Groupe de travail « Veille collaborative »

Synthèse de l'analyse des trois thèmes de veille

« Cybersécurité-Résilience / Intelligence Artificielle / Traçabilité-Blockchain »

Méthodologie

Les membres du groupe de travail se sont accordés sur une **grille d'analyse** intégrant les critères suivants :

- niveau de maturité (dans une logique de type TRL simplifié) :
. Exploration R&D,
. Emergence et 1ères applications,
. Phase de déploiement dans les usages.
- prédominance des domaines d'application ou d'intégration des usages (ex : agro, santé).
- singularité-tendance-signal faible.

Le travail d'analyse s'est effectué par sous-groupes.
Chaque sous-groupe a produit sa propre synthèse.
Les éléments ci-dessous en constituent la consolidation.

1/ Thématique « Cybersécurité –Résilience »

1.1. Cette thématique a été classée en 10 principales sous-thématiques/domaines d'application : *(présentées ci-après par ordre décroissant d'apparition)*

- Cyber et outils ou compétences IA
- Evénements Cyber
- Sensibilisation / Formation / Bonnes pratiques
- Observation des tendances / Analyses / Enquêtes
- Appels à Projet / Initiatives institutionnelles
- Cyber – IoT et technologies numériques
- Etudes Prospectives / Tendances / Anticipation
- Pôles de compétence Cyber / Mise en réseau d'acteurs
- Cyber attaques / Détection menaces
- Investissements dans la Cyber / Partenariats industriels

A noter : le premier bulletin, ne comportait pas de rubrique spécifique « cybersécurité » ; le sujet était traité dans les thèmes « Blockchain » ou « Intelligence Artificielle ».

1.2. Tous les domaines d'application sont concernés.

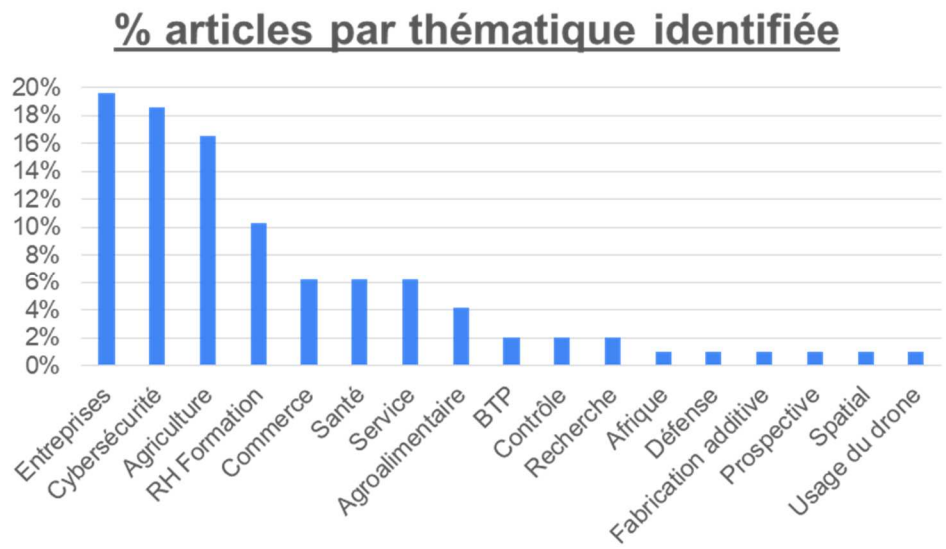
Il ressort plus spécifiquement des articles diffusés les domaines applicatifs suivants :

- Naval / défense, aéronautique,
- Industries (**automobile**, agro-alimentaire, pharmaceutiques, …),
- Etablissements de santé,
- Administrations / collectivités.

1.3. Une analyse SWOT a été produite à partir des unités d'information retenues pour leur pertinence :

FORCES	FAIBLESSES
• L'IA est essentielle pour analyser les menaces en temps réel • IA – Machine Learning / Deep Learning > capacité d'apprentissage	• Peu d'entreprises se sont accaparées du sujet de menace cyber (manque de moyens, manque d'information, …) • L'homme = premier facteur de risque
OPPORTUNITES	**MENACES**
• La sécurité est un enjeu organisationnel : politique de sécurité du système d'information • Emergence de nouveaux métiers > nouvelles formations • Cybercampus : sensibilisation / formation ; mutualisation des outils, compétences et données ; développement de la filière industrielle.	• Ransonware –- cryptojacking – hameçonnage • Objets connectés peu ou pas sécurisés notamment dans le secteur industriel • Cloud • Dépendance des entreprises et des gouvernements à l'IA et au machine learning (conséquence d'un déficit de compétences).

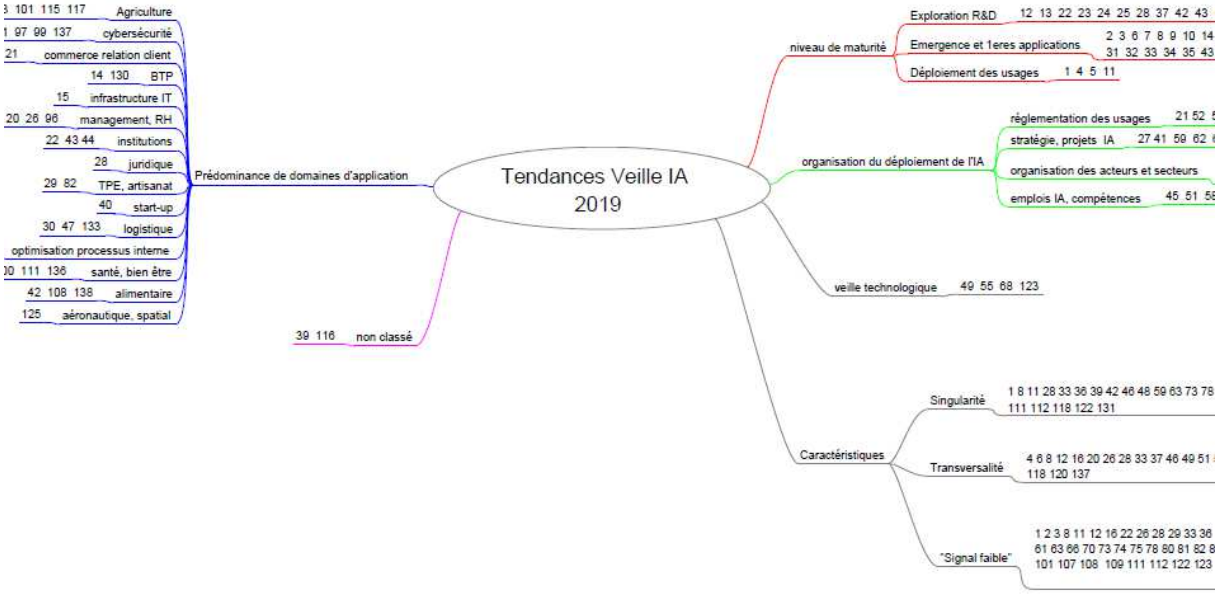
2/ Thématique « Intelligence Artificielle »



- Un biais ressort pour le critère d'analyse « prédominance » en raison d'une **très forte contribution de la Chambre d'Agriculture Normandie** dans la production des informations de veille : beaucoup d'articles apparaissent ainsi liés à l'agriculture,
- Par ailleurs, une tendance assez marquée porte sur la création de formations, de cursus universitaires, de chaires, de clusters de recherche… sur ce thème de l'IA : engouement passager, ou phénomène durable ? Il faudrait analyser de plus près le phénomène,
- L'IA apparait aussi fortement concerner le domaine des RH,
- Tendance au développement d'utilisations conjointes des technologies IA et blockchain dans plusieurs secteurs : agro-alimentaire, logistique, santé, énergie,

- Tendance enfin au lancement de travaux, en parallèle de la diffusion des applications technologiques, pour préciser la terminologie, créer un cadre règlementaire, définir des règles d'éthique.

Ci-après, la cartographie des informations diffusées au cours de l'année 2019 :



3/ Thématique « Blockchain-Traçabilité »

3.1. Tendances :

Ce thème concerne potentiellement aussi **tous les secteurs d'activités**.

- La blockchain est en émergence voire en déploiement à petite échelle selon les secteurs, pour faire face aux **enjeux de confiance et de sécurisation dans la traçabilité de données numériques partagées**,
- Les secteurs Finance, Agri-agro et Santé particulièrement confrontés aux enjeux de traçabilité sont davantage avancés dans l'appropriation la techno blockchain,
- Globalement, les usages ne sont pas généralisés (plusieurs échéances sont évoquées : entre 5 et 10 ans) et sont évoqués **au futur**.

3.2. Facteurs différenciants :

- **Différents niveaux de maturité sont observables, avec un TRL ≤ 6** :

. **Agri-Agro** : émergence voire déploiement selon les applications au sein de partenariats, de consortiums ou de blockchains privées (exemple : « Blockchain Filière Qualité Carrefour »),

. Des POCs (preuves de concept) sont engagés dans les domaines de la **finance** (gestion et sécurisation des transactions commerciales internationales) et de l'**assurance** (certification et sécurisation des contrats et polices),

. **Santé** (conformité et validité pour les données médicales stockées),

. Exploration R&D et 1ères applications dans d'**autres secteurs** : luxe, joaillerie (lutte *vs* contrefaçons) ou les services publics (formalités administratives), jeux vidéos en ligne, impression 3D, …

- **La blockchain vient en appui d'autres technologies émergentes nécessitant la sécurisation des échanges de données entre différents acteurs :**

. Digitalisation dans la santé : conformité et validité pour les données médicales stockées,

. Impression 3D : vérification de la validité des données d'entrées,

. Energies renouvelables : certification de données de production/consommation.

3.3. Signaux faibles :

- Intérêt de quelques acteurs forts (par exemple IBM avec sa plateforme « Food Trust » créée il y a 5 ans, Microsoft…), dans le secteur agro-agri avec de multiples coopérations,
- De nombreuses entreprises étrangères (+ ou – importantes) expérimentent en France,

→ *Enjeux de défense et de sécurité publique*

- Développement d'une stratégie nationale : création d'une Task Force (2019),
- Déjà des freins au déploiement :

. Capacité des logiciels à tenir la charge,

. Nécessité de règlementer et de clarifier la gouvernance : règles et normes pour l'intégration dans les systèmes existants et dans les différentes organisations partenaires

→ *Actuellement, 11 normes en conception par le* ***comité technique l'ISO/TC 307***

3.4. Approche économique :

- Peu de données économiques sur les coûts, le ROI de l'implémentation et la mise sur le marché de solutions Blockchain,

-Exemple du coût d'une prestation de mise en place d'un architecture Blockchain de consortium et de déploiement d'une application de notarisation de données ~55k€ (hors support individualisé et définition de Uses cases appliqués).

<u>Remarques générales / Propositions</u>

Ce travail d'analyse a permis aux membres du groupe de travail de porter un **regard critique sur l'exercice de veille collaborative** :

- Richesse des informations diffusées,
- Réelle pertinence du travail collectif sur le long terme (même si peu de retombées directement mesurable),
- Les tendances détectées sont souvent déjà assez bien établies : en effet, les sources consultées par les « veilleurs » sont généralement des études et articles de media, certes spécialisés, mais qui publient des articles lorsque la technologie ou l'usage commence à se développer,
- Il conviendrait donc de diversifier encore plus les sources *(bases brevets, articles scientifiques, thèses et autres publications universitaires)* afin d'avoir réellement un « coup d'avance ». Cependant, il est certain que les cibles PME vont plutôt adopter des technologies ou utiliser des services dès lors qu'ils sont éprouvés afin de limiter les risques suite à l'adoption de ceux-ci, exception faite des entreprises spécialisées,
- Pertinence d'enrichir ce « corpus » de veille par des spécialistes / experts afin d'identifier les signaux faibles (mais alors attention au supplément d' « effort » nécessaire *vs* gain pour le collectif),
- Opportunité de valoriser cette démarche d'intelligence collective.