au-delà de la perspective, plus récente, de l'interaction entre les humains et la technologie.

Elle pousse la leçon de l'analyse stratégique à son essence même et à son implication pluridisciplinaire - et quasi philosophique : la sécurité est un comportement émergent de nos sociétés complexes, une construction sociale, politique, culturelle, émotionnelle – et récursive – de ce comportement. Elle nous met en garde contre la tentation des simplifications illusoires. Un avertissement plus indispensable que jamais par temps de turbulente incertitude.

Jean Pariès
Ancien directeur scientifique, Icsi-Foncsi

Sommaire

Introduction

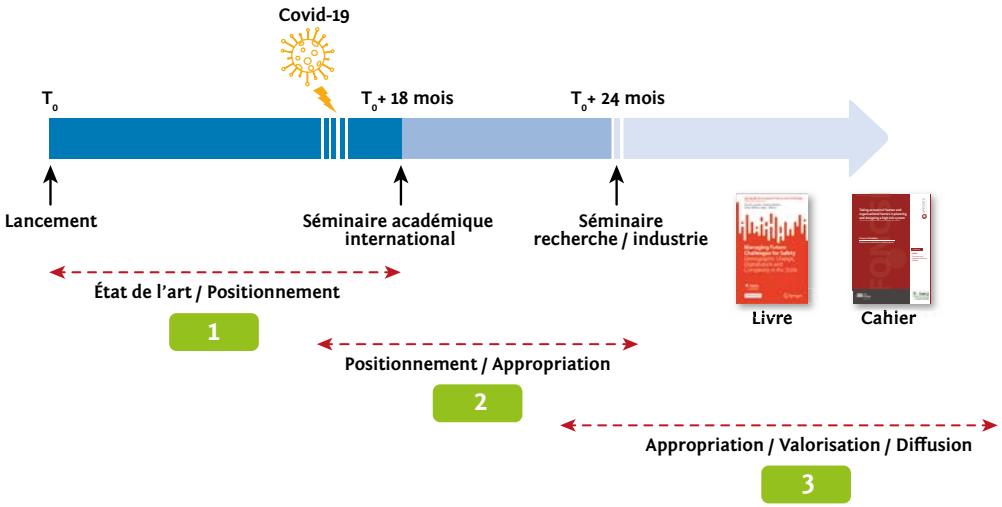
Contexte

L'idée de ce document, tout comme son contenu, sont principalement issus d'une analyse stratégique menée entre 2019 et 2021 par la Foncsi (Fondation pour une culture de sécurité industrielle) sur le rôle de l'homme (des hommes en réalité) dans la sécurité des industries à risques à l'horizon 2030-2040. L'objectif de ce travail était non seulement d'examiner comment certaines mégatendances sont susceptibles d'affecter le monde, et notamment l'industrie, dans les décennies à venir, mais aussi de réfléchir à la manière dont ces évolutions pourraient impacter le rôle de l'homme dans la sécurité de l'industrie de demain. Parmi ces tendances figure l'accélération du développement des technologies numériques et les nombreux impacts actuels et à venir sur l'évolution du monde (Okhrimenko, Sovik, Pyankova, & Lukyanova, 2019). Dans les industries à risques, certaines des questions soulevées par cette évolution technologique étaient déjà apparues avec le développement et la généralisation de l'automatisation. Cependant l'intelligence artificielle, tout en ouvrant la voie à de nouvelles opportunités, s'accompagne de nouveaux enjeux. Bien que la contribution des humains à la sécurité des industries à risques soit actuellement largement reconnue (même si certaines problématiques liées aux facteurs humains, organisationnels et culturels subsistent) (Roe & Schulman, 2008 ; Daniellou, Simard, & Boissières, 2011), l'avènement d'une technologie censée être « intelligente » pourrait remettre en question cette assertion.

L'analyse stratégique en un clin d'œil

L'analyse stratégique « Opérateur du futur-Génération des travailleurs à venir 2030-2040 » a émergé des préoccupations rapportées par les organisations mécènes de la Foncsi (secteurs industriels de l'énergie et des transports, autorités de régulation et autres organismes). Ce projet, mené par le groupe scientifique d'analyse stratégique (GSAS) de la Foncsi, visait à générer une recherche de qualité dans un délai relativement court et à créer un continuum entre la recherche, l'innovation et l'industrie. Comme les précédentes analyses stratégiques de la Foncsi, ce projet comprenait 3 grandes étapes (décrites dans la figure ci-dessous) :

1. **État de l'art**. Il s'agit d'établir un panorama de la littérature, de préparer un plan d'analyse, de reformuler le problème et d'identifier les experts internationaux qui contribuent à la thématique de l'analyse stratégique. Cette première étape est marquée par un temps fort, un séminaire de recherche avec les chercheurs internationaux identifiés et invités par le GSAS. Ce séminaire fournit l'essentiel du matériel scientifique sur lequel s'appuie un ouvrage collectif.
2. **Appropriation**. Le GSAS s'approprie les résultats du séminaire international et confronte théories et concepts aux pratiques en vigueur dans l'industrie. Cette étape se termine par un séminaire de restitution et d'échange rassemblant chercheurs et partenaires industriels.
3. **Transfert**. La Foncsi assure la diffusion des résultats de la recherche ainsi que leur traduction pour un public de praticiens au travers de différentes publications : un ouvrage académique collectif en anglais et des rapports de synthèse tels que les *Cahiers de la sécurité industrielle*. Conformément au statut d'utilité publique de la Foncsi, toutes les publications sont librement téléchargeables.



Bien entendu, tout comme pour de nombreuses activités, le calendrier de l'analyse stratégique a été perturbé par la crise du Covid-19.

Au-delà de ces jalons « classiques », la Foncsi a organisé dans le cadre de cette analyse stratégique un atelier prospectif sur la sécurité ferroviaire du futur. L'objectif était de susciter un débat entre experts reconnus du rail et de proposer des pistes pour se préparer à de futurs problèmes de sécurité dans le ferroviaire en 2030 et au-delà. Les personnalités ayant participé à cet événement sont les suivantes :

- François Davenne, directeur général de l'UIC (Union internationale des chemins de fer) ;
- Loïc Dorbec, président de l'AGIFI (Association française des gestionnaires d'infrastructures ferroviaires indépendants) ;
- Yann Leriche, directeur général de Getlink (Eurotunnel, Europorte, ElecLink et CIFFCO) ;
- Pierre Messulam, directeur risques sécurité-sûreté du Groupe SNCF ;
- Dominique Riquet, député européen, membre de la Commission des transports et du tourisme.

Les échanges ont été animés par Pierre-Franck Chevet, président de IFP Energies Nouvelles et Jean Pariès, directeur scientifique de la Foncsi et de l'Icsi.

Le groupe scientifique d'analyse stratégique

Le projet a été piloté par le Groupe Scientifique d'Analyse Stratégique (GSAS) de la Foncsi, et coordonné par Caroline Kamaté. Ce dernier est constitué d'un noyau permanent de chercheurs et de la direction de la Foncsi qui participent à toutes les analyses stratégiques :

- René Amalberti, Foncsi, France
- Corinne Bieder, ENAC, France
- Hervé Laroche, ESCP Business School, France
- Jean Pariès, Foncsi/Icsi, France
- Jesús Villena López, Ergotec, Espagne

Sur ce thème particulier, le comité a été renforcé par des experts des organisations partenaires de la Foncsi, largement reconnus dans le domaine de la sécurité et des risques :

- Florence Reuzeau, Airbus, France
- Raluca Ciobanu, EDF, France
- Laurent Cebulski & Bruno Dember, EPSF, France
- Franck Ollivier, Eurovia, France
- Nicolas Engler & Thierry Escaffre, GRTgaz, France
- Dounia Tazi, Icsi, France
- Alexandre Largier & Tania Navarro Rodriguez, IRSN, France
- Stella Duvenci-Langa & Cyril Cappi, SNCF, France
- Raphaël Waxin, TotalEnergies, France

Les experts internationaux

Pour cette analyse stratégique, les perturbations liées à la crise du Covid 19 ont empêché la tenue d'un séminaire académique résidentiel. Les sept experts internationaux listés ci-dessous ont donc présenté leurs travaux lors d'un événement organisé à distance en novembre 2020 :

- John Allspaw, Adaptive Capacity Labs, USA
- Stian Antonsen, Université norvégienne de science et technologie (NTNU), Norvège
- Michael Baram, Université de Boston, USA
- Flore Barcellini, CNAM, France
- Gérard de Boisboissel, Centre de recherche de l'Académie militaire de Saint-Cyr Coëtquidan, France
- Steven Shorrock, Eurocontrol, Royaume-Uni et France
- Akira Tosé, Université de Niigata, Japon.

La visée principale de ce séminaire était de confronter les points de vue, d'induire de stimulants débats et de proposer des pistes d'amélioration. L'objectif final était de rassembler ces éléments dans un livre collectif, publié dans la collection en libre accès « SpringerBriefs in Safety Management ». Ce dernier est sorti en octobre 2022, sous le titre « *Managing future challenges for safety* » (H. Laroche, C. Bieder ; J. Villena-Lopez (Eds), 2022).

Ce document : structure et objectifs

Ce document aborde plus spécifiquement la thématique suivante : comment conjuguer humanité et technologie pour assurer la sécurité des industries à risques dans les décennies à venir ?

Il débute avec une question fondamentale soulevée par une technologie qui tend à devenir plus « humaine » : qu'est-ce qui fait de nous des humains ? Il existe une littérature abondante sur ce qui distingue l'humain des autres espèces, mais réfléchir au rôle des humains dans la sécurité des industries à risques de demain amène une question quelque peu différente : qu'est-ce qui fait de nous des humains, et qui, par rapport aux nouvelles technologies numériques, est singulier pour contribuer à la sécurité ?

Tenter d'apporter une réponse à cette question en soulève une autre, traitée ensuite dans le document : sur quelles bases les capacités singulières des humains et/ou des technologies sont-elles évaluées ?

Dans la vie quotidienne, et plus encore dans les industries à risques, les humains et les technologies n'existent pas isolément les uns des autres. Le document se poursuit donc par une description des interdépendances qui existent entre humanité et technologie, et engage une réflexion sur la façon de les rapprocher et de les envisager ensemble, en interrelation, de manière cohérente, du niveau opérationnel aux niveaux organisationnels, sociétaux et même philosophiques.

Pour en savoir plus

Nous renvoyons le lecteur intéressé à la partie bibliographie en fin de document, et notamment aux autres publications de l'analyse stratégique « Opérateur du futur-Génération des travailleurs à venir 2030-2040 » :

- le livre en anglais publié en libre accès chez Springer en octobre 2022 ;
- la synthèse de l'atelier ferroviaire publiée en mai 2021, téléchargeable gratuitement sur le site de la Foncsi.

1

Une tendance à opposer humain et technologie

Tenter d'identifier les propriétés ou caractéristiques spécifiquement humaines n'est pas nouveau. Au siècle des Lumières, une « *tendance générale s'est installée pour définir les êtres humains comme étant hors nature, et le rationalisme des Lumières a conduit à une vision d'un environnement dominé par la technologie* » (Williams, 2020). Les anthropologues ont également fait, et font toujours de gros efforts pour identifier ce qui fait de nous des êtres humains, en particulier par rapport aux singes [voir par exemple (Pollard, 2009)].

Avec les progrès de la médecine, des biotechnologies et l'avènement de l'ère « post-humaine », la même question s'est posée sous un angle différent. Dans cette tentative de comparaison de l'homme à d'autres espèces ou d'autres éléments, le progrès technologique, exacerbé ces dernières années par le développement du numérique, semble avoir généré une autre référence à laquelle l'homme tente de se comparer. Norman (2014) souligne que l'évolution de la société a promu une perspective centrée sur la machine ; il appelle à inverser ce point de vue et à en adopter un autre centré sur l'humain. En cela, il perpétue la tradition d'opposer humains et machines, comme s'il était essentiel de « prendre parti » pour l'un ou pour l'autre, de les penser forcément séparément.

Au cours de notre réflexion sur le rôle des humains dans la sécurité des industries à risques de demain, les qualités spécifiquement humaines ont également été largement mentionnées. La plupart d'entre elles sont similaires à celles évoquées au moment de l'introduction des systèmes automatisés, mais d'autres ont été introduites pour des raisons différentes. Shorrock (2022), en analysant les micro récits de professionnels de la santé à la suite de la pandémie de Covid 19, met en évidence, à titre d'exemple, la mobilisation des capacités suivantes pour faire face à des situations plutôt imprévisibles : « *la capacité à anticiper les défis potentiels nécessite de l'imagination et une compréhension approfondie des réalités du travail quotidien* » ou « *l'intelligence collective via une collaboration inclusive et une communication ouverte* » pour prévenir les dommages aux patients et aux travailleurs de la santé. L'auteur cite également des travaux antérieurs sur ces capacités uniques : Cook (2020), « *Les praticiens humains sont l'élément adaptable des systèmes complexes* », et « *Le système continue de fonctionner parce qu'il comporte de nombreuses redondances et parce que les gens peuvent le faire fonctionner, malgré la présence de nombreux défauts* » ou Dekker (2015, p. vi), « *les personnes comme source de diversité, de perspicacité, de créativité et de sagesse en matière de sécurité, et non comme source de risques qui minent un système par ailleurs sûr* ». L'anticipation, l'imagination, l'intelligence collective, l'adaptabilité, la diversité, la perspicacité, la créativité et la sagesse apparaissent comme des caractéristiques spécifiques à l'homme et essentielles à la sécurité. Boucher (2019), cité par Antonsen (2022) enrichit cette liste de capacités humaines uniques en mentionnant ce qui manque à la technologie de l'IA : « *Elle n'est pas vivante, elle n'a pas de conscience, et elle est complètement incapable de comprendre, de faire montre de créativité ou d'empathie* ». Les principaux aspects qui rendent ces capacités critiques pour la sécurité incluent les nombreux défauts des systèmes, mais aussi leur complexité et leur imprévisibilité.

En revanche, plusieurs propriétés spécifiques aux machines sont mises en avant par les technologues, la première étant leur puissance de traitement de l'information. Selon le contexte, d'autres sont également évoquées comme la capacité à effectuer des tâches physiquement difficiles, dangereuses ou bien répétitives et ennuyeuses. Dans les activités à risques, les spécificités des technologies qui sont souvent alléguées sont l'absence d'erreur, la rapidité de réaction ou la disponibilité opérationnelle 24h/24 (De Boisboissel, 2022), autrement dit la fiabilité et la régularité de la performance ainsi que sa reproductibilité.

Bien que ces deux points de vue apparaissent inconciliables, rappelons que les dichotomies tendent à simplifier la réalité. Aller au-delà de cette compréhension limitée de l'humanité et de la technologie, dépasser le discours général, réducteur, sur les humains d'un côté et les machines de l'autre, nécessite de faire le lien entre les qualités uniques respectives des humains ou des machines, et les contextes dans lesquels elles sont pertinentes ou requises. L'exemple développé par Norman (2014) sur la distractibilité propre à l'homme en constitue une bonne illustration. L'auteur montre qu'il est à la fois important de ne pas se laisser distraire lors de l'exécution de certaines tâches, mais que, pourtant, la distractibilité est aussi ce qui peut permettre à l'opérateur humain de remarquer de nouveaux événements dans l'environnement qui l'entoure, ce qui peut être tout aussi critique,

sinon plus, notamment pour la sécurité des activités à risques. Expliciter le contexte et le référentiel par rapport auxquels les propriétés sont évaluées est essentiel pour approfondir la réflexion.

2

Le cadre implicite sous-jacent à l'évaluation

Parmi les conséquences de l'adoption d'un point de vue techniciste privilégié par la société, Norman (2014) souligne que les machines deviennent la référence par rapport à laquelle tout est évalué. Les humains ne font pas exception, ils sont ainsi jugés sur des propriétés mécaniques et calculatoires. Parmi les exemples courants, on citera la comparaison des capacités de traitement de l'information respectivement de l'IA et de l'humain, ou bien le fait que les machines ne font pas d'erreurs (ou plus précisément que les humains commettent des erreurs, contrairement aux machines).

À l'inverse, des qualités humaines telles que l'empathie, l'adaptabilité, la créativité, la sagesse – qualités qui, jusqu'à présent, sont absentes chez les machines – ne sont identifiées et reconnues que dans un référentiel spécifique à l'homme. Il n'est pas surprenant qu'en utilisant des référentiels différents, on arrive à des conclusions, des positionnements et des propositions différentes.

Antonsen (2022), en rendant explicite le domaine d'utilisation, introduit une certaine nuance dans la manière d'appréhender les qualités ou capacités des humains et des algorithmes. Il distingue deux types de tâches. Tout d'abord celles comportant peu de variabilité comme les actions simples et les décisions récurrentes où les algorithmes représentent « *la préprogrammation statique de connaissances expertes* ». Dans ce premier cas, l'auteur confirme que la première génération d'IA, pilotée par l'homme, peut alléger les tâches routinières, ainsi que d'autres plus complexes, effectuées par l'humain. Pour le deuxième type de tâches, où bonnes ou mauvaises solutions ne peuvent pas toujours être facilement ni identifiées, ni gérées par des règles et un codage simple, les conclusions ne sont pas si évidentes. Et ceci malgré une deuxième génération d'algorithmes d'IA basés sur les données, s'appuyant sur l'apprentissage automatique et les réseaux de neurones. Bien que dans IA, il y ait le terme « intelligence », l'auteur appelle à en distinguer différentes formes. La première catégorie est l'intelligence spécialisée et étroite, qui fait référence à l'exécution parfaite d'une tâche particulière telle que la reconnaissance faciale ou l'obéissance à une commande vocale. Antonsen nous rappelle que ce type d'IA « *ne peut appliquer l'intelligence qu'aux problèmes spécifiques pour lesquels elle est programmée* ». La seconde est l'intelligence physique, qui lie les compétences mentales et motrices. L'auteur souligne que pour ce type d'intelligence, l'effort investi dans l'IA et les performances qu'elle atteint sont sans commune mesure avec ce qui peut être réalisé par n'importe quel humain, prenant l'exemple de robots « courant » sur un terrain accidenté. Il souligne que « *bien que notre capacité de traitement de l'information dans des domaines étroits puisse être limitée, notre répertoire d'actions dans le monde physique n'est pas particulièrement limité, puisque nous pouvons improviser avec tous les outils et informations dont nous disposons*[1] » (Antonsen, 2022). Enfin, la dernière catégorie d'intelligence, le « bon sens », fait référence à « *la capacité d'interpréter et de comprendre pratiquement n'importe quelle situation et d'apprendre à agir en situation* ». Cela implique un certain nombre d'aptitudes telles que la compréhension contextuelle d'une situation sociale, la recherche de sens ou la capacité à « *faire les bonnes suppositions dans des situations rarement rencontrées et sur la base d'informations incomplètes* ». Malgré le développement accéléré de l'IA, ces qualités, jugées critiques pour la sécurité par l'auteur, restent uniques à l'homme et ne sont pas encore, du moins jusqu'à présent, accessibles aux algorithmes.

La distinction entre ces différentes tâches, entre ces formes d'intelligence multiples, permet à Antonsen de nuancer des affirmations générales telles que la supériorité de l'IA sur l'homme en matière de capacité de traitement de l'information, en insistant sur la forme spécifique d'intelligence à laquelle elle s'applique, à savoir « *sur des domaines étroitement définis, où il y a des données suffisantes et où des situations similaires se reproduisent sans cesse* » (Antonsen, 2022). Dans ces cas, remplacer des humains par des machines peut avoir une valeur significative, d'autant plus lorsque cela protège les humains de l'exposition à des situations dangereuses, comme les soldats sur un champ de bataille par exemple, ou bien quand cela permet une activité permanente et continue, comme le précise De Boisboissel (2022).

1. "Nous" et "notre" se référant aux humains en général (NDT).

Cependant, les situations opérationnelles réelles dépassent généralement ces domaines. Revenir à ce que la tâche, ou plus généralement la situation exige, est nécessaire pour éviter de tirer des conclusions hâtives et approximatives sur les humains et les technologies numériques.

3

Conjuguer humanité et technologie dans les industries à risques

3.1 Questions opérationnelles

Dans les industries à risques, les qualités singulières respectivement des humains et des machines sont pertinentes et sont sollicitées au plus haut point compte tenu de la complexité des situations et de leurs conséquences potentielles. Du point de vue de la sécurité, il est aussi essentiel pour un humain de remarquer certaines choses dans son environnement de travail et d'être capable de les interpréter comme nécessitant un changement de mode de performance ou de plan d'action que, pour une machine, d'effectuer une tâche répétitive de manière fiable. L'existence d'incertitudes dans les opérations est largement reconnue même si cela ne se traduit pas nécessairement par des stratégies formelles de gestion de la sécurité. Certaines de ces incertitudes sont liées à la conception même de la technologie et dues à l'incomplétude des connaissances sous-jacentes, aux limites inévitables du modèle du monde utilisé comme référence, comme le soulignent Downer (2011 ; 2020). Avec le développement des technologies numériques et plus particulièrement des algorithmes d'IA capables d'apprendre et de modifier progressivement leurs « comportements », les incertitudes sont d'autant plus flagrantes que certaines sont créées par la technologie elle-même. Par conséquent, opérer en toute sécurité avec ces (nouvelles) incertitudes nécessite plus que jamais l'intelligence du « bon sens » telle qu'introduite par Antonsen (2022), ainsi que des qualités propres à l'homme telles que l'adaptabilité, la créativité ou le discernement en matière de sécurité.

Plus généralement, bien que partiellement autonomes, les algorithmes d'IA auto-apprenants nécessitent toujours l'intervention humaine en opération[2]. Même dans des domaines technologiques avancés comme le militaire, où les atouts des robots sont largement reconnus notamment pour limiter les risques d'exposition humaine, toute action requiert un leader ainsi que des opérateurs humains. De Boisboissel (2022) en expose les raisons :

« Le leader est la clé humaine de toute action militaire. Il lui donne un sens, il reste responsable de la manœuvre et de la façon dont la guerre est menée et il s'adapte « en conduite » en fonction des événements ».

« L'opérateur a la meilleure conscience de la situation et, si la machine peut faire des calculs probabilistes, la probabilité ne tient pas compte de la complexité des situations militaires sur le champ de bataille qui nécessitent une analyse humaine ».

Cependant, plutôt que d'opposer les humains et les machines, les opérations les rassemblent en tant qu'acteurs qui collaborent entre eux.

Au regard des impacts potentiels liés à la sécurité des opérations dans les activités à risques, la confiance apparaît comme l'un des défis majeurs induits par cette collaboration. De Boisboissel (2022) souligne l'importance de la confiance pour que les militaires utilisent des systèmes auto-apprenants. Avec ces systèmes, on dépasse la traditionnelle question de confiance dans la technologie qui fût soulevée aux débuts de l'automatisation : la confiance dans ces algorithmes adaptatifs concerne non seulement leur conception et leur développement, mais aussi leur apprentissage et tout ce que cela implique en termes de données[3]. La transparence est généralement mise en avant comme un moyen d'instaurer la confiance. *« Les systèmes adaptatifs et auto-apprenants doivent pouvoir expliquer leurs raisonnements et leurs décisions aux opérateurs humains de manière transparente et compréhensible »* (De Boisboissel, 2022), Antonsen (2022) désigne cela comme un « paradoxe de la transparence », paradoxe qui devra être résolu avant que l'IA sophistiquée ne soit introduite dans les processus critiques pour la sécurité des industries à risques. « *Lorsque les algorithmes apprennent, ils deviennent acteurs du management de la sécurité.*

2. Faire fonctionner des technologies numériques nécessite en arrière plan un effort humain invisible, mais significatif.
3. Le développement d'algorithmes et la formation sont d'autres opportunités de rapprocher l'humain (les data scientists en l'occurrence) et les technologies numériques comme nous le verrons plus loin.

C'est un principe de base des HRO (Organisations à Haute Fiabilité) et de la plupart des approches de management de la sécurité que les décisions et actions importantes soient vérifiées et revérifiées ». (Antonsen, 2022).

Outre la question que cela génère de la confiance dans les algorithmes eux-mêmes, l'utilisation massive de technologies numériques engendre de nouveaux types de vulnérabilités, notamment les risques de cyberattaques. Cet aspect est brièvement développé dans le premier Cahier issu de l'analyse stratégique qui synthétise les impacts des mégatendances sur l'avenir de la sécurité dans les industries à risques (GSAS - Opérateur du futur, 2023).

3.2 Questions organisationnelles et questions de conception

L'avènement de l'IA de deuxième génération soulève des questions non seulement sur la collaboration entre les humains et les technologies en opération, mais également à des niveaux plus organisationnels. Elle induit des changements organisationnels ou étend le champ de la conception, affectant ainsi les interrelations entre humains/organisations et technologies numériques avancées.

3.2.1 Multiplication et diversification des parties prenantes nécessitant davantage de coordination

Les algorithmes auto-apprenants impliquent une coordination non seulement entre les systèmes numériques ou entre les humains et les systèmes numériques, mais aussi entre les organisations, et par suite, entre les humains agissant davantage sur les décisions de haut niveau qu'en première ligne opérationnelle. Les organisations qui contribuent au fonctionnement des systèmes à risques figurent parmi les premières à coordonner. On assiste à une multiplication et à une diversification des organisations supports indispensables aux opérations, avec notamment de nouveaux entrants tels que les développeurs de logiciels[4], les fournisseurs de services de communication ou les fournisseurs de données. La fragmentation des organisations qui a commencé il y a des décennies s'est amplifiée non seulement en nombre, mais aussi en diversité. Étant donnée leur dépendance vis-à-vis de ces nouvelles activités et organisations associées qui ne font pas partie de leur industrie en tant que telle, les industries à risques deviennent, de facto, plus ouvertes. À cet égard, la propagation des technologies numériques conduit à brouiller les frontières industrielles. Ainsi, la sécurité devient une préoccupation d'importance variable selon les organisations impliquées (plus ou moins directement) dans les opérations. Outre le besoin accru de coordination, la multiplication des organisations concernées pourrait conduire à une atomisation et éventuelle perte ou transfert de responsabilités. La situation pourrait devenir encore plus complexe. En effet, certains algorithmes sont disponibles gratuitement sur internet sans qu'aucune organisation soit identifiée derrière. À un autre niveau encore, lorsque des capacités (par exemple, des algorithmes ou des satellites de communication) d'un autre pays sont utilisées pour exploiter un système à risques, les conditions géopolitiques peuvent avoir un impact direct sur le fonctionnement du système. Ces vulnérabilités s'ajoutent à l'augmentation des cyber-risques dus à l'ouverture de systèmes numériques avancés comprenant notamment des capteurs, des capacités de transmission, des algorithmes ou des packages parfois accessibles à tous.

Un autre défi en lien avec l'introduction dans le périmètre des industries à risques de systèmes et d'organisations numériques spécialisés, est celui des compétences. Comme l'a indiqué l'un des experts ayant participé à l'atelier ferroviaire mentionné dans l'introduction du cahier, les systèmes numériques sont aujourd'hui développés par des personnes qui connaissent mal le système ferroviaire et ses caractéristiques physiques. La déconnexion entre industries à risques et entreprises du numérique désincarne la conception de la partie IA des systèmes technologiques. Cela pourrait s'avérer encore plus critique si les compétences nécessaires pour vérifier et valider/approuver les systèmes développés par des entreprises du numérique ne sont pas disponibles au sein des organisations à risques et que ces activités sont déléguées à un tiers (impliquant une partie prenante supplémentaire). Cette situation pose à nouveau la question de la responsabilité et de l'obligation de « rendre compte »[5], qui peut devenir encore plus complexe dans certains cas où les algorithmes sont développés dans des pays où la réglementation diffère de celle applicable dans le pays d'implémentation.

3.2.2 Représentation du monde basée sur les données

Outre le faible degré de familiarité des développeurs de logiciels avec les opérations, la conception d'algorithmes auto-apprenants implique un aspect qui n'existait pas dans les technologies précédentes, à savoir les données. Comme nous le rappelle Antonsen (2022), une première caractéristique des algorithmes auto-apprenants est qu'ils ne peuvent être développés que dans des domaines où des données peuvent être collectées, et en quantité

4. Un grand nombre de failles dans les algorithmes sont détectées et corrigées en temps réel par des myriades de développeurs de logiciels.

5. Ces aspects seront abordés plus loin dans cette section 3.3

suffisante. Le type de données sur lesquels ces algorithmes s'appuient représente un deuxième élément crucial. Enfin, le résultat de ces algorithmes dépendra fortement des données d'apprentissage. Par exemple, un algorithme de traitement du langage naturel entraîné sur des données générales disponibles sur le Web (du texte dans ce cas), peut conduire à des résultats différents de ceux obtenus par le même algorithme entraîné sur un texte spécifique à un domaine (par exemple le ferroviaire, le nucléaire, l'aéronautique…). Antonsen (2022), citant Parmiggiani, Østerlie, & Almklov (2022) rappelle que, « *les données sont rarement 'découvertes' comme des faits objectifs et analysées comme telles - elles sont à la fois sélectionnées et préparées avant d'être disponibles pour analyse* ». Ainsi, les données choisies façonnent les algorithmes ou introduisent des biais comme l'indique encore Antonsen (2022). « *Dans les contextes critiques pour la sécurité, nous ne pouvons pas nous permettre d'ignorer le fait que les données seront biaisées, que leur caractérisation contient des biais et que les algorithmes d'apprentissage peuvent créer leur propre ensemble de biais. Il n'y a par conséquent aucune raison de croire que l'IA supprime la faillibilité humaine. Elle remplace une forme de faillibilité humaine par une autre.* »

Par conséquent, de la même manière que les concepteurs intègrent dans la technologie leur modèle limité du monde, les data-scientists intègrent dans les algorithmes d'IA une représentation du monde restreinte aux données, au travers à la fois des données disponibles et collectées en quantité suffisante, et des données sélectionnées pour entraîner les algorithmes. Les algorithmes d'IA produisent ensuite des résultats utilisés par des personnes autres que les concepteurs ou les développeurs, personnes qui, à leur tour, construisent sans même en avoir conscience leurs représentations sur ces bases-là. La transparence des algorithmes comme condition nécessaire pour établir la confiance dans les systèmes auto-apprenants pourrait donc englober non seulement ce que font les algorithmes, mais aussi sur quelle base et pour quelles raisons ils le font.

3.3 Questions sociétales

3.3.1 Réglementation et gouvernance

Dans le cas des industries à risques, la question de la transparence des algorithmes d'IA et de la confiance qu'on leur accorde n'est pas l'affaire des seuls opérateurs ou dirigeants de l'organisation dans le contexte opérationnel ; c'est également celle de l'ensemble de la société qui pourrait être affectée par les conséquences potentielles sur la sécurité d'un accident. À ce titre, ces algorithmes posent question en matière de gouvernance. Ces préoccupations sont d'autant plus urgentes que les approches traditionnelles de réglementation et de contrôle ne s'appliquent pas aux algorithmes auto-apprenants ni, plus généralement, aux systèmes dont le comportement évolue dans le temps ou qui sont imprévisibles. Le modèle de contrôle qui, historiquement, sous-tend la certification des systèmes (qui est l'un des piliers de la gouvernance de la sécurité) a ignoré la variabilité de la performance humaine malgré les nombreuses illustrations et documentations existantes. La certification s'appuyait (et s'appuie toujours) sur des analyses et essais probabilistes de sécurité jugés suffisants pour anticiper le niveau de sécurité des dispositifs technologiques et de leur utilisation. Il est désormais communément reconnu que le comportement des algorithmes auto-apprenants ne peut pas être prédit, ce qui met en évidence les limites des approches traditionnelles de certification. Ironie du sort, alors que ces approches étaient considérées comme suffisantes en matière de comportements des opérateurs de première ligne, elles sont jugées inappropriées pour certifier des technologies qui deviennent plus « humaines », notamment dans le sens où leurs performances ne sont plus déterministes ni même probabilistes. Au-delà de la certification, c'est l'approche de gouvernance dans son ensemble qui est à revoir. Selon Antonsen (2022), *« les régulateurs et les autorités de contrôle ne permettront jamais que les processus décisionnels critiques changent sans supervision. La gouvernance des algorithmes auto-apprenants nécessite de la réglementation, des outils d'audit et des compétences, ce qui n'est pas en place, et il est difficile de voir comment cela pourrait être fait, du moins dans un régime réglementaire prescriptif »*.

Avec les algorithmes auto-apprenants, il devient encore plus évident que nous devons reconnaître une part d'incertitude et apprendre à vivre avec. La pandémie de Covid 19 a aussi été l'occasion d'en faire l'expérience brutale. Cela a cependant aussi été l'occasion d'envisager des approches alternatives de gouvernance, comme le décrit un anesthésiste-réanimateur interrogé par Shorrock (2022) : « *Pour de nombreux professionnels, elle [la pandémie] a créé un sentiment touchant d'humilité, tant chez les acteurs de première ligne que chez les managers. Je crois que cette humilité a facilité la communication et l'émergence d'une gouvernance partagée entre les soignants et les administrateurs là où j'ai travaillé.* ». Bien que cette expérience se réfère à la gouvernance au sein des organisations, des phénomènes similaires se sont produits lors d'échanges ponctuels entre régulateurs et régulés. Dans l'aviation par exemple, l'expérience sans précédent de pilotes incapables de se conformer au nombre de vols requis ou de suivre la formation périodique requise pour maintenir leur licence valide, a conduit à une collaboration inédite entre les différentes parties pour trouver des moyens d'aller au-delà de l'approche normative actuelle. À une échelle plus large, celle de la gouvernance de la science, Jasanoff (2007) va plus loin en appelant à une

approche encore plus inclusive pour vivre avec l'incertitude et l'ignorance, en impliquant aussi les citoyens, non seulement pour trouver des solutions mais pour, en premier lieu, définir le(s) problème(s).

Saisir les multiples facettes d'un problème ainsi que ses spécificités contextuelles pourrait être encore plus critique à une époque où une majorité de sociétés sont préoccupées par d'autres questions majeures telles que la sûreté (au sens de la protection contre des actes intentionnellement malveillants) ou le changement climatique. Comme l'a évoqué l'un des participants de l'atelier ferroviaire, la question des moyens financiers d'accompagnement de cette révolution technologique est centrale. Est-il raisonnable d'accumuler des technologies coûteuses au regard des enjeux sociétaux et des préoccupations croissantes face au changement climatique ? Plus généralement, revisiter la gouvernance des technologies numériques, et notamment dans les industries à risques, pourrait nécessiter d'aller au-delà non seulement des acteurs traditionnels régulateur/régulé, mais aussi de dépasser la seule question de la sécurité. Comme le soulève Jasanoff (2007) : *« Suffit-il, par exemple, d'évaluer les conséquences de la technologie, ou bien faut-il aussi chercher à évaluer ses finalités ? »*.

3.3.2 Éthique

L'un des aspects qu'il faudrait aborder dans une nouvelle approche de gouvernance serait l'éthique. Comme le souligne De Boisboissel (2022) dans un contexte militaire, *« la prise en compte des enjeux éthiques dans le développement, la maintenance et l'exécution des logiciels devient un impératif induit par l'autonomie des systèmes robotiques »*. D'autres industries/activités à risques partagent cette préoccupation qui, en association avec des questions de responsabilité, a été explicitement mentionnée lors de l'atelier ferroviaire. Plus généralement, il existe une abondante littérature sur l'éthique de l'IA. Selon Siau & Wang (2020) *« Construire une IA éthique est une tâche extrêmement complexe et stimulante »*. Deux questions préliminaires seraient : Est-ce seulement possible ? ou est-ce même souhaitable ? Les positions sont mitigées quant à remettre au centre du débat l'opposition entre humains et machines. Selon De Boisboissel (2022), *« une machine est, par nature, amorale. L'humain reste le seul et unique agent moral, donc le seul responsable »*. Citant Lambert (2020), l'auteur ajoute que *« le raisonnement éthique nécessite une connaissance et une conscience de la situation, qui sont des caractéristiques uniquement humaines (ibid.) »*. Le principal défi devient donc comment faire collaborer l'IA et les humains pour prendre des décisions éthiques dans des situations critiques ? À l'inverse, essayer d'intégrer de l'éthique dans les machines, c'est plutôt essayer de faire en sorte que les machines deviennent plus humaines. Une telle approche, s'inscrivant dans une perspective de substitution[6] (par opposition à une stratégie collaborative), considère implicitement que c'est faisable à condition d'y consacrer des ressources suffisantes. Ces compréhensions différentes du problème vaudraient la peine d'être affinées par des réflexions plus contextualisées et inclusives, en revenant à un niveau supérieur de questionnement commun, par exemple, comment prendre des décisions éthiques ? Qu'est-ce qu'une décision éthique ?

3.3.3 Cadre légal

Le problème de la responsabilité sous-tend plus ou moins explicitement presque toutes les questions soulevées jusqu'à présent à tous les niveaux, qu'ils soient opérationnels, organisationnels et liés à la conception, ou sociétaux. Dès lors, le cadre juridique est au cœur des réflexions associant humanité et technologie, d'autant plus avec les capacités des algorithmes auto-apprenants et la multiplication des parties prenantes qui, comme nous l'avons formulé précédemment, est inhérente à l'introduction de ces technologies.

Cependant, comme mentionné lors de l'atelier ferroviaire, nous parvenons à améliorer le niveau de sécurité au prix d'une complexité et d'une fragmentation accrues impliquant une perte ou un transfert de responsabilité. Le cadre juridique, tel qu'il existe en Europe, ne peut appréhender l'incertitude et la fragmentation à mesure qu'elles évoluent. Il est très difficile d'encadrer juridiquement le progrès technologique. La loi ne peut pas évoluer au même rythme que celui des progrès technologiques. Le législateur essaie de définir un cadre, mais au bout du compte, il y a le juge. Le système parfait n'existe pas. L'idée qu'il existerait un cadre législatif qui clarifierait toutes les responsabilités est une illusion. L'œil du juge et celui de la société sont ceux qui comptent finalement. Ces constats appellent également à des réflexions plus inclusives et plus contextualisées sur l'IA.

3.3.4 Questions sociétales et philosophiques

L'usage de l'IA dans les industries à risques, mais aussi au-delà de ce domaine, interroge la relation entre l'homme et la technologie à tous les niveaux, y compris sur le plan philosophique. Le sujet n'est pas nouveau. En 1954, (Heidegger) avançait déjà que *« nous avons une compréhension technologique de nous-mêmes et du monde »*.

6. Cette hypothèse de substitution s'applique principalement à la phase opérationnelle. Dans la conception, le développement et la maintenance/correction des systèmes d'IA, le rôle des humains tend à se renforcer.

Cependant, la question se pose en termes différents au regard du pas supplémentaire franchi avec les artefacts technologiques auto-apprenants vers une « humanisation », avec l'utilisation d'expressions telles que « intelligence » artificielle ou IA « éthique ». « *Après tout, le monde dans lequel nous vivons est de plus en plus peuplé non seulement d'êtres humains, mais également d'artefacts technologiques qui contribuent à façonner nos modes de vie* » (Verbeek, 2009). Avec l'avènement de l'IA avancée et des systèmes autonomes, une nouvelle question se pose, non pas sur la façon dont nous vivons notre vie, mais plutôt sur la façon dont nous pourrions la perdre : dans quelle mesure la sécurité des humains et de l'environnement peut-elle être gérée par la technologie ?

Comme l'a souligné Williams (2020), avec les progrès des machines, « *la technologie elle-même en est venue à être considérée comme déterministe, « une force autonome et transhumaine dans les affaires sociales ». (...) nous nous distinguons mentalement de la technologie (...). Et où cela nous mène-t-il ? Sommes-nous à la merci ou bien sommes-nous en contrôle à la fois de la technologie et de la nature, ou de l'un plus que de l'autre, ou ni de l'un ni de l'autre ?* ».

Norman (2014) voit la relation entre les humains et les machines « *[comme] un problème social autant que technologique* ». L'auteur affirme que « *ce sont principalement nos structures sociales qui déterminent à la fois la direction que prend la technologie et son impact sur nos vies* » (Préface). Il semblerait qu'avec la digitalisation, la société non seulement ait adopté un point de vue centré sur la technologie, mais qu'elle soit aussi en train de limiter, dans une certaine mesure, sa représentation et sa compréhension du monde à ce qui peut être appréhendé par des capteurs ou à travers des données (en quantité massive). Ce tournant semble reposer sur une sorte de mythe ou de magie. Comme le souligne Antonsen (2022) « *il existe une forme d'incertitude épistémique intégrée aux modèles et aux algorithmes qui acquièrent une forme d'objectivité parce qu'ils sont apparemment épargnés par la faillibilité humaine du jugement, alors qu'en fait, ils ne le sont pas* ».

Conclusion : vers une réflexion inclusive et contextualisée sur l'humain, l'intelligence artificielle et la sécurité

Avec l'accélération des progrès des technologies numériques, en particulier de l'IA, de nouvelles questions se posent sur le rôle des hommes dans la sécurité des industries à risques pour les décennies à venir. Les machines sont perçues comme de plus en plus humaines, notamment avec l'utilisation pour elles aussi de termes comme « intelligence », et leurs capacités spécifiques sont souvent opposées aux « faiblesses » humaines. Pourtant, aller plus loin dans l'analyse du référentiel utilisé pour caractériser les humains ou les machines, ou des capacités réelles des machines, au-delà du mythe socialement construit, conduit à nuancer les jugements définitifs sur leurs qualités respectives.

Considérer l'humanité et la technologie comme séparées l'une de l'autre à toutes les échelles et vouloir rendre d'une part les humains plus semblables à des machines et, d'autre part, les machines plus humaines, représente un immense défi. Humains et machines ont des qualités spécifiques et ne peuvent raisonnablement être remplacés par l'autre à tous égards. Les deux existent dans le monde d'aujourd'hui à toutes les échelles, mais ce qui pourrait requérir une attention accrue, c'est de les faire coexister de manière fructueuse. Cela nécessiterait de les considérer chacun pour ce qu'ils sont, de penser et concevoir leur complémentarité et leur articulation pour éviter de favoriser/entretenir la concurrence entre eux. Cela signifie également qu'il faut contextualiser les réflexions plutôt que de rester à des niveaux très généraux. Faire une distinction entre différentes échelles, différents types d'activités, mais aussi entre différentes situations de travail, organisations ou différents environnements socio-économiques, juridiques et politiques est indispensable pour réfléchir aux conditions nécessaires pour rendre pertinente la collaboration entre les humains et les technologies de l'IA dans le contexte particulier en question. L'utilisation d'IA sophistiquée dans les industries à risques pourrait être différente de celle que l'on en fait dans les activités non critiques. Comme l'a déclaré Antonsen (2022), « *nous devrions repenser la façon dont nous conceptualisons et étudions la relation entre l'agent humain et l'agent technologique de la sécurité* ». Tout comme les ergonomes suggèrent de partir des situations de travail et d'impliquer les opérateurs dans la conception de nouveaux systèmes, revenir aux situations réelles et impliquer les experts de ces situations pourrait conduire à des débats plus réalistes et plus fructueux autour de la relation entre l'humain et la machine dans le domaine opérationnel, ainsi qu'à des décisions quant à leur articulation fondées sur de meilleures bases. Pourtant, cette relation est aussi à penser et à discuter au-delà des opérations, à des niveaux supérieurs – notamment organisationnels, sociétaux et philosophiques – afin de développer une réflexion plus large sur les liens entre humain et technologie. En effet, les différents niveaux mentionnés ne sont pas déconnectés les uns des autres et la combinaison d'éléments de toutes ces échelles ainsi que de perspectives diverses, pourrait aider à dépasser l'actuelle dichotomie simpliste entre humanité et technologie, et à relever certains des défis qui en découlent.

Références

Antonsen, S. (2022). Between Natural and Artificial Intelligence—Digital Sustainability in High-Risk Industries. Dans H. Laroche, C. Bieder, & J. Villena-López (Eds.), *Managing Future Challenges for Safety* (pp. 41-50). Cham : Springer. doi :https://doi.org/10.1007/978-3-031-07805-7_5

Boucher, P. (2019). *How artificial intelligence works.* European Parliament. Récupéré sur https://www.europarl.europa.eu/RegData/etudes/BRIE/2019/634420/EPRS_BRI(2019)634420_EN.pdf

Cook, R. I. (2020). How complex systems fail. *HindSight, 31*, pp. 13-16.

Daniellou, F., Simard, M., & Boissières, I. (2011). *Human and organizational factors of safety : a state of the art.* Toulouse, France : Foundation for an Industrial Safety Culture. Récupéré sur https://www.foncsi.org/en/publications/collections/industrial-safety-cahiers/human-organizational-factors-of-safety

De Boisboissel, G. (2022). Evolution in the Way of Waging War for Combatants and Military Leaders. Dans H. Laroche, C. Bieder, & J. Villena-Lopez (Eds.), *Managing Future Challenges for Safety* (pp. 13-24). Cham : Springer. Récupéré sur https://doi.org/10.1007/978-3-031-07805-7_2

Dekker, S. (2015). *Safety differently : Human factors for a new era* (Second ed.). CRC Press.

Downer, J. (2011). « 737-Cabriolet" : the limits of knowledge and the sociology of inevitable failure. *American Journal of Sociology, 117*(3), pp. 725-762.

Downer, J. (2020). On ignorance and apocalypse : A brief introduction to « epistemic accidents ». Dans J.-C. Le Coze (Ed.), *Safety Science Research : Evolution, Challenges and New Directions.* Boca Raton : CRC Press.

GSAS 'Opérateur du futur'. (2023). *Le monde change, la sécurité industrielle aussi - Humain, numérique, nouvelles organisations : 10 points-clés à l'horizon 2040.* Toulouse : Fondation pour une culture de sécurité industrielle. doi :10.57071/240dpc

H. Laroche, C. Bieder ; J. Villena-Lopez (Eds). (2022). *Managing Future Challenges for Safety.* Cham : Springer. Récupéré sur https://link.springer.com/book/10.1007/978-3-031-07805-7

Heidegger, M. (1954). The question concerning technology. *Technology and values : Essential readings*, pp. 99-113.

Jasanoff, S. (2007). Technologies of humility. *Nature, 450*(33). doi :https://doi.org/10.1038/450033a

Lambert, D. (2020). *Que penser de...? La robotique et l'Intelligence artificielle.* Fidélité.

Norman, D. (2014). *Things that make us smart : Defending human attributes in the age of the machine.* Diversion Books.

Okhrimenko, I., Sovik, I., Pyankova, S., & Lukyanova, A. (2019). Digital transformation of the socio-economic system : prospects for digitalization in society. *Revista Espacios, 40*(38).

Okhrimenko, I., Sovik, I., Pyankova, S., & Lukyanova, A. (2019). Digital transformation of the socio-economic system : prospects for digitalization in society. *Revista Espacios, 40*(38).

Parmiggiani, E., Østerlie, T., & Almklov, P. (2022). In the Backrooms of Data Science. *Journal of the Association for Information Systems, 23*(1), pp. 139-164.

Pollard, K. (2009). What makes us human? *Scientific American, 300*(5), pp. 44-49.

Roe, E., & Schulman, P. (2008). *High Reliability Management : Operating on the Edge.* Stanford, CA : Stanford University Press.

Shorrock, S. (2022). Adaptive Imagination at Work in Health Care. Dans H. Laroche, C. Bieder, & J. Villena-López (Eds.), *Managing Future Challenges for Safety* (pp. 95-104). Cham : Springer. doi :https://doi.org/10.1007/978-3-031-07805-7_12

Siau, K., & Wang, W. (2020). Artificial intelligence (AI) ethics : ethics of AI and ethical AI. *Journal of Database Management, 31*(2), pp. 74-87.

Verbeek, P. P. (2009). Cultivating humanity : Towards a non-humanist ethics of technology. Dans *New waves in philosophy of technology* (pp. 241-263). London : Palgrave Macmillan. doi :https://doi.org/10.1057/9780230227279_12

Williams, J. (2020). Humanity, Technology, and Nature. *Icon, 25*(2), pp. 8-28.

Reproduction de ce document

FONCSI
Fondation pour une culture de sécurité industrielle

Fondation pour une culture de sécurité industrielle
Fondation de recherche reconnue d'utilité publique

http://www.foncsi.org/

6 allée Émile Monso – CS 22760
31077 Toulouse Cedex 4
France

Téléphone : +33 (0) 532 093 770
X : @LaFonCSI
Email : contact@foncsi.org

ISSN 2100-3874

FONCSI

Fondation pour une culture
de sécurité industrielle

6 allée Émile Monso
ZAC du Palays - CS 22760
31077 Toulouse cedex 4

www.foncsi.org