



Radar orientation client et transformation

Secteur public

Région bruxelloise

Unité veille – pôle DT - Paradigm

Octobre 2025

FINAL

INTRODUCTION	3
Intro.....	3
AVANT PROPOS	3
Cloud et souveraineté numérique	3
Désinformation	4
RADAR PARADIGM V5	6
Cadran Radar Orientation client	6
Cadran Radar Gouvernement digital	8
CONTEXTE	14
METHODOLOGIE	14
A PROPOS	15

INTRODUCTION



Intro

Bienvenue dans l'édition de novembre 2025 du **Radar de transformation digitale du secteur public et d'orientation client** en Région bruxelloise. Ce Radar de veille fait suite à l'enquête Radar de l'été 2025.

Pour une explication sur la méthode du Radar, voir la section *Méthodologie*.

AVANT PROPOS

Le Radar, en tant qu'outil de veille, ne vise pas seulement à distinguer les priorités, mais aussi à cartographier les évolutions par rapport à la période précédemment étudiée. Ces changements par rapport à l'enquête précédente, qui accordait la priorité aux thèmes du cloud et de la désinformation, ne peuvent être dissociés du contexte géopolitique profondément modifié : l'arrivée d'un nouveau gouvernement aux États-Unis début 2025, qui remet en question l'axe historique Europe-État-Unis ; ainsi que la guerre - dite hybride - sur le continent, avec des actions de la Russie visant à déstabiliser le continent européen.

Cloud et souveraineté numérique

Les évolutions géopolitiques récentes ont clairement influencé les priorités stratégiques des organisations, notamment en matière de cybersécurité, de cloud computing et de souveraineté numérique.

Mais concrètement, que signifient ces notions de cloud et de souveraineté numérique ?

Enjeu 1 : Le cloud, la sécurité et la confidentialité des données

L'usage du cloud, en particulier en mode SaaS (Software as a Service), soulève des préoccupations importantes lorsqu'il s'agit de données sensibles. Ces données peuvent être exposées à différents risques :

- Transferts hors de l'Union européenne, soumis à des lois extraterritoriales comme le Cloud Act américain ;
- Perte de contrôle sur le traitement et l'hébergement des données ;
- Cyberattaques ou indisponibilité des services.

Cela amène des questions concrètes :

- Où les données sont-elles stockées et traitées par le fournisseur cloud, et sous quelle juridiction tombent-elles ?
- Où se situent l'application SaaS et les données spécifiques qu'elle utilise ?
- Quelles mesures doivent être mises en place concernant la gestion des accès, le chiffrement des données et la conformité réglementaire ?

Enjeu 2 : La souveraineté numérique

La souveraineté numérique vise à garantir que les données et les infrastructures critiques restent sous contrôle européen ou national. Elle repose sur trois piliers :

- Une maîtrise juridique : quelle juridiction s'applique ?
- Une maîtrise technique : accès, auditabilité, réversibilité des systèmes ;
- Une maîtrise stratégique : indépendance vis-à-vis des fournisseurs non européens.

Cependant, le concept reste encore flou. Les partenariats entre géants américains du cloud (Amazon AWS, Microsoft Azure, etc.) et des acteurs locaux brouillent les lignes de cette souveraineté.

Cela soulève plusieurs questions quant à la stratégie à ADOPTer :

- Faut-il opter pour une approche hybride ? Par exemple, utiliser un cloud souverain pour les données critiques et des solutions SaaS pour les services moins sensibles ?
- Comment garantir la conformité réglementaire dans un cadre européen de plus en plus contraignant ?
- Doit-on tout revoir en faveur d'une architecture numérique souveraine (comme dans l'initiative [*Euro-Stack*](#)) ?

Les textes législatifs à prendre en compte incluent :

- RGPD : protection des données personnelles ;
- NIS2 : sécurité des réseaux et des systèmes d'information ;
- Data Act (2023) : accès et partage des données entre acteurs publics et privés ;
- Digital Services Act (DSA) et Digital Markets Act (DMA) : régulation des grandes plateformes numériques.

Désinformation

La désinformation constitue une menace croissante pour les institutions publiques. Elle affaiblit la confiance des citoyens, perturbe le débat démocratique et peut être exploitée par des acteurs étrangers pour déstabiliser les États. Exemple : de faux profils sur les réseaux sociaux, d'origine russe, perturbant une élection démocratique ou sapant la confiance.

Les services publics ont la responsabilité de :

- garantir une information fiable,

- corriger les fausses informations,
- renforcer la résilience des citoyens face aux manipulations numériques.

La Commission européenne a mis en place une stratégie globale articulée autour de plusieurs piliers :

Cadre réglementaire :

- Le Digital Services Act (DSA) impose aux grandes plateformes des obligations de transparence et de modération des contenus illicites.
- Le Code européen de bonnes pratiques contre la désinformation, renforcé en 2022, engage les plateformes à promouvoir les contenus fiables et à coopérer avec les vérificateurs de faits.
- Les administrations publiques sont invitées à :
 - renforcer leur communication institutionnelle, en diffusant des informations claires, accessibles et vérifiées ;
 - collaborer avec les vérificateurs de faits et les médias de confiance pour détecter et corriger les fausses informations ;
 - former les agents publics à repérer et contrer les campagnes de désinformation ;
 - participer aux initiatives européennes, telles que l'EDMO (Observatoire européen des médias numériques), ou aux campagnes de sensibilisation ;
 - intégrer la lutte contre la désinformation dans les plans de gestion de crise afin d'anticiper et de contrer efficacement d'éventuelles campagnes malveillantes.

RADAR PARADIGM V5

Cadran Radar Orientation client

Il est intéressant de rassembler les priorités exprimées par les clients et les tendances d'applications métier en relation avec les citoyens/entreprises et leur pertinence.

Il est pertinent de rapprocher les priorités exprimées par les clients des tendances en matière d'applications métiers liées aux citoyens et aux entreprises.

- 1 (ADOPT) Action – passer à l'action
- 2 (TRIAL) Etude – approfondir, préparer
- 3 (ASSESS) Monitoring – surveiller
- 4 (HOLD) Pause – hors scope pour la période analysée
- 5 hors périmètre
- 6 pas d'avis

Adopt

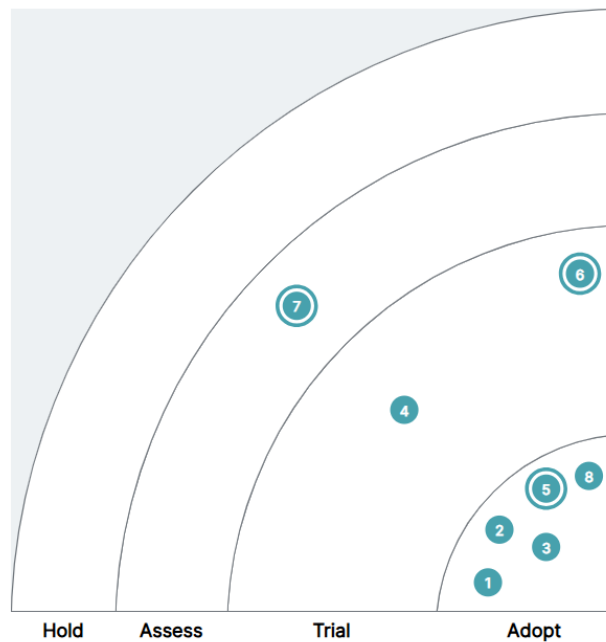
- 1. IT inclusif
- 2. Expérience utilisateur
- 3. Numérique responsable
- 5. IA – LLM use policy
- 8. Conformité aux réglementations (NIS2,DGA,...)

Trial

- 4. Automatisation contact utilisateur (chatbot)
- 6. Pièces d'identité digitalisées

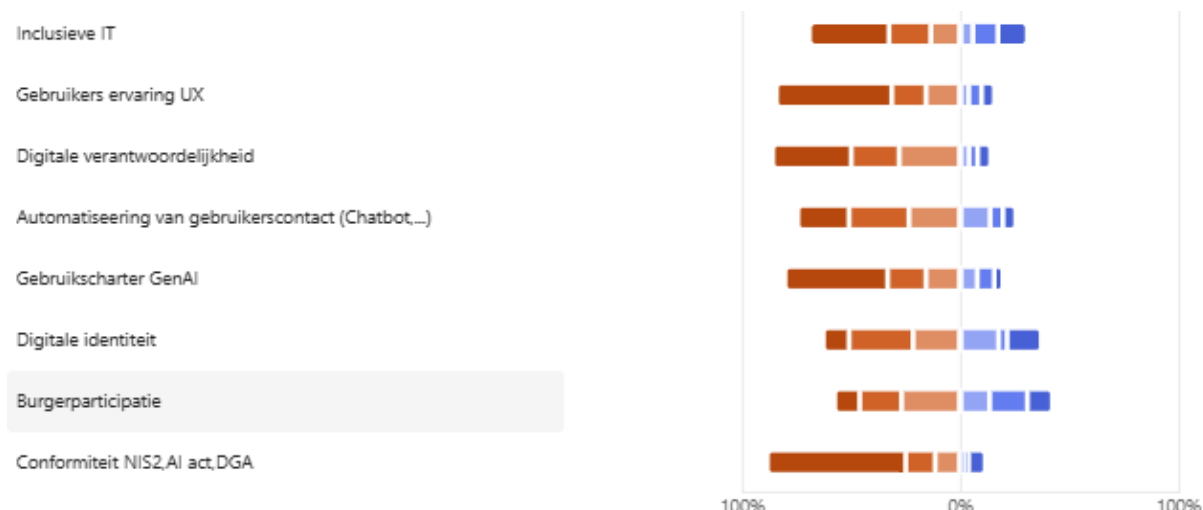
Assess

- 7. Participation citoyenne



1 2 3 4 5 6

(résultats de l'enquête)



Les évolutions principales par rapport au Radar précédant sont :

ADOPT : montée en puissance et confirmation du sujet prioritaire : conformité NIS 2 , AI Act , DGA ; confirmation de l'importance de l'expérience utilisateur (UX). Léger recul des thématiques numérique responsable et inclusion numérique.

TRIAL : progression notable de l'identité numérique (portefeuille d'identité), qui passe de ASSESS à TRIAL ; et *status quo* concernant l'automatisation de contact utilisateurs.

ASSESS : recul du thème de la participation citoyenne, désormais classé en ASSESS au lieu de TRIAL.

Voici une explication des termes utilisés dans le Radar orientation client :

ADOPT	Inclusion numérique	L'inclusion numérique, ou e-inclusion, est un processus qui vise à rendre le numérique accessible à tous, principalement la téléphonie et internet, et à leur transmettre les compétences numériques qui leur permettront de faire de ces outils un levier de leur insertion sociale et économique.
ADOPT	Expérience utilisateur	L'expérience utilisateur désigne la manière dont un client perçoit une organisation à travers l'ensemble de ses interactions avec elle. Elle couvre l'intégralité du parcours, depuis le premier contact jusqu'au support après l'utilisation du service : plus les interactions sont positives, meilleure est l'expérience.
ADOPT	Numérique responsable	Le numérique peut réduire l'empreinte écologique de certains processus, mais il possède lui-même une empreinte carbone importante tout au long de son cycle de vie (de l'extraction des matières premières au traitement des déchets électroniques). Le secteur public doit maximiser le premier effet et réduire le second.
ADOPT	Charte GenAI	Mise en place d'une politique interne encadrant l'usage d'outils d'IA approuvés, afin d'assurer un cadre sécurisé et d'améliorer la productivité.

ADOPT	Conformité aux réglementations (NIS2,DGA, etc.)	NIS2 est un ensemble de règles relatives à la cybersécurité ; le DGA (Digital Governance Act) encadre le partage des données, etc.
TRIAL	Automatisation contact utilisateur (chatbot)	L'automatisation du support client est tout ce qui vise à réduire ou à éliminer le besoin d'implication humaine dans la résolution des demandes des clients, par exemple en répondant automatiquement aux questions par e-mail ou même aux appels téléphoniques. Il comprend également une assistance pour les agents des centres d'appels en fournissant des suggestions de réponses, par un chatbot interne ou même un assistant virtuel
TRIAL	Pièces d'identité digitalisées	Les portefeuilles d'identité numériques (DIW) permettent le partage de données d'identité ou d'attestations avec un large éventail d'organisations, tout en conservant le contrôle de ses données.
ASSESS	Participation citoyenne	Usage des technologies numériques pour encourager la participation des citoyens et leur auto-organisation afin de créer de la valeur sociétale. Le citoyen peut endosser différents rôles, par exemple celui de fournisseur de données.

Cadran Radar Gouvernement digital

Les résultats du Radar Gouvernement digital mettent en évidence des évolutions dans la perception des priorités technologiques au sein du secteur public. Ces priorités présentent souvent un double volet : un volet digital, lié à l'accélération des technologies, et un volet méthodologique, nécessaire dans un processus de transformation organisationnelle (par exemple, le design thinking).

- 1 (ADOPT) Action – passer à l'action
- 2 (TRIAL) Etude – approfondir, préparer
- 3 (ASSESS) Monitoring – garder en vue
- 4 (HOLD) Pause – hors scope pour la période analysée
- 5 hors périmètre
- 6 pas d'avis

Adopt

9. IA : Agent IA	▼
10. IA-ANPR et autre technologies intelligente	▼
18. Parcours Transformation digitale	▼
14. Plateforme de données	▼
16. Cybersécurité	▼
17. Désinformation	▼
19. Approche de gestion en design thinking	▼
20. Plateforme low code	▼
22. Cloud	▼

Trial

11. Office + AI	▼
13. Smart Building, GML	▼
15. Informatique spatiale	▼

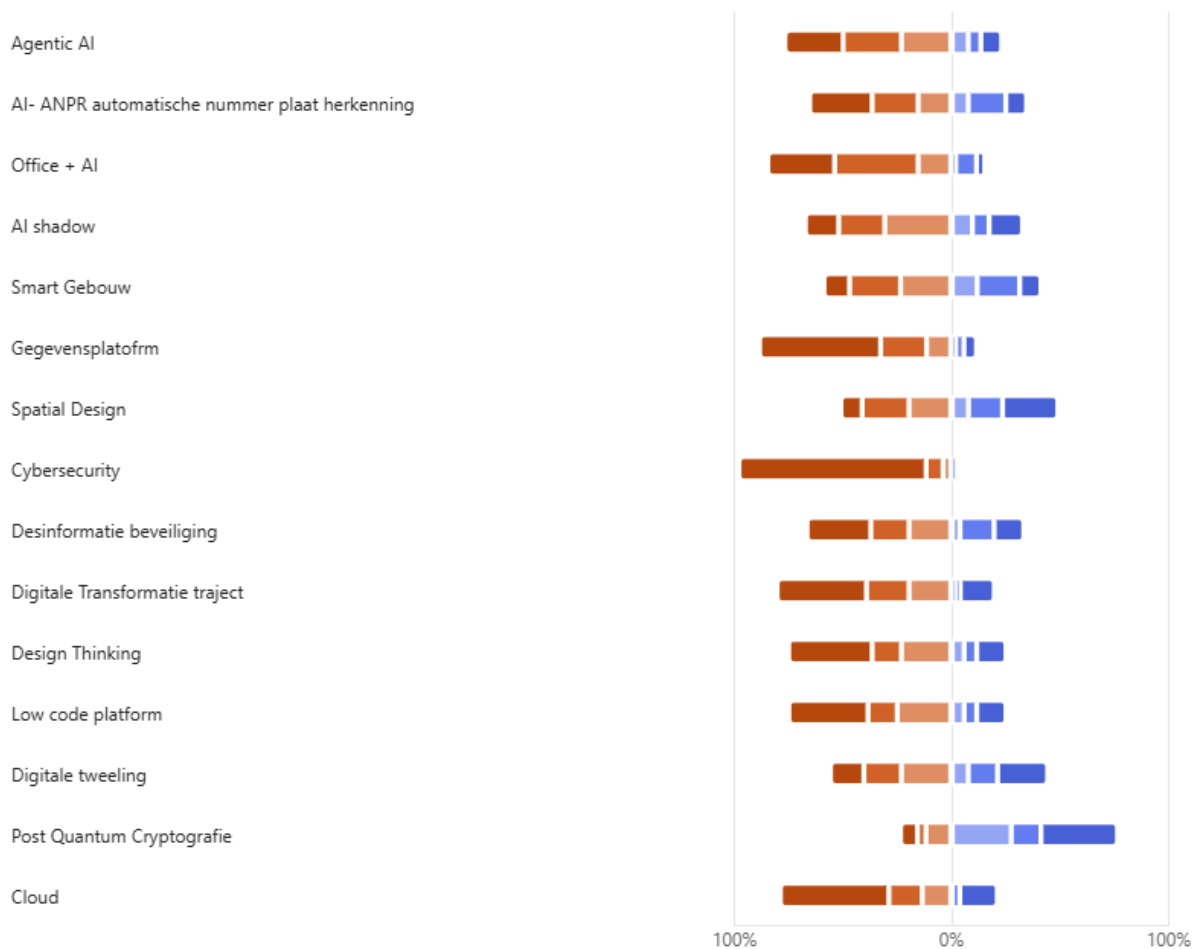
Assess

12. Shadow AI	▼
21. Jumeau numérique	▼

Hold

23. Quantum computing cryptography	▼
------------------------------------	---





Les évolutions principales par rapport au Radar précédent sont les suivantes.

Au niveau du cadran ADOPT :

Une priorisation claire de la cybersécurité, élément centrale et croissant dans l'administration publique. Le cloud poursuit également sa montée en puissance, avec une question importante : vers un clou souverain ?

Deux nouveaux termes apparaissent désormais dans le cadran ADOPT :

- Agentic AI ;
- Désinformation.

Le terme Office AI et Agentic AI apparaissent à la fois dans ADOPT et TRIAL, ce qui traduit une volonté d'intégrer l'IA dans la productivité individuelle tout en continuant à explorer d'autres éléments.

Le sujet Smart Building recule et passe dans le cadran TRIAL.

Dans le cadran ASSESS, on retrouve certaines tendances aujourd'hui peu populaires, notamment le shadow AI et le jumeau numérique. Ce dernier constitue toutefois une exception notable dans ce Radar : il reste en effet une priorité dans d'autres niveaux de pouvoir, en particulier dans certaines communes ou dans d'autres régions.

La cryptographie et les ordinateurs quantiques ne semblent pas encore être une priorité. Ces sujets passent en ASSESS, voire en HOLD.

Explication des termes utilisés dans le Radar gouvernement digital :

ADOPT	IA-ANPR et autre technologies intelligente	ANPR (Automatic Number Plate Recognition) est un système capable de reconnaître les plaques d'immatriculation des véhicules à partir d'images vidéo et, par exemple, d'ouvrir automatiquement les barrières dans un parking souterrain.
ADOPT	Cybersécurité	La cybersécurité est composée d'un ensemble de technologies, de processus et de pratiques conçus pour protéger les réseaux, les ordinateurs, les applications et les données contre les attaques, les dommages ou les accès non autorisés. La défense contre des attaquants puissants et organisés gagne en importance. Les ransomwares sont une tendance inquiétante.
ADOPT	Approche de gestion en design thinking	Méthodologie visant à améliorer la conception de logiciels, produits et services. L'empathie envers les utilisateurs et la collecte d'informations sur leurs besoins et leurs motivations sont essentielles. Cette approche favorise l'innovation numérique centrée sur l'humain et est étroitement liée à la conception humaine et à l'ADOPTION des applications (gouvernementales).
ADOPT	Plateforme low code	Une plateforme software qui permet de créer des programmes informatiques sans connaissances approfondies des langages de programmation.
ADOPT	Cloud	Le cloud computing est le stockage et le traitement de données sur des serveurs externes via internet, au lieu d'infrastructures locales (comme son propre ordinateur ou serveur).
ADOPT	IA : Agent IA	Les systèmes d'Intelligence Artificielle agentiques sont capables de planifier et d'agir de manière autonome pour atteindre des objectifs définis par l'utilisateur. L'IA agentique offre la promesse d'une main-d'œuvre virtuelle capable de décharger et d'augmenter le travail humain.
ADOPT	Plateforme de données	Une plateforme de données est une solution complète pour l'importation, le traitement, l'analyse et la visualisation des données générées par les systèmes, les processus et les infrastructures des entreprises numériques modernes.
ADOPT	Désinformation	La sécurité contre la désinformation est une catégorie émergente de technologie qui discerne systématiquement la confiance et vise à fournir des systèmes méthodologiques pour assurer l'intégrité, évaluer l'authenticité, prévenir l'usurpation d'identité et suivre la propagation des informations nuisibles.
ADOPT	Parcours Transformation digitale	En exploitant les dernières technologies (comme l'IoT, l'analyse, l'apprentissage automatique...), les modèles de fonctionnement peuvent être changés / transformés et de nouveaux modèles numériques robustes peuvent être créés.
TRIAL	Smart Building, GML	Un « smart building », ou bâtiment intelligent, intègre des outils numériques offrant de nombreux avantages, qui vont de l'optimisation des ressources énergétiques au confort des collaborateurs. Pour les entreprises, c'est la possibilité de diminuer les coûts opérationnels, tout en proposant à leurs équipes les meilleures conditions de travail possibles.
TRIAL	Informatique spatiale	L'informatique spatiale améliore numériquement le monde physique avec des technologies telles que la réalité augmentée et la réalité virtuelle.

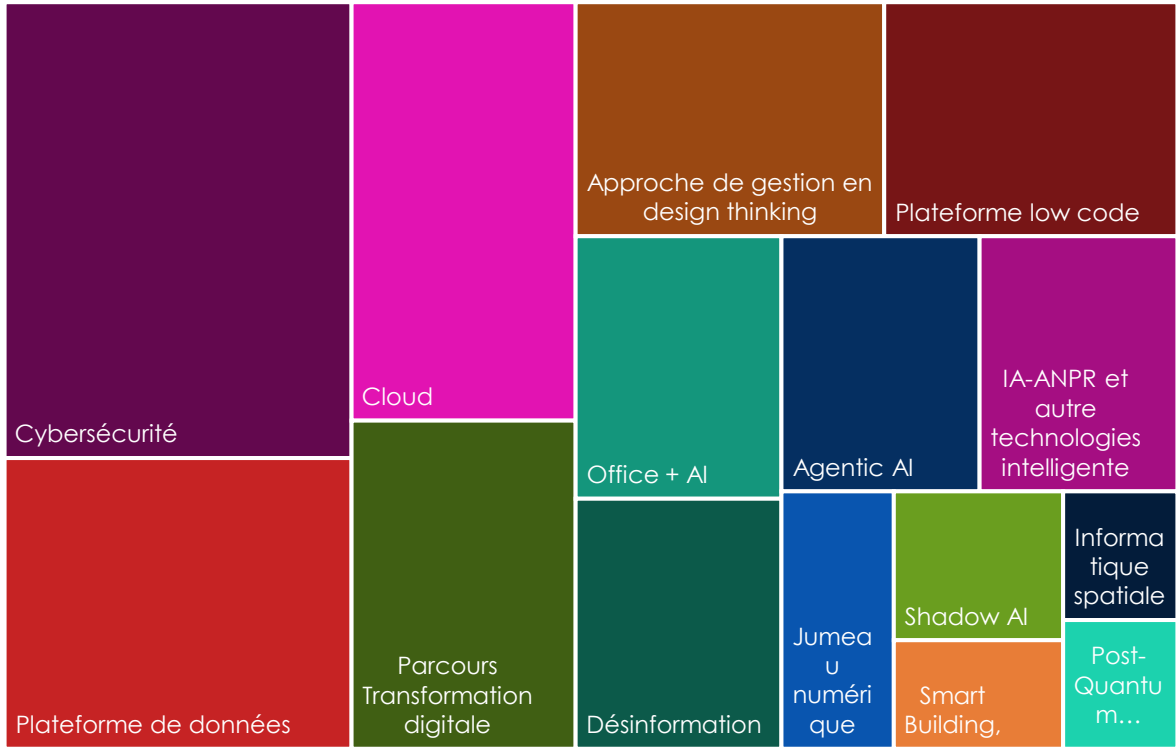
TRIAL	office + AI	Activation d'outils comme Microsoft Copilot dans les applications bureautique classique.
ASSESS	Shadow AI	Ou IA de l'ombre ; c'est un terme qui décrit quand l'IA générative est utilisée à des fins professionnelles pour, par exemple, rédiger un article ou coder, et ce en dehors de la gouvernance du département IT. Cela peut avoir un impact sur de l'information critique d'entreprise comme la divulgation d'informations critiques, la création de code software non conforme, etc.
ASSESS	Jumeau numérique	Un jumeau numérique est une représentation virtuelle dynamique d'un objet, d'un processus, d'un système, d'un réseau, d'un environnement ou même d'une personne, qui se comporte de manière identique à son homologue du monde réel. Un jumeau numérique est utilisé pour prédire les résultats de performance possibles et anticiper les problèmes que l'homologue du monde réel pourrait subir (exemple pour simulation/prévision catastrophe).
HOLD	Post quantum Cryptography	Utilisation de modèles avancés de mécanique quantique dans les sciences informatiques, pouvant entraîner des dangers pour les systèmes informatiques en matière de sécurité et de cryptographie.

Une autre manière de visualiser la tendance est de **voir la relative importance dans la partie ACTION du Radar transformation digitale.**

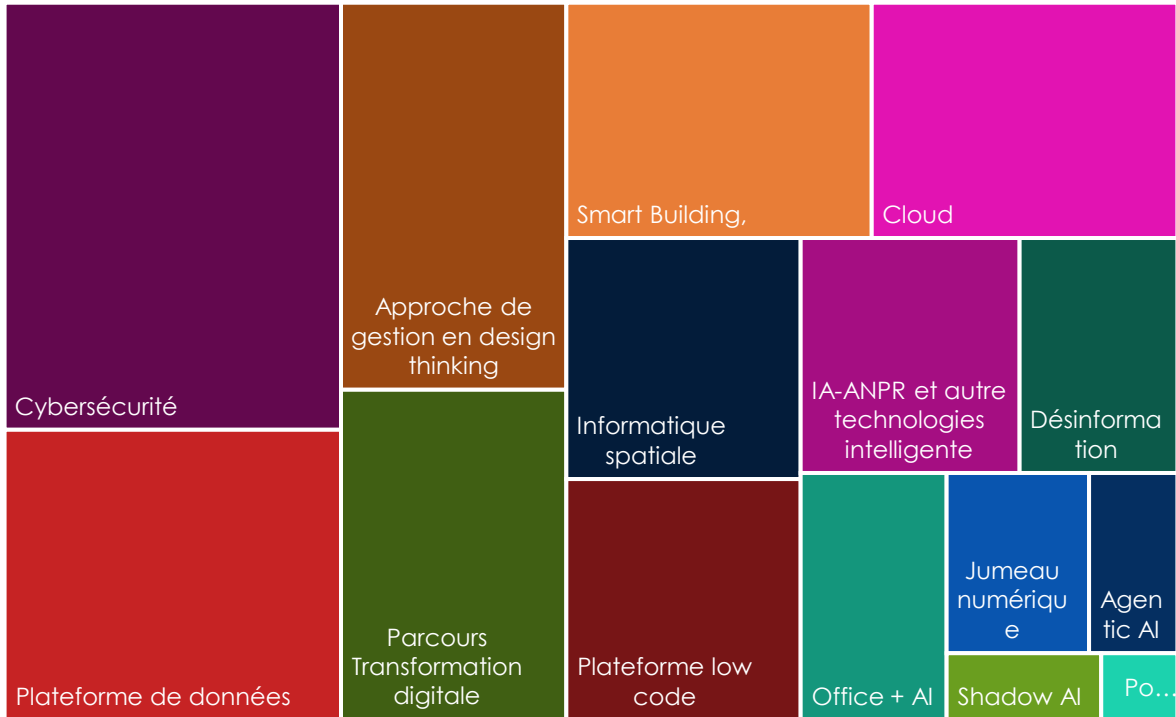
Le top 3 reste identique : **cybersécurité, plateforme donnée parcours transfo digitale.**

On y remarque la montée des domaines cloud et désinformation (voir intro).

2025 IMPLEMENT



2024 IMPLEMENT



CONTEXTE

Le **Radar de transformation digitale secteur public et d'orientation client** est un outil de veille permettant de suivre les **tendances** et les **priorités** en matière de transformation digitale.

Il permet de **visualiser** les tendances émergentes et aide à les prioriser en fonction de leur importance. Le Radar de transformation digitale constitue une image figée de la situation à un moment donné, et il peut être mis à jour régulièrement pour suivre l'évolution des priorités et des actions qui en découlent.

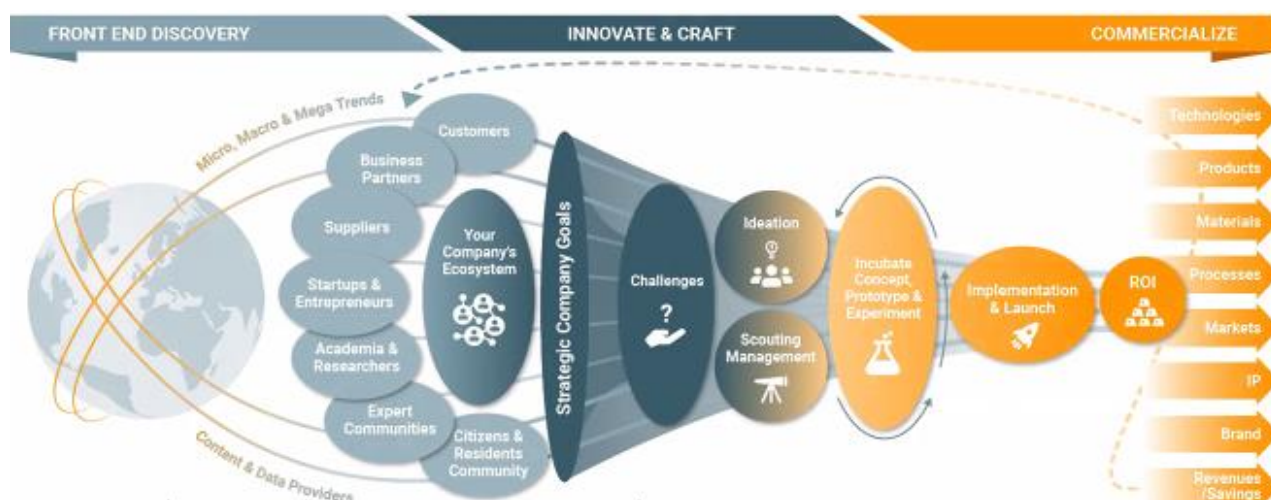


Illustration du trajet d'innovation : (source : *Qmarkets innovation*) – Le Radar se situe dans la partie gauche, appelée “Front End Discovery”, où l’on analyse les tendances. La suite du parcours comprend : la mise en place de projets d’innovation (Innovate and Craft), l’idéation, le scouting management (recherche d’applications start-up existantes), la création d’un lab pour tester des approches dans un environnement sécurisé permettant cette expérimentation (sandbox), pour ensuite passer dans une phase de lancement et d’utilisation.

METHODOLOGIE

Le Radar de transformation digitale et d'orientation client est structuré autour de quatre cercles de pertinence, avec les tendances les plus actionnables au centre. Les tendances sont classées en fonction de leur pertinence et de leur impact potentiel sur les activités de transformation digitale des acteurs publics de la Région bruxelloise.

Le Radar de transformation digitale et d'orientation client constitue un outil précieux pour les instances de gouvernance régionales bruxelloises qui cherchent à innover et à rester à jour avec les dernières tendances en matière de transformation digitale.

Il peut, dans ses premières zones, aider à cadrer une veille structurée et à démarrer des activités d'innovation tout en restant en phase avec les enjeux propres, le contexte et la mission de transformation digitale de Paradigm et des institutions de la Région bruxelloise en général.

Le terme Radar provient de l'aviation militaire, qui par un système de scan permet de détecter des objets ou des avions dans l'espace aérien. Les contrôleurs aériens utilisent cette vue typique pour identifier les points en approche et prioriser leurs actions. Dans notre contexte, le terme Radar a été repris dans l'idée de scanner les tendances émergentes et évaluer leur impact dans un futur plus ou moins proche.

Eléments d'un radar de tendances :

- Une tendance, accompagnée d'une courte définition,
- La priorisation de cette tendance selon 4 gradations de pertinence : ce qui est au centre est le plus important.

Il faut lire le Radar selon 4 cercles de pertinence :

- (ADOPT) Action – passer à l'action
- (TRIAL) Etude – approfondir, préparer
- (ASSESS) Monitoring – garder en vue
- (HOLD) Pause – hors scope pour la période analysée

Le Radar a été mis en place de la manière suivante :

- Enquête interne et externe (auprès de la gouvernance régionale) de Paradigm en juillet-septembre 2025. Plus de 50% des participants étaient externes à Paradigm, comme le montre ce graphique :



- CIO briefing Gartner ;
- Echanges avec l'équipe Digital Transformation ;
- Remerciements à Smals Research pour les échanges méthodologiques <https://www.smalsresearch.be/>;
- Inspiration d'autres radars plus technologiques : Thoughtworks (<https://www.thoughtworks.com/radar>), Devoteam (<https://techradar.devoteam.com/>) et Zalando (<https://opensource.zalando.com/tech-radar/>)
- Référence aux rapports Gartner 2025 Top Tech Trends ([2025-top-tech-trends-ebook.pdf](https://www.gartner.com/en/publications/2025-top-tech-trends-ebook)) et TechTrends 2025 ([go.infotech.com/it-tech-trends-2025-report](https://www.gartner.com/en/publications/2025-tech-trends-report))

A PROPOS

Pour toute remarque, suggestion d'amélioration ou participation à la prochaine édition prévue en septembre 2026 :

Contact : Tanguy De Lestré – Lead Innovation Paradigm

Email : tdelestre@paradigm.brussels

Tél. : 0486 38 46 18

Le Radar est un outil de veille proposé par Paradigm dans le cadre de sa valeur innovation et de sa mission officielle définie dans l'Ordonnance Paradigm. Il est soutenu par des actions exploratoires, telles que des trajets d'expérimentation et un service de facilitation.