

FILIÈRE INFRASTRUCTURES NUMÉRIQUES

Webinaire sur le futur des infrastructures numériques



Daniel Kofman
Directeur du PEPR « Réseaux du futur »



Emmanuel Dotaro
VP, Thales fellow



Arnaud Vilain
CSF IN Rapporteur du GT Innovation



Marianne Mohali
Stratégie Réseaux Orange

FILIÈRE INFRASTRUCTURES NUMÉRIQUES

Le livre blanc sur le futur des infrastructures numériques

Une analyse prospective pour éclairer les transformations et accompagner les choix de la filière



FILIÈRE INFRASTRUCTURES NUMÉRIQUES

Télécharger le livre blanc

1. **Contexte et objectifs de la démarche du CSF**
   Arnaud Vilain, rapporteur du GT Innovation du CSF des infrastructures numériques
2. **Vision d'ensemble des transformations en cours dans les réseaux de télécommunications**
   Marianne Mohali, stratégie réseaux (Orange)
3. **Nouveaux paradigmes pour les infrastructures numériques, enjeux de souveraineté, opportunités et recommandations**
   Daniel Kofman, directeur du PEPR "Réseaux du future", coéditeur du livre blanc, Prof. à Télécom Paris - IMT
4. **Cyber et confiance des infrastructures**
   Emmanuel Dotaro, VP, Thales fellow
5. **Débat + questions/réponses**

1. Contexte et objectifs de la démarche du CSF

Arnaud Vilain
CSF IN – rapporteur du GT Innovation

FILIÈRE
INFRASTRUCTURES
NUMÉRIQUES

Une recomposition mondiale des infrastructures numériques

La convergence des réseaux, du cloud et de l'IA transforme les chaînes de valeur et les rapports de dépendance. [1]

- **Les positions industrielles évoluent.** Les architectures 5G/6G intègrent les technologies du cloud, largement dominées par des acteurs extérieurs au secteur traditionnel des télécommunications, notamment les géants américains. [1]
- **La France connaît déjà des dépendances fortes.** En 2025, les fournisseurs américains représentent **79 % des achats de logiciels auprès des 50 premiers fournisseurs de l'UGAP.** [2]
- **Les conséquences dépassent la filière numérique.** Elles concernent la maîtrise des coûts, la protection des données et la continuité des services, ainsi que l'accès des entreprises et des citoyens aux technologies avancées. [1][2]

L'enjeu pour la filière est de préserver sa capacité à innover et à maîtriser les infrastructures dont dépend l'économie.

Sources

[1] Livre blanc sur le futur des infrastructures numériques et le positionnement des acteurs des secteurs impliqués (CSF Infrastructures numériques).

[2] Rapport fait au nom de la commission d'enquête sur les dépendances structurelles et les vulnérabilités systémiques dans le secteur du numérique et les risques pour l'indépendance de la France (Assemblée nationale).

Une vision commune pour orienter les actions de la filière

Les évolutions technologiques remettent en jeu la place des acteurs traditionnels des infrastructures numériques.

- **Une transformation profonde des chaînes de valeur.** Les architectures 5G/6G adoptent les technologies du cloud, dominées par des acteurs extérieurs aux métiers traditionnels des opérateurs et des équipementiers, notamment les GAFAM.
- **Des opportunités nouvelles, mais aussi des menaces existentielles.** Ces évolutions peuvent fragiliser les télécommunications et les filières critiques utilisatrices des réseaux, avec des conséquences pour l'ensemble des économies européennes.
- **Une compréhension encore trop fragmentée.** Les analyses restent souvent centrées sur une catégorie d'acteurs ou un type d'impact. Le cadre d'ensemble et les principaux risques demeurent insuffisamment identifiés, alors que les frontières entre télécommunications, cloud et IA s'estompent.

Le livre blanc apporte une vision transversale pour comprendre ces transformations, identifier les opportunités et les risques, et proposer des actions communes

Les coopérations européennes au service de la création de valeur

- **Un marché fragmenté, des complémentarités à organiser.** Face aux marchés américain et chinois structurés autour d'un nombre limité de grands opérateurs télécoms, les acteurs européens doivent mieux articuler leurs capacités pour gagner en échelle.
- **Des financements et une impulsion politique européenne.** Les programmes sur les réseaux 5G/6G et les projets communs sur le cloud soutiennent la recherche et les premiers déploiements industriels. La proposition de Digital Networks Act vise à harmoniser le marché et à favoriser l'investissement.
- **Des coopérations à traduire en offres concrètes.** Partenariats entre télécommunications, cloud, cybersécurité et IA, mutualisation des ressources et interopérabilité peuvent permettre de construire des offres communes et des modèles économiques viables pour chacun.

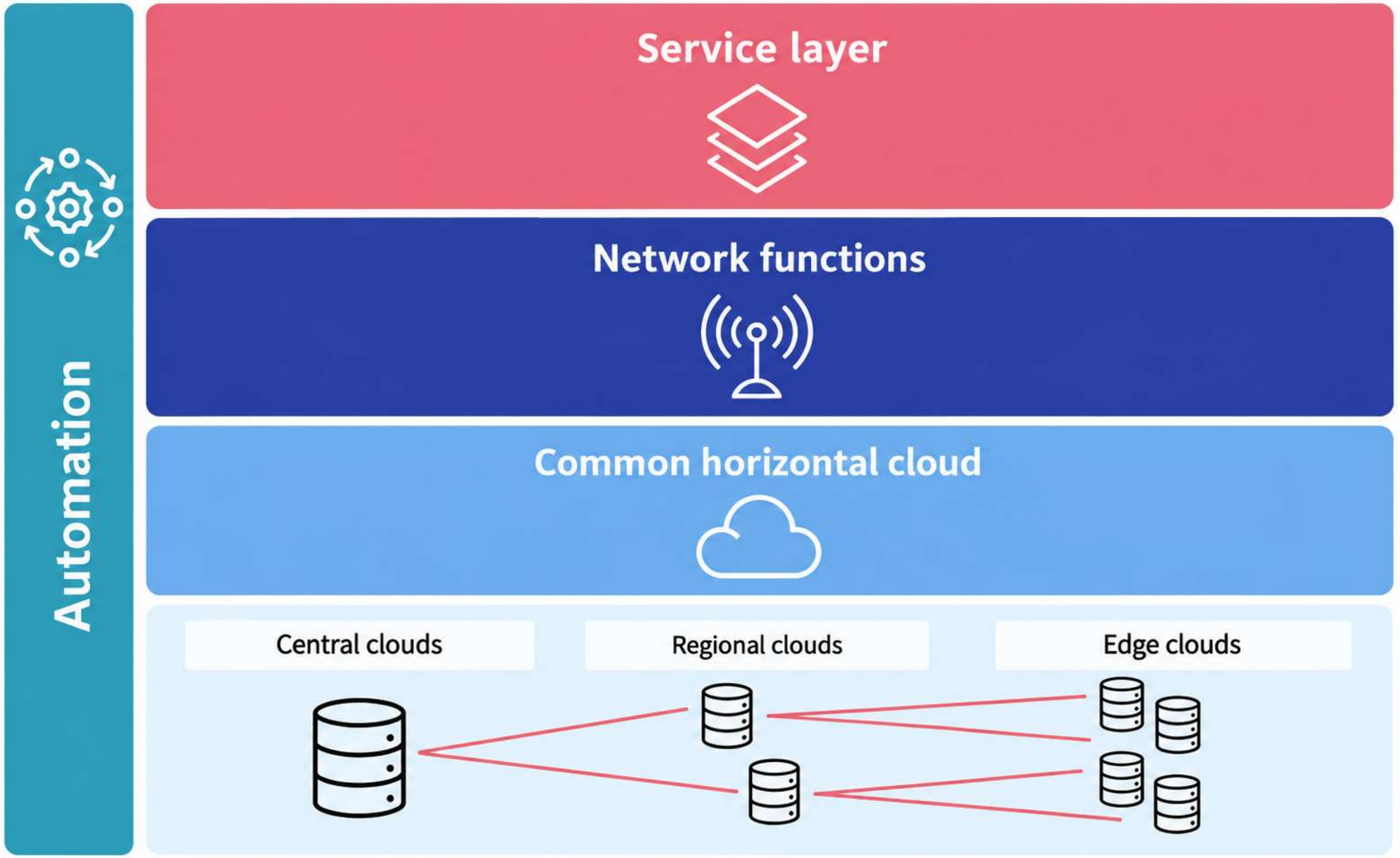
La suite de cette présentation se concentrera sur les opportunités ouvertes par ces transformations et sur la manière dont les acteurs français et européens peuvent créer de la valeur ensemble.

2. Vue d’ensemble des transformations en cours dans les réseaux de télécommunications

Marianne Mohali
Stratégie « Réseaux »
Orange

FILIÈRE
INFRASTRUCTURES
NUMÉRIQUES

Vision d’ensemble des transformations en cours dans les infrastructures numériques



FILIÈRE
INFRASTRUCTURES
NUMÉRIQUES

La double nature du réseau en constante évolution

Le monde physique

Poteau cassé par une tempête

Déploiement d'une antenne

Coupure de fibre optique

Le monde logiciel, data et IA

Software & automation

Core 5G

RAN

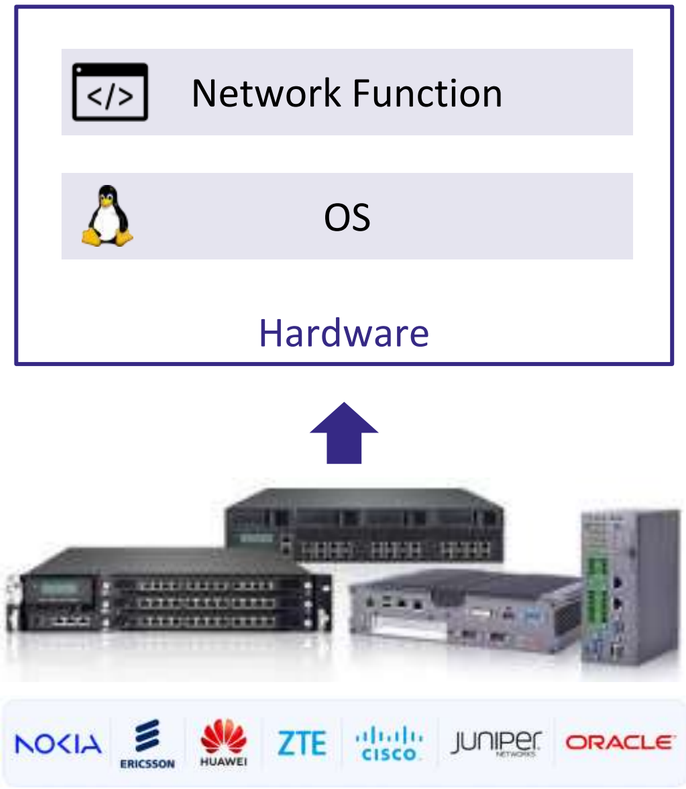
Data & AI

Platforming transformation

Chemin de transformation des fonctions réseaux

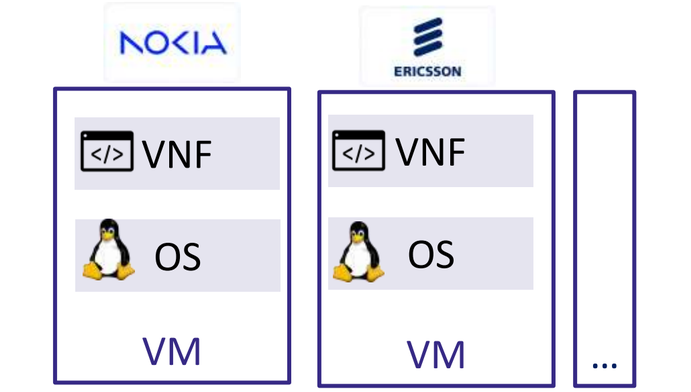
1980-1990 → 2010 → 2020

Fonction Réseau Physique (PNF)



NOKIA ERICSSON HUAWEI ZTE cisco JUNIPER ORACLE

Fonction Réseau Virtuelle (VNF)

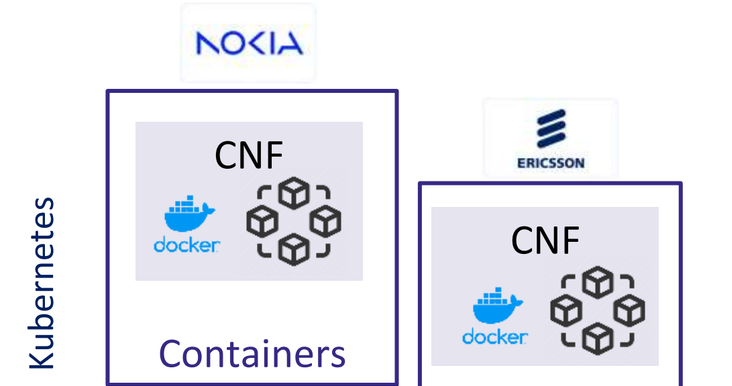




DELL hp Lenovo

Serveurs standards

Fonction Réseau Cloud Native (CNF)





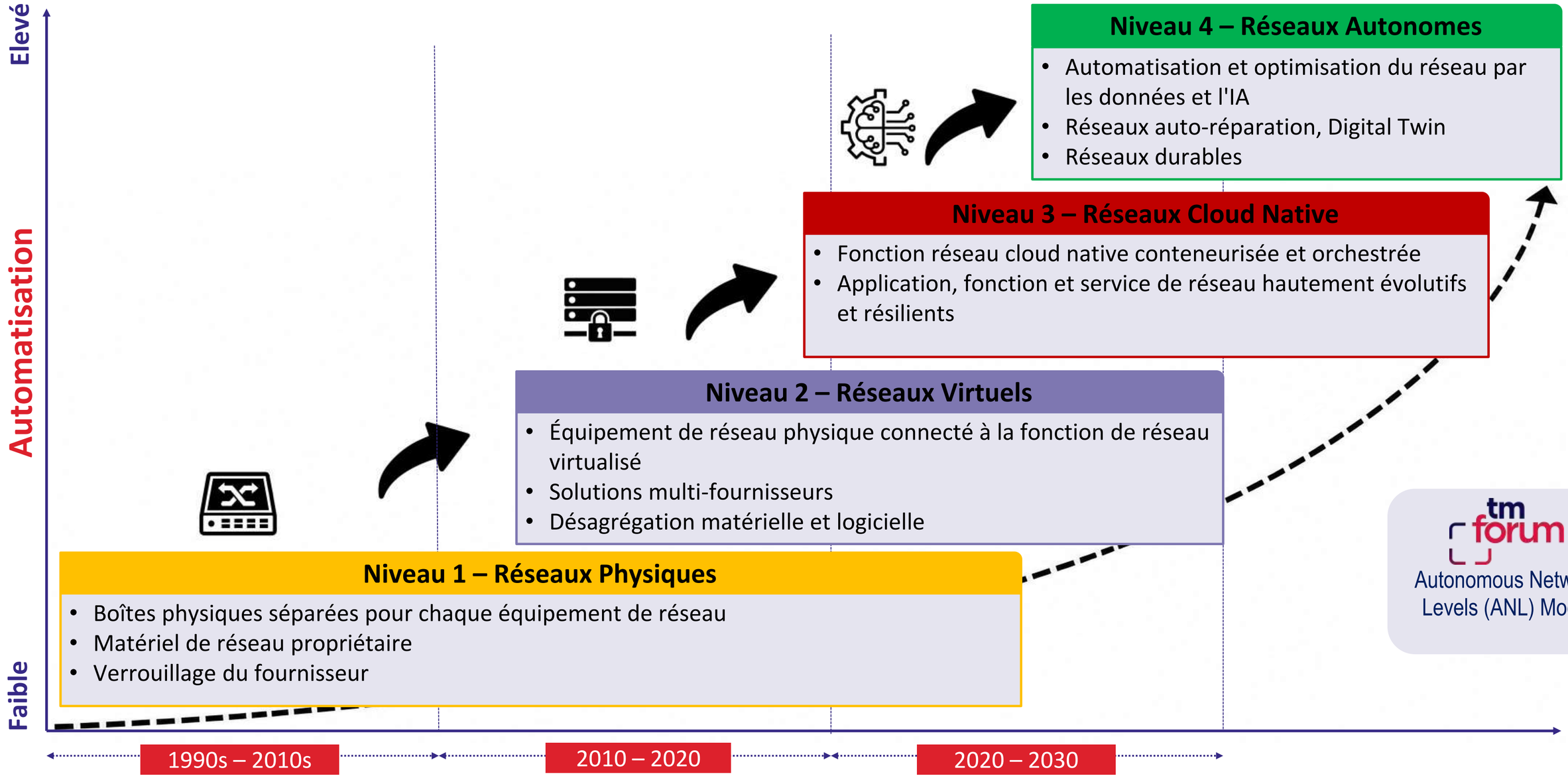
DELL hp Lenovo

Serveurs standards

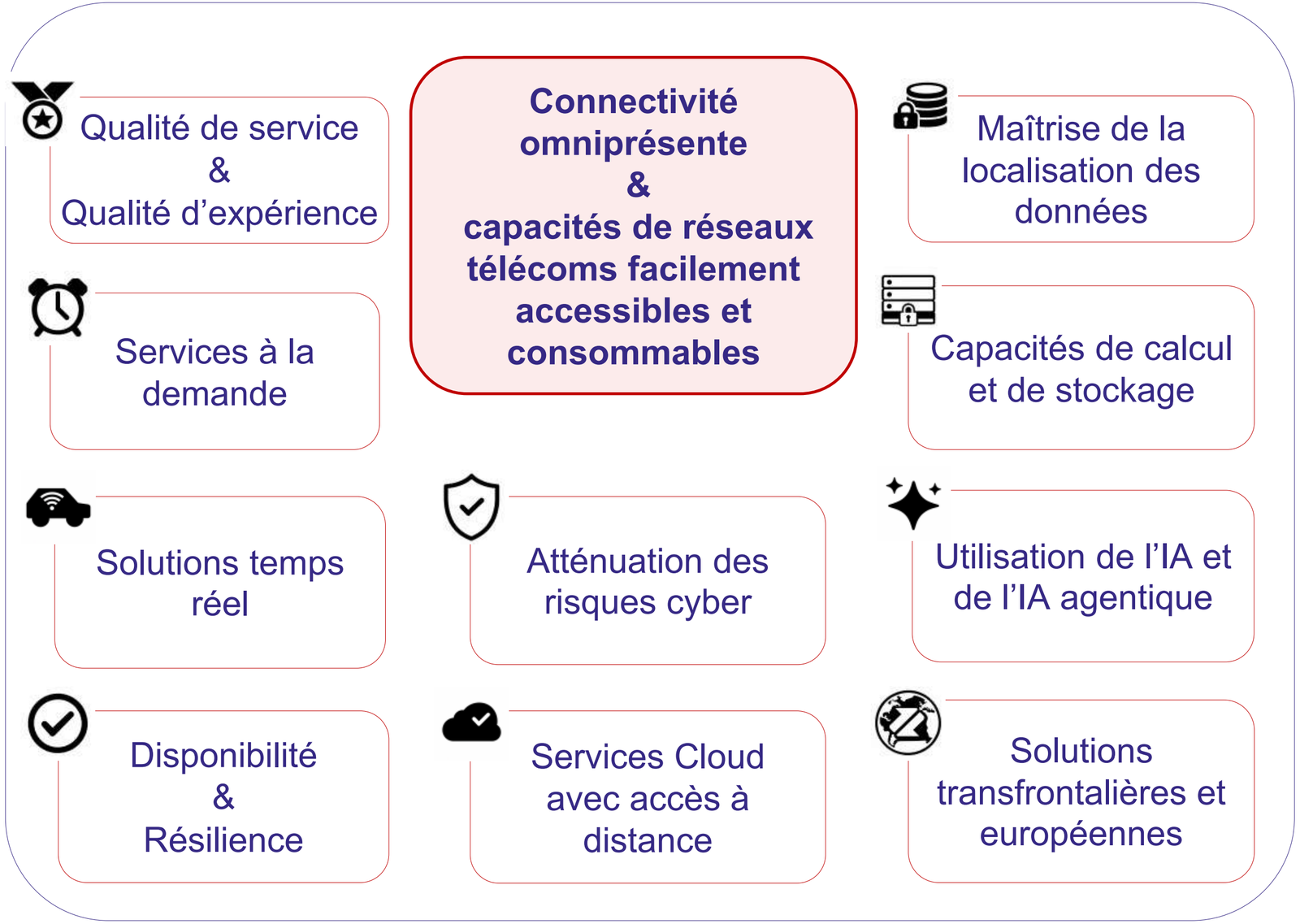
FILIÈRE INFRASTRUCTURES NUMÉRIQUES

PNF: Physical Network Function
VNF: Virtualized Network Function
CNF: Containerized Network Function
VM: Virtual Machine

L’évolution du modèle va permettre l’automatisation



Les attentes et les besoins des utilisateurs évoluent de la simple connectivité vers de l'expérience connectée



FILIÈRE INFRASTRUCTURES NUMÉRIQUES

3. Nouveaux paradigmes pour les infrastructures numériques, enjeux de souveraineté, opportunités et recommandations

Daniel Kofman
Directeur du PEPR « Réseaux du futur »
Coéditeur du livre blanc
Prof. à Télécom Paris - IMT

FILIÈRE
INFRASTRUCTURES
NUMÉRIQUES

01a

CONTENU

Le Livre Blanc

- Réseaux, Cloud, IA et verticaux, des changements de paradigme
- La chaîne technologique et ses enjeux de souveraineté
- Positionnement des acteurs actuels
- Les principales évolutions technologiques à considérer
- Catégorisation des opportunités et des risques pour les acteurs actuels et les nouveaux entrants
- Recommandations

01b

CONTENU

Le Livre Blanc, premier chapitre

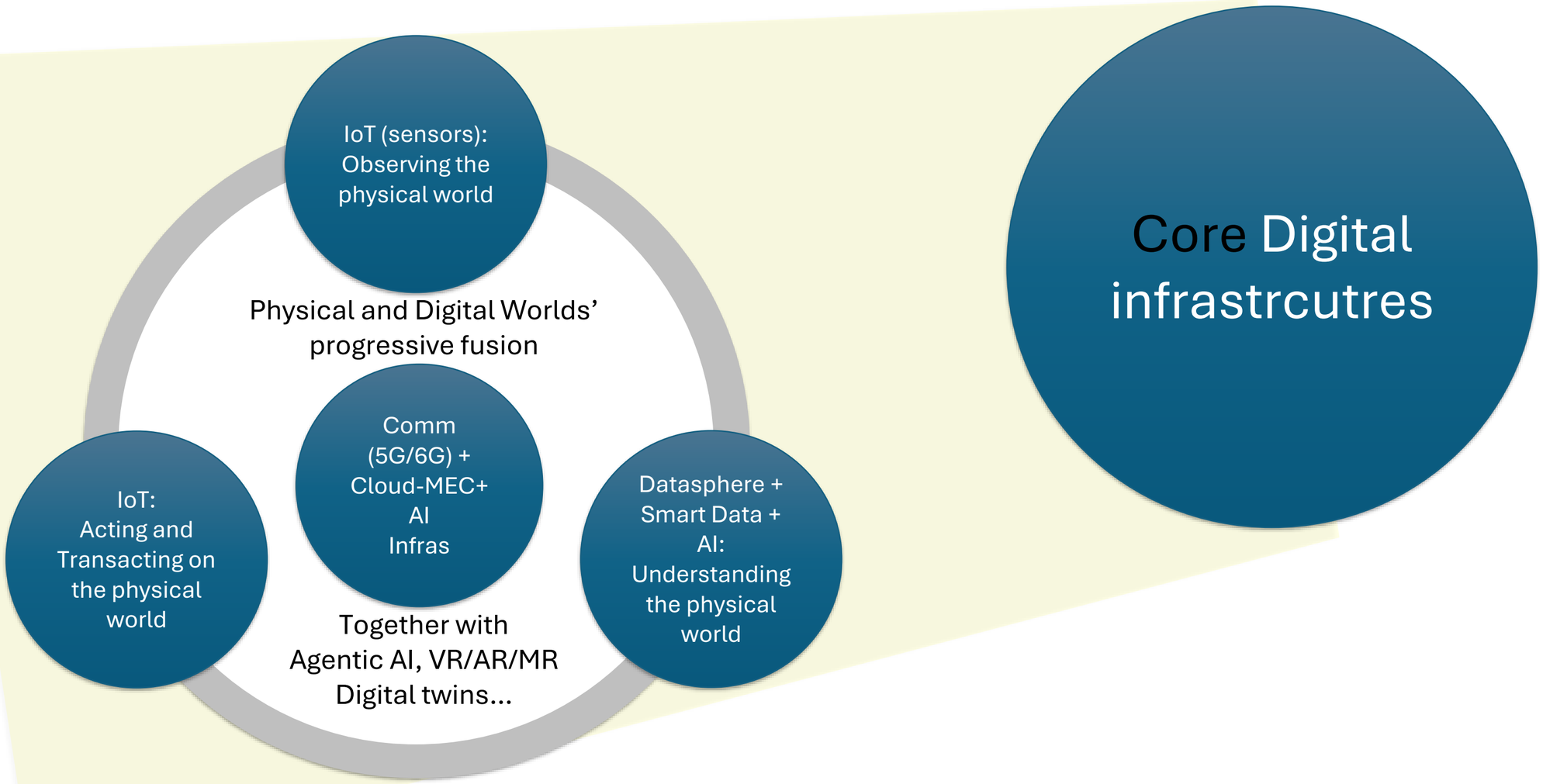
- Réseaux, Cloud et verticaux, un changement de paradigme
  - Convergence Réseaux-Cloud, MEC
  - L’IA pour les infrastructures numériques
  - Ouverture des réseaux
  - Les infrastructures numériques pour l’IA
  - Des services réseaux aux plateformes du numérique
  - Vers les services multisectoriels

- Convergence Réseau-Cloud-IA+Ouverture Vs Hyperscalers, un futur incertain

01c

CONTEXTE TECHNOLOGIQUE

Le Paradigme Général de la Numérisation

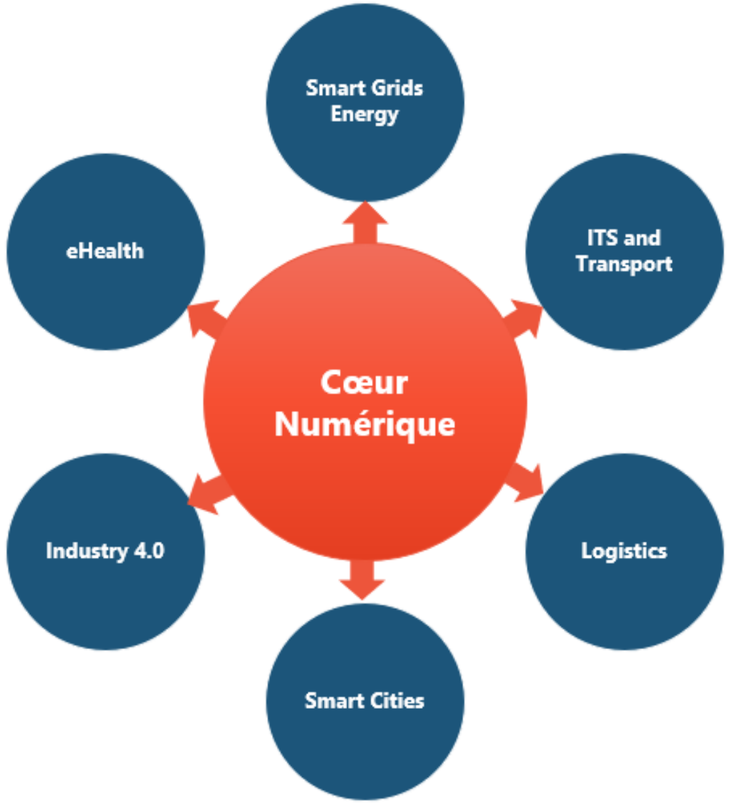


01d

NOUVEAUX PARADIGMES

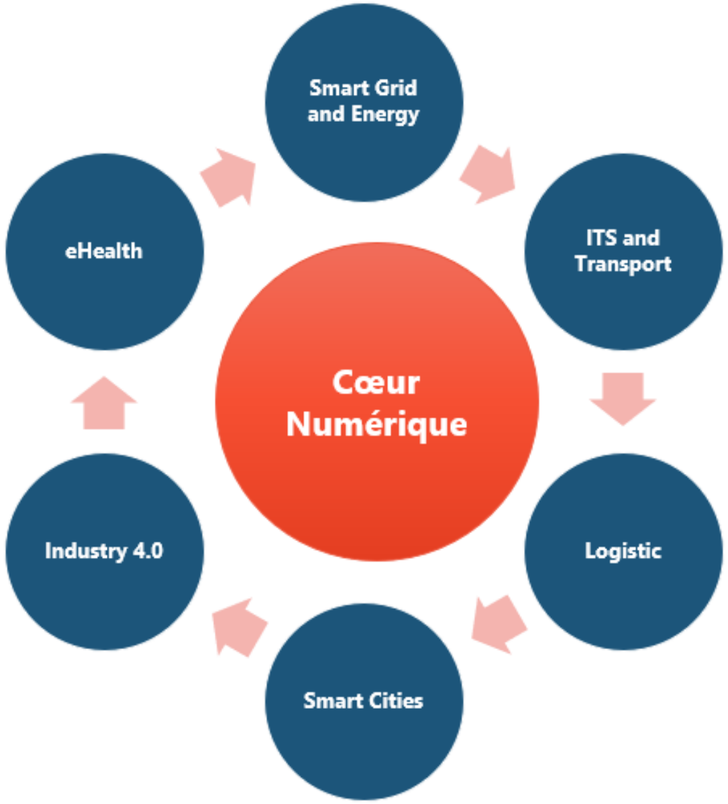
Vers des services multi-sectoriels dans les écosystèmes

5G – Conception jointe avec les verticaux



Embarquement dans les réseaux de fonctionnalités de tiers, liées aux services,
Cœur ouvert par des API (Interfaces de programmation d'applications)

6G – Systèmes multisectoriels, multi-acteurs Création jointe de valeur



Partage et orchestration dynamique d'un large spectre de fonctionnalités embarquées et de données et d'agents d'IA
Cœur ouvert par des API (Interfaces de programmation d'applications)
IA Agentique

01e

RECOMMANDATIONS

Premières recommandations transversales

- Élaborer une ou des visions pour motiver les interactions fortes inter filières.
- Promouvoir et faciliter la coordination entre acteurs européens

02a

CONTEXTE ET OBJECTIFS

Des transformations qui redéfinissent les chaînes de valeur

Les infrastructures numériques — réseaux, cloud, IA, edge, NTN, plus des briques logicielles nécessaires à l'orchestration des services numériques — connaissent une transformation profonde, sous l'effet de plusieurs évolutions technologiques majeures.

Cela impacte de façon de plus en plus importante les acteurs traditionnels de leurs chaînes de valeurs (fournisseurs de composants matériels et logiciels, équipementiers, opérateurs réseaux et cloud, producteurs et distributeurs de services, contenus, applications et agents…).

Les transformations sont souvent portées par des paradigmes venus des écosystèmes cloud, largement dominés par des acteurs extérieurs à la filière télécom, au premier rang desquels les hyperscalers américains.

CE QUI EST EN JEU

- Souveraineté numérique, autonomie stratégique France / Europe
- Compétitivité des opérateurs télécom, des équipementiers… impact sur les OIV
- Gouvernance des données et de l'IA
- Nouveaux paradigmes de services
  Création de valeur sectorielle et multisectorielle
  Résilience des services numériques essentiels

Des transformations qui redéfinissent les chaînes de valeur

Ce livre blanc adopte une vision systémique : les infrastructures numériques comme un continuum

- *technologique horizontal et vertical,*
- *économique*
- *stratégique*

Dont les composants deviennent de plus en plus indissociables.

CE QUI EST EN JEU

- Souveraineté numérique, autonomie stratégique France / Europe
- Compétitivité des opérateurs télécom, des équipementiers… impact sur les OIV
- Gouvernance des données et de l'IA
- Nouveaux paradigmes de services
  Création de valeur sectorielle et multisectorielle
  Résilience des services numériques essentiels

01
Poser une vision holistique de l'écosystème face aux transformations en cours

02
Analyser opportunités et risques pour les acteurs et pour nos sociétés et nos économies

03
Faire des recommandations pour faciliter la construction d'un plan d'action global face aux opportunités et aux risques

02c

LES RECOMMENDATIONS SPECIFIQUES

Recommandation #2

- Les convergences technologiques ne produiront pleinement leurs effets que si elles s'accompagnent de l'émergence de **nouveaux modèles économiques** adaptés.
- Les pouvoirs publics devraient donc promouvoir et soutenir, au même titre que les innovations technologiques, la conception, l'expérimentation et la diffusion de modèles économiques innovants permettant
  - de **structurer de nouvelles chaînes de valeur,**
  - de favoriser le **partage des investissements** et des risques et un partage équitable des bénéficies globaux,
  - **d'accroître la compétitivité** des acteurs européens des infrastructures numériques.
- Cela permettrait une plus grande capacité de création de valeur pour les entreprises de divers secteurs d'activité et un meilleur positionnement les citoyens.
- Quelques pistes d'action :
  - Lancer des appels à projets centrés autant sur l'innovation économique et organisationnelle que sur l'innovation technologique.
  - Adapter, lorsque nécessaire, les cadres réglementaires afin de faciliter les coopérations entre filières.
  - Soutenir des démonstrateurs intégrant simultanément innovation technologique et innovation économique.
  - Organiser des groupes de travail dédiés aux nouveaux modèles économiques, en s'appuyant sur les pôles, les IRT, etc.
  - Orienter les appels d'offre publics pour y inclure des clauses de souveraineté et de résilience.
- Tout cela devrait mener à ce que les industriels visualisent plus tangiblement le potentiel de mise en œuvre de modèles de co-investissement et de partage des risques et des revenus entre acteurs des différentes filières.

02d

LES RECOMMENDATIONS SPECIFIQUES

Recommandation #3

- Dans le cadre des **objectifs réalisables de souveraineté**, il est nécessaire d'évaluer les **dépendances existantes** et de définir des objectifs exigeants mais réalistes, d'évaluer les risques en lien avec les **partenaires de confiance** et prévoir les moyens pour les réduire, pour le court et le plus long terme.
- Il faudra en particulier :
  - Mettre en place une cartographie régulièrement actualisée des dépendances technologiques et industrielles, avec une approche transversale à toute la chaîne technologique et de valeur.
  - Définir, dans un **cadre multi-filière, des niveaux cibles de réduction des dépendances en fonction des risques. Le cadre holistique multi-filière est le seul qui permettrait des positionnements efficaces dans ce contexte.**
  - S'appuyer sur l'Indice de Résilience Numérique (IRN) pour aider les organisations à réfléchir à leurs dépendances en termes de solutions de communication internes et externes

03

LES ENJEUX DE SOUVERAINETÉ

Des contraintes de souveraineté adaptatives, pilotées dynamiquement

- Une souveraineté numérique totale — de la maîtrise des composants aux services — est irréaliste à court et moyen termes, malgré les compétences françaises et européennes.

- L'enjeu n'est donc pas l'autonomie absolue, mais de définir les niveaux de maîtrise indispensables à la sécurité nationale, la résilience, la compétitivité et la capacité d'innovation, **en lien direct avec des nouveaux modèles économiques à concevoir, notamment fédératifs au niveau européen.**
- Chaque service, chaque usage, peut requérir un niveau de souveraineté différent, selon les acteurs impliqués, les données manipulées, etc.

Rec #4 - Compte tenu du caractère structurant et transversal des orchestrateurs, notamment multisectoriels, il est recommandé de lancer **un programme national ou européen de recherche et d'innovation associant technologies, économie et sciences sociales afin de concevoir les architectures d'orchestration, les mécanismes de décision et les modèles économiques permettant la mise en œuvre opérationnelle de cette souveraineté adaptative.**

★

L'idée forte

Les orchestrateurs sensibles à la souveraineté, IA-natifs

De nouveaux orchestrateurs, IA-natifs, sélectionnent, allouent et adaptent dynamiquement les composants et ressources (calcul, réseau, stockage, données, agents) selon le niveau de souveraineté requis par chaque usage — dans le respect des régulations.

Cadres sectoriel et multisectoriel

❑ *Résultat : le niveau de souveraineté attendu est assuré tout en optimisant performances et coûts — sans imposer par défaut un niveau maximal, qui pourrait bloquer l'innovation ou la création de valeur.*

Il ne s'agit pas ici de se focaliser sur un composant, mais concevoir les solutions qui permettront de mettre en œuvre et d'articuler les divers composants et les nouveaux modèles économiques, notamment dans un cadre multisectoriel.

04a

LE PÉRIMÈTRE DU LIVRE BLANC

Un continuum numérique, horizontal et vertical

↔ Horizontal

Le cloud sort des grands data centers et se dissémine jusqu'aux objets connectés, via le mobile edge computing — où les points de présence télécom intègrent calcul et stockage. Résultat : des services cloud plus performants (latence) et plus sûrs.

↕ Vertical

Du composant matériel et logiciel jusqu'aux applications et services offerts par les différents secteurs d'activité — avec une tendance émergente vers des services multisectoriels.

Pour les 2

Les réseaux non terrestres

Les constellations de satellites embarquent déjà calcul et stockage : une intelligence dont l'impact potentiel, dans un contexte hybride civil-militaire, est majeur pour la souveraineté.

Un focus et diverses recommandations sur les NTN

Rec #8 - Pour garantir la souveraineté spatiale de la France et de l'Europe sur le volet critique des infrastructure numériques, plusieurs axes doivent être adressés au travers de la formulation d'un programme tendant à :

- Assurer une autonomie dans l'ensemble de la chaine de valeur, telle que décrite dans ce document
- Valoriser la complémentarité TN-NTN et l'opportunité de la 5G et de la 6G
- Prendre en compte le secteur aval dans la conception des politiques spatiales, en différentiant les divers besoins : large bande, connectivité d'objets, services critiques, etc.
- Appréhender la dualité civil-militaire de l'espace extra-atmosphérique
- Faire du cadre réglementaire de la LOS (Loi sur les Opérations Spatiales) française un avantage compétitif pour l'industrie européenne.

Une analyse des nouveaux modèles économiques est indispensable ; en effet, le risque est que les acteurs ayant pris des positions fortes dans le cadre des NTN absorbent l'intégralité du marché des télécommunications, en s'appuyant sur les réseaux nationaux pour offrir à leur client des services globaux.

Rec #11

- **Construire une autonomie stratégique européenne sur l'ensemble de la chaîne de valeur des réseaux non terrestres (NTN), ce qui inclus l'embarquement de l'IA.**

05a

LA PLACE CENTRALE DE L'INTELLIGENCE ARTIFICIELLE

L’IA pour les IN et les IN pour l’IA

- Outil incontournable pour concevoir, déployer et opérer des infrastructures convergentes de plus en plus complexes.

- L’IA devient de plus en plus distribuée, notamment dans le cadre de l’IA agentique, et impose de nouvelles exigences aux infrastructures numérique.
  - L'IA génère un trafic bidirectionnel et symétrique — contrairement au streaming vidéo mettant sous forte pression le lien montant des réseaux mobiles.
  - Le trafic machine-to-machine est désormais majoritaire dans les cœurs de réseaux, porté notamment par les applications LLM.

M2M

trafic désormais majoritaire dans les réseaux, porté par l'IA

05b

LA PLACE CENTRALE DE L'INTELLIGENCE ARTIFICIELLE

L'IA agentique redéfinit usages et gouvernance

- Il est aujourd'hui admis que l'IA agentique a un pouvoir de transformation majeur de tous les secteurs d'activité, avec une promesse de très forte création de valeur.

Exploiter pleinement ce potentiel suppose toutefois de mettre en œuvre des **mécanismes innovants de gouvernance de l'IA et des données**, notamment dans un cadre multi-acteurs, potentiellement multi-sectoriel et en respectant les règlementations.

Cela requiert une traduction automatique de la gouvernance humaine des entreprises en une gouvernance numérique, la génération automatique des mandats donnés aux agents, la mise en œuvre des contrôles d'accès et d'usage entre agents, ainsi que de traçabilité, la supervision des agents tout en respectant le niveau d'autonomie souhaité, etc.

OPPORTUNITÉ STRATÉGIQUE

Rec#11 - Les opérateurs d'infrastructures numériques, de part leur position transverse, **peuvent proposer un plan de gouvernance de l'IA et des données en mode PaaS — nouveau levier de croissance pour eux, et levier de souveraineté nationale et européenne**.
Nous parlons ici d'une composante logicielle offerte en "mode service".

06

L'OUVERTURE DES INFRASTRUCTURES NUMÉRIQUES

Vers des IN en mode PaaS et vers des marketplaces de composants : un changement de paradigme

1

Réseaux ouverts via API

Network as a Service : instanciation des ressources à la demande, en temps réel, contrôlée par le client.

→

2

Composants tiers intégrés

Les entreprises clientes orchestrent leurs propres services avec des composants logiciels répondant à des besoins spécifiques.

→

3

Marketplaces de composants

Nouvelles places de marché — analogie avec les stores d'applications mobiles — ouvrant de nouvelles lignes d'affaires.

Ceci ouvre de nouvelles lignes d'affaires pour les opérateurs d'infrastructures numériques et de nouveaux débouchés pour les fournisseurs de composants.
Mais surtout, une grande agilité dans la création de nouveaux services
Rec#7 - une stratégie claire d'ouverture, associée à une gouvernance européenne rigoureuse, est essentielle pour bâtir des infrastructures numériques souveraines, résilientes et innovantes, tout en maîtrisant les enjeux de sécurité, de propriété intellectuelle et de standardisation. Il est fortement souhaitable d'analyser plus en détail le besoin d'orienter des financements vers des innovations européennes en avance, ce qui est détaillé dans ce document, d'identifier les briques technologiques pour lesquelles l'open source constitue un avantage stratégique et d'élaborer une feuille de route coordonnée entre les initiatives nationales et européennes.

07

LES COMPOSANTS TECHNOLOGIQUES

La souveraineté se joue *fortement* au niveau des briques technologiques

Électronique | **Optique** | **Quantique** | **Logiciel (calcul, stockage, IA, HPC)**

Conception des briques

Sujet clé de souveraineté et de propriété intellectuelle, fortement adossé à la recherche académique.
Réflexions sur les couplages matériel-logiciel

« Fonderie » des composants

Mise en œuvre matérielle — hors périmètre de ce document (CSF électronique, quantique).

Open source — atouts

Ouverture et interopérabilité, accélération des déploiements, innovation collaborative, réduction de la dépendance à un fournisseur unique.

Open source — risques

Propriété intellectuelle fragilisée, gestion des vulnérabilités, fragmentation des écosystèmes — nécessite une gouvernance européenne rigoureuse.

FILIÈRE INFRASTRUCTURES NUMÉRIQUES

08

Synthèse des axes de travail pour retrouver un positionnement fort

1. Vers une souveraineté faisable et Gestion dynamique de contraintes de souveraineté adaptatives
2. Infrastructures Numériques en mode « as a service », ouverture
3. Fédérations multisectorielles
4. Gouvernance de l’IA (notamment agentique) et des données
5. Matières premières, composants: partenaires de confiance, rôle de l’open source
6. Services multisectoriels

09

UNE SUITE DE RECOMMANDATIONS TRANSVERSALLES ET ESPECIFIQUES AUX ENJEUX IDENTIFIES

Dans le cadre de cinq priorités

1. Renforcer, par le numérique et l'IA, le pouvoir d'agir des citoyens et des entreprises
2. Faciliter le positionnement des entreprises du numérique, des grands groupes aux start-ups
3. Faciliter l'innovation et l'émergence de services à fort impact sociétal et économique
4. Maintenir et développer une recherche académique de haut niveau, en synergie forte avec le monde économique
5. Protéger citoyens et entreprises contre toute forme d’attaque facilité par le numérique (données, services, biens, personnes)

★

Principale recommandation globale : Une impulsion publique transversale

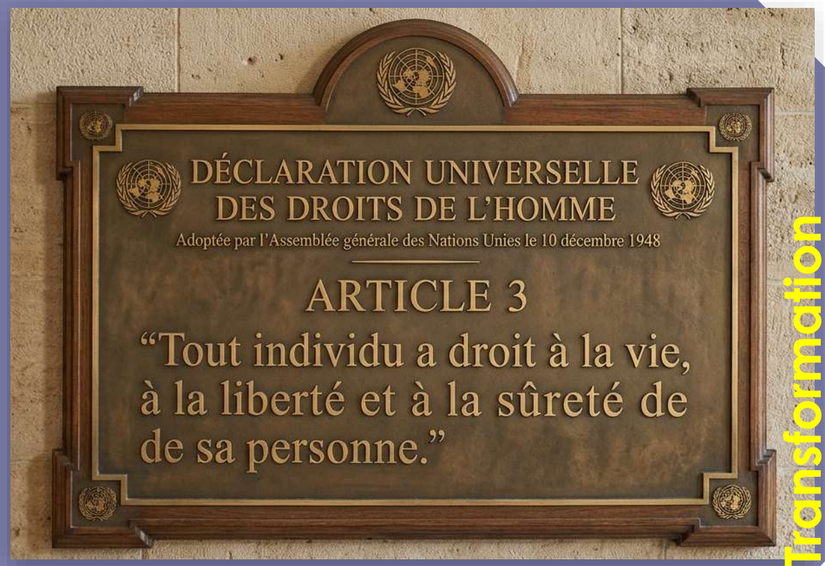
Fédérer les filières pertinentes, aux interactions historiquement faibles, autour de nouveaux modèles économiques, se basant sur une stratégie R&D&I transversale coconstruite notamment avec les CSF, sur les articulations inter-PEPR (Réseaux du Futur, Cloud, IA, Quantique, Cyber, Electronique…), sur des efforts accrues d’impact à la normalisation en dépassant la 6G pour y intégrer notamment des organismes liés à l’IA et au cloud (France6G et autres acteurs d’autres filières), sur un continuum recherche-innovation-marché (FRAMExG, pôles de compétitivité…), avec notamment la production de feuilles de route inter-CSF.

4. Cyber et confiance des infrastructures

Emmanuel Dotaro
VP
Thales fellow

FILIÈRE
INFRASTRUCTURES
NUMÉRIQUES

Un peu de perspective « sociétale »



Transformation numérique

Monde numérique

- Sans sécurité, pas de **confiance** dans les services numériques.
- Sans confiance, pas **d'adoption** durable par la société
  - Citoyens
  - Entreprises
  - Innovations (sectorielles)
- Sans **résilience**, pas de continuité des services **essentiels**:
  - santé, énergie, transport, finance, communication, administration,…
- Sans **maîtrise** des dépendances, pas de souveraineté de liberté réelle de choix.
- **Sans sécurité, l'IA et les infrastructures numériques peuvent amplifier les vulnérabilités, les inégalités et les atteintes aux droits**

la sécurité numérique conditionne le droit à: l'exercice des libertés, la protection des personnes, la continuité des services essentiels, la confiance économique, l'innovation et la souveraineté.

…Réalité ?

This document may not be reproduced, modified, adapted, published, translated, in any way, in whole or in part or disclosed to a third party without the prior written consent of Thales - © Thales 2015 All rights reserved.

Une typologie alimentée en continu…Mythos etc…

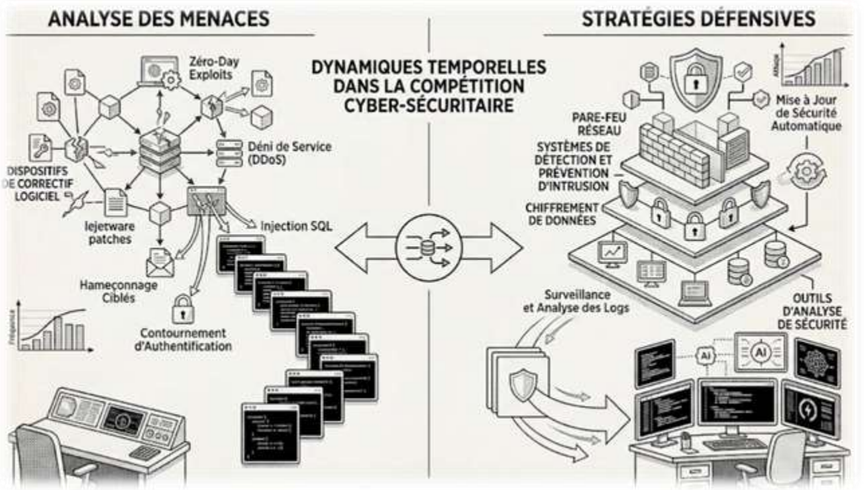
Script kiddie — *Curiosity · low capability · opportunistic*

Hacktivist — *Ideology · DDoS, defacement · 79% of EU attacks ideology-driven*

Organised crime — *Financial · RaaS, double extortion · ransomware = top EU impact*

Insider — *Coercion / error · trusted access · 60% of high-cost telco breaches*

Nation-state / APT — *Espionage · 0-days, Living Off The Land · Salt Typhoon in ≥3 EU states*



This document may not be reproduced, modified, adapted, published, translated, in any way, in whole or in part or disclosed to a third party without the prior written consent of Thales - © Thales 2015 All rights reserved.

SECTORIAL APPLICATIONS

ESSENTIAL ENTITIES HEALTH | ESSENTIAL ENTITIES TRANSPORT | ESSENTIAL ENTITIES ENERGY | ESSENTIAL ENTITIES DEFENCE/BLUE LIGHT | ESSENTIAL ENTITIES IMPORTANT ENTITIES ENTERPRISES | MASS MARKET CITIZENS

DATASPACE | DATASPACE | DATASPACE | DATASPACE | DATASPACE | DATASPACE

KNOWLEDGE GRAPH | KNOWLEDGE GRAPH

AGENTIC AI PLANE

Model Context Protocol | RAG | NEURO SYMBOLIC GUARDIAN

Multi-Lateral, Multi-stakeholders,

AI-based Resource & services scheduling/orchestration

Compute(s) | Network(s) | Security(s) | AIaaS(s)

MISSION ORIENTED | 5G 6G | AI NATIVE | FEDERATED LEARNING | SMART ALLOCATION | 3C | TELCO CLOUD | TINYML | ON PREMISE | PUBLIC | PRIVATE | PUBLIC | SLM | WAN | PRIVATE | PUBLIC

FULL E2E FEDERATED SecOps

Governance CTI | Federated IAM | Detection | Response | ZTA/DCS/CC

MUTI-CLOUD MANAGEMENT | LLM | LEGACY MIGRATION | HYPERSCALER | SOVEREIGN CLOUD | LLM

FAR EDGE | NEAR EDGE | CLOUD/DATA CENTER

OPEN

This document may not be reproduced, modified, adapted, published, translated, in any way, in whole or in part or disclosed to a third party without the prior written consent of Thales - © Thales 2015 All rights

Convergence pour le meilleur ? … +/- surface d'attaque ?

Avantages intrinsèques opportunités

Interfaces ouvertes (propagation)

Chaîne d'approvisionnement (SBOM,…)

IA

OSS

SecOps Opérations distribuées

XaaS

Lock_in

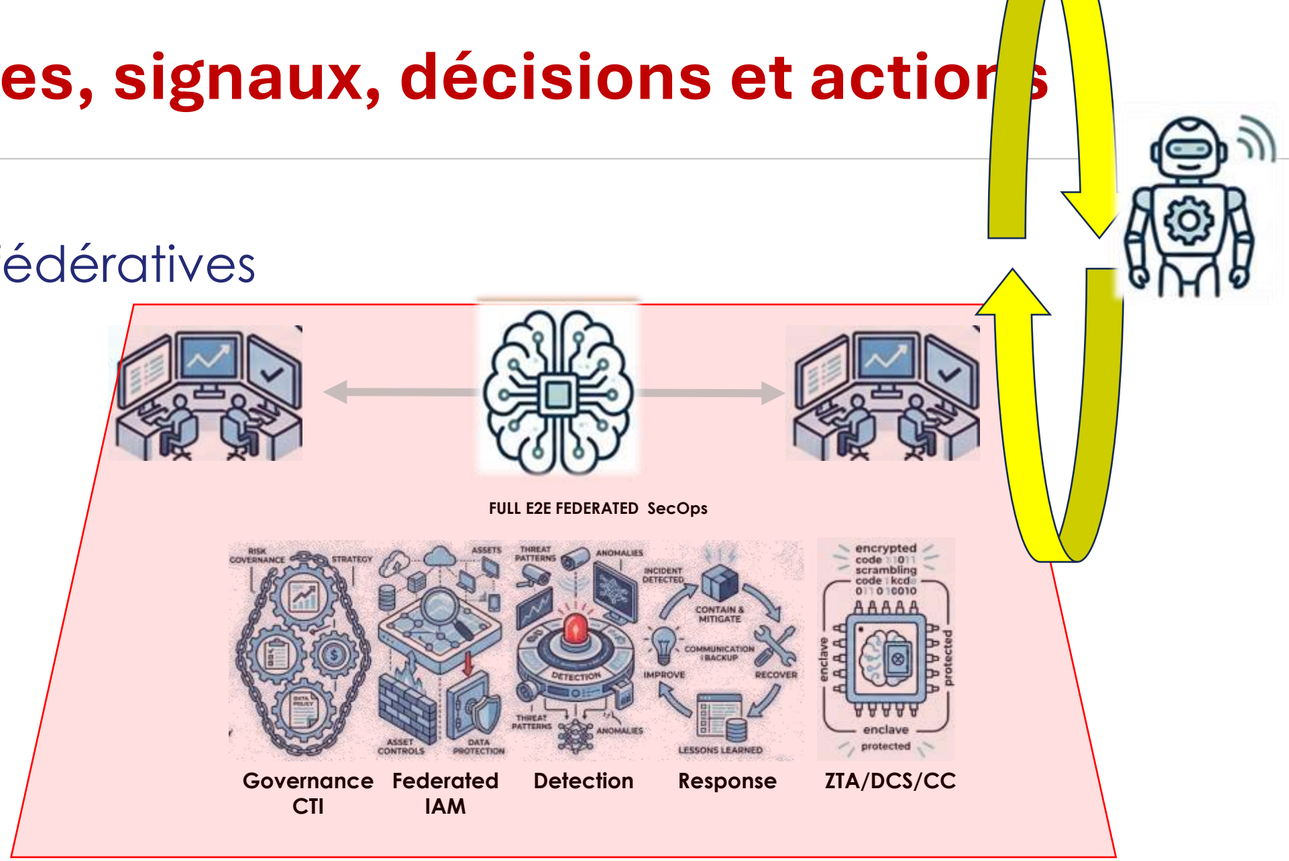
CTI partagée ?

Coopération >> agnostique

This document may not be reproduced, modified, adapted, published, translated, in any way, in whole or in part or disclosed to a third party without the prior written consent of Thales - © Thales 2015 All rights reserved.

Cohérence: politiques, signaux, décisions et actions

Approches convergentes fédératives



GOUVERNANCE & CONFIANCE	Politiques communes • identité fédérée • conformité • preuves d'assurance
PROTECTION	Zero Trust • IAM personnes / workloads / agents • chiffrement • sécurité de la chaîne logicielle
DÉTECTION	Télémétrie cross-domain • CTI partagée • xDR fédéré • détection d'anomalies assistée par IA
RÉPONSE & RÉSILIENCE	SOAR orchestré • confinement local • remédiation coordonnée • reprise et apprentissage

This document may not be reproduced, modified, adapted, published, translated, in any way, in whole or in part or disclosed to a third party without the prior written consent of Thales - © Thales 2015 All rights reserved.

De l’admission à la résilience



This document may not be reproduced, modified, adapted, published, translated, in any way, in whole or in part or disclosed to a third party without the prior written consent of Thales - © Thales 2015 All rights reserved.

Security as a Service : industrialiser la confiance sans la centraliser

Protection as a Service

- IAM fédéré et identités attestées.
- Zero Trust, chiffrement, DLP et gestion des secrets.

Detection as a Service

- Télémétrie normalisée et partage de renseignement.
- xDR inter-domaines, corrélation multi-couches et supervision 24/7.

Response as a Service

- Playbooks orchestrés, automatisation sous contrôle humain.
- Confinement à l'edge, coordination SOC/CSIRT et retour d'expérience.

Compliance as a Service

- Évidences NIS2/CRA/AI Act, SBOM et gestion des vulnérabilités.
- Assurance multi-niveaux selon le risque et le secteur.

This document may not be reproduced, modified, adapted, published, translated, in any way, in whole or in part or disclosed to a third party without the prior written permission of Thales. All rights reserved.

Quelques (bons) principes

- **Confiance zéro, vérifiée en continu.**
- **Identités distinctes : humain, workload, agent IA.**
- **Sécurité by design (! ne veut pas dire statique) et chaîne logicielle traçable.**
- **Données protégées en transit, au repos et en usage.**
- **Détection et réponse fédérées, avec CTI partagée.**
- **Résilience locale : modes dégradés, sauvegardes, reprise**
- **Assurance proportionnée au risque (MLS): certification, tests continus, transparence et auditabilité.**

This document may not be reproduced, modified, adapted, published, translated, in any way, in whole or in part or disclosed to a third party without the prior written consent of Thales - © Thales 2015 All rights reserved.

Conclusion : faire de la cybersécurité un avantage compétitif

Nb: petit aparté sur la confiance

This document may not be reproduced, modified, adapted, published, translated, in any way, in whole or in part or disclosed to a third party without the prior written consent of Thales - © Thales 2015 All rights reserved.

Merci !

N’hésitez pas à poser vos questions !



FILIÈRE
INFRASTRUCTURES
NUMÉRIQUES

1 FOUNDATIONS

Security starts with the CIA triad — and EURO-3C extends it

Confidentiality, Integrity, Availability is the baseline; a federated sovereign continuum adds resilience, sovereignty, accountability and privacy.

Confidentiality

Data disclosed only to authorised identities — encryption, access control, data-centric protection.

Integrity

Data and systems are accurate and untampered — signatures, attestation, SBOMs.

Availability

Services resist and recover from disruption — resilience, redundancy, anti-DDoS.

EURO-3C extended properties

Resilience

Back-up modes, root of trust, graceful degradation across federated domains.

Sovereignty

EU data jurisdiction, EU values and leading regulation, control over critical tech, non-EU supplier independence.

Accountability

Traceability, audit, explainable AI, **evidence-based** trust.

Privacy

Data protection by design (GDPR), data-centric trust, Privacy Enhancing Technologies (PET).

inspired from NIST Cybersecurity Glossary, I recommend to check “our” glossary against this one

This document may not be reproduced, modified, adapted, published, translated, in any way, in whole or in part or disclosed to a third party without the prior written consent of Thales - © Thales 2015 All rights reserved.

FRAMEWORK

NIST CSF 2.0: Govern is cross-cutting; the rest maps to the lifecycle



Governance is not a phase — it steers Identify, Protect, Detect, Respond, Recover across every EURO-3C security workflow and beyond this project should pave the way for next steps covering the convergence

GOVERN — strategy, policy, risk; cross-cutting across all functions

Identify	Protect	Detect	Respond	Recover
Assets, risks, supply chain, posture	IAMs, data security, platform hardening	Continuous monitoring, anomaly detection	Incident response, mitigation	Resilience, restoration, lessons
Domain admission	***phase*** **Service on-boarding**	**Runtime predictive**	**Runtime reactive**	**Cooperative response East–West**

security functions map NIST Cybersecurity Framework 2.0

This document may not be reproduced, modified, adapted, published, translated, in any way, in whole or in part or disclosed to a third party without the prior written consent of Thales - © Thales 2015 All rights reserved.

2 ECONOMICS : AI is in the game

Cybercrime is a $10.5T economy — and growing

A record-high average breach cost and AI-enabled attacks make security investment a board-level economic issue. Considering the demand side !

$10.5T

Global cybercrime cost, 2025

→ $12.2T by 2031

$4.99M

Avg. data breach cost (record)

+12% YoY

241 days

Breach lifecycle (identify + contain)

9-year low

$1.9M

Saved by AI/automation in SecOps

80 days faster

Cost by sector (USD M, IBM 2025)



**IBM "Communications" = media/PR, not telecom operators.*

AI is a double-edged lever

- 1 in 4 malicious breaches now AI-enabled (+56% YoY); avg. cost $6M
- 97% of AI-incident victims lacked AI access controls
- AI/automation saves ~$2M & 80 days when governed
- 85% plan to raise security spend after seeing frontier-AI threats

Source: IBM Cost of a Data Breach 2026, Cybersecurity Ventures 2025

This document may not be reproduced, modified, adapted, published, translated, in any way, in whole or in part or disclosed to a third party without the prior written consent of Thales - © Thales 2015 All rights reserved.

OPEN

THALES

Supply-chain & human-element breaches are rising fast

Third-party involvement doubled; DDoS dominates EU incident volume; ransomware remains the most impactful EU threat.

Verizon DBIR 2025 — global breaches

22,052 incidents · 12,195 confirmed breaches · 139 countries

Human element	**~60%**
Ransomware in breaches	**44% (+37%)**
Third-party / supply chain	**30% (doubled)**
Credential abuse	**22%**
Vulnerability exploitation	**20% (+34%)**

ENISA Threat Landscape 2025 — EU

4,875 incidents analysed (Jul 2024–Jun 2025)

DDoS share of incidents	**77%**
Incidents hitting NIS2 essential entities	**53.7%**
Ransomware = most impactful threat	**▼ 11% vol.**
Phishing as initial vector	**~60%**
Attacks that were AI-supported	**>80% (SE)**

Attacker objectives (EU): ideology 79% · financial 13% · espionage 7%.

Source: Verizon DBIR 2025, ENISA Threat Landscape 2025

This document may not be reproduced, modified, adapted, published, translated, in any way, in whole or in part or disclosed to a third party without the prior written consent of Thales - © Thales 2015 All rights reserved.

3 (security) MARKET

A ~$213B global market growing double-digit — Europe is ~25% of it

Fast-growing segments (confidential computing, PQC, Zero Trust, IAM) are exactly where EURO-3C sits.

$213B

Global infosec spend, 2025

→ $240B in 2026 (+12.5%)

$54.8B

Europe cyber market, 2025

→ $83B by 2030 (8.7% CAGR)

~25%

Europe share of global

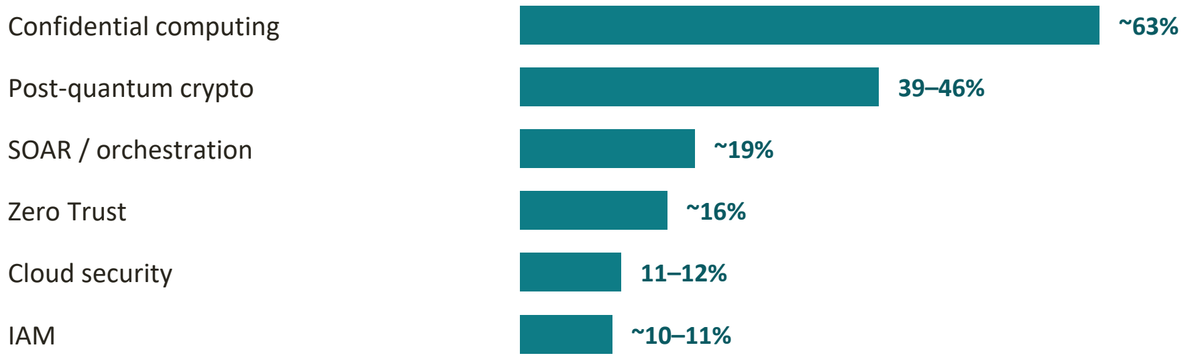
2nd-largest market

9%

Cyber = share of IT budget

median €1.5M (ENISA)

Fast-growing segments (CAGR)



Structural fragmentation (EU)

- **~7,000 EU cyber companies; 90% are SMEs = only 25% of revenue**
- **EU cyber VC funding ~5× lower than the US**
- **Top 20 global vendors hold 66% share; no EU name in the top 5**
- *Analyst figures are estimates — boundaries differ across reports*

CSF can contribute/lead to aggregate/focus the security ecosystem on digital infrastructure and services including SecaaS..;and as such also make a real step on sovereignty

Source: Gartner 2025, MarketsandMarkets Europe, BDO, ENISA NIS Investments 2025

This document may not be reproduced, modified, adapted, published, translated, in any way, in whole or in part or disclosed to a third party without the prior written consent of Thales - © Thales 2015 All rights reserved.