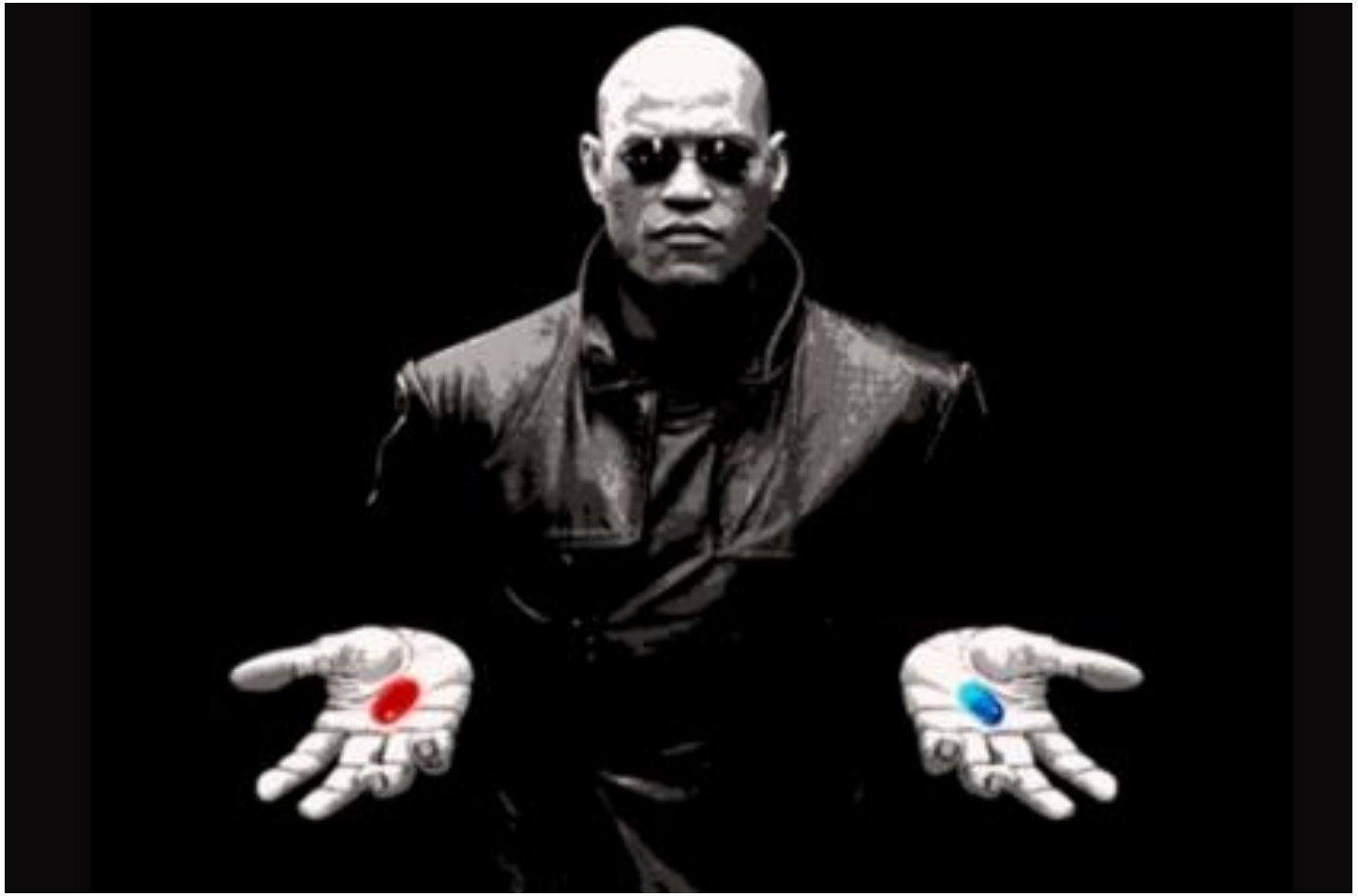
Arnaud Taddei – ITU-T SG17 Chair

Welcome

Why this workshop?
Who are you?
Why are you here?
Context?



Why this workshop?

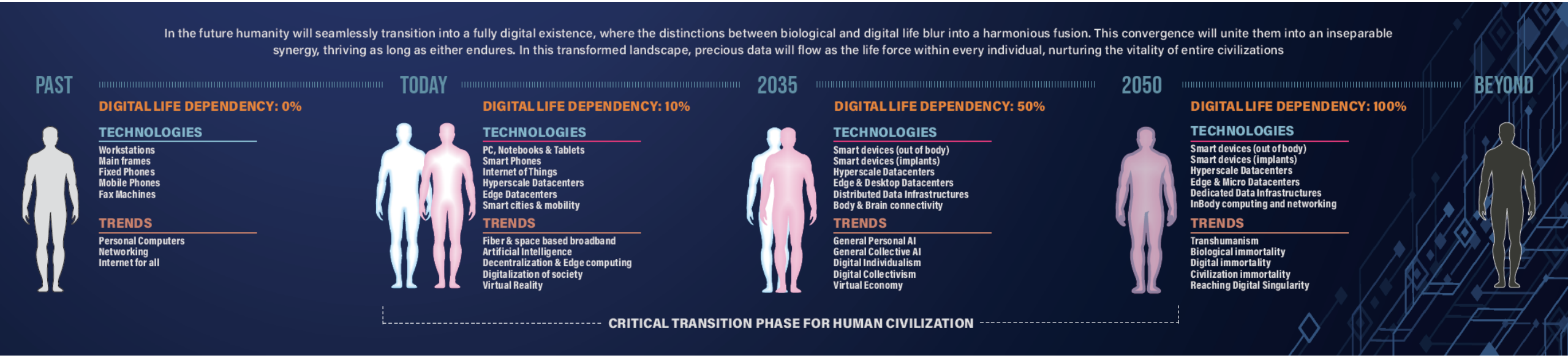
THE BIG PICTURE

OMEGA FASE FRAMEWORK

Frederick Tschernutter

Why do some systems – biological, social, or digital – survive while others collapse and disappear?

Synthetic evolution is exponential, not linear



OMEGA FASE FRAMEWORK

THE QUESTION

- For 40 years we built the internet as a network that connects machines.
- The next phase will connect intelligence (Human and Artificial).
- Autonomous agents + Humans on a shared common infrastructure.

What infrastructure do we need when intelligence itself becomes a networked phenomenon and when some of that intelligence is no longer human but artificial?

Perhaps we need a new layer? Let's call it the sovereignty plane

OMEGA FASE FRAMEWORK

There is no protocol level mechanism to answer 3 fundamental questions about any agent operating on the network

HUMANS - INFRASTRUCTURE - AGENTS

ACCOUNTABILITY

Who is responsible for this agent?

Which human or organization bears accountability for its actions?

What are its boundaries?

What is it authorized to do, and what is it not?

How is it identified?

Not the machine it runs o, but the agent itself as a persistent, accountable entity.

This is not a feature gap. It is an existential architectural deficit

ARCHITECURAL DEFICIT?

OMEGA FASE FRAMEWORK

If every autonomous agent is not entangled with a responsible human or organization, bound to them through cryptographic identity, accountability protocols, and enforceable boundaries, then we are building a network of unaccountable intelligences.

Every agent must be entangled with a human principal, and critical data needs to remain under human control

OMEGA FASE FRAMEWORK

HUMANS - INFRASTRUCTURE - AGENTS

ACCOUNTABILITY

ITU-T SG17 Status on Agentic AI Security and Trust

A strategy, A new structure, First work items, A roadmap, A schedule

In general a LOT of work since December 2024 at high cadence

- ITU-T SG17 grew to 400 participants and 57 member states as per strong modernization program
- One new member per month mostly western industry (Thales, Cognizant, Google, Vodafone, etc.)
- First workshop Challenging the status quo on AI Security 11th of July 2025 (LS 2077)
- AI Strategy available to IETF (LS 2106)

Leads to

Restructuring (to be fully approved beginning April)

- Creation of new Question 16 for AI Security including Agentic AI with a carve out for no overlap with IETF!
- Merge of Question 3 and Question for Agentic AI Digital Identity Amendment of Question 7 for Agentic AI

Leads to

Leads to

New Q10 work items

Out of 40 work items on AI security 7 are related to Agentic AI (+20 in draft!)

- X.LLMCC Guidelines for large language model data security based on confidential computing, already sent to IETF per liaison 2108
- X.S-AIA Security requirements and guidelines for Artificial Intelligence agent
- XSTR.sem-AIA Security evaluation methods for Artificial Intelligence agent
- X.sr-taimas Security requirements for terminal-based artificial intelligence multi-agent system
- X.dpidm-aAI Terminology and design guidelines for Agentic AI identity management
- XSTR.gidi Globally interoperable digital identity (including humans/enterprise/non-humans i.e. Agentic AI) Even the European Union contributes!
- XSTR.ltf-AAI Landscape of trust framework for agentic AI

Supports / is supported by

A specific scheduled roadmap through Workshops opened to everyone and SG17 meetings

- **1st Workshop** 30-31st of March - ITU Workshop on "Trustable and Interoperable Digital Identities for Human and Agentic AI"
  - First SG17 Content Week 30th of March - 2nd of April
- **2nd Workshop** 2nd of June - Workshop on globally interoperable digital identity
  - Fifth SG17 Plenary 1-10th of June
- **3rd Workshop** 10th of July - Designing Trust Management for Agentic AI
  - AI for Good 6-10th of July

Leads to

Leads to

How does this translate into Standardization space

Example of SG17! A Weekly cadence to win the Agentic AI pole position …

2024	September	SG17 Plenary	6 AI work items established including key ones as X.sr-ai
	Oct - March	Interregnum	
2025	April	SG17 P	
	July	AI For Go	
	August	Correspond	
	September	WP4/17 Plena	
	October	SG21 Workshop,	
	November	IETF + OECD +	
	December	SG17	
2026	January	TSAG	
	March	IETF +	
	April	SG17 Content Week	First Content Week with 2 days Digital Identity Workshop with all parties and discussion on Agentic AI
	May	X.509 Day	Likely discussion on Agentic AI and Trust control plane
	June	SG17 Plenary	Structure in place for AI (Q16, Q3+Q10, MODs of Qs, etc.) expected new workload growth
	July	AI For Good | IETF	New SG17 AI Secrurity Workshop + Perhaps AI WG in IETF

We are here!

Want to have an impact?

30-31st of March SG17 Worskhop in Geneva during the 1st Content Week
Trustable and Interoperable Digital Identities for Human and Agentic AI

2nd of June SG17 Workshop in Geneva during 5th SG17 Plenary Meeting
Globally interoperable digital identity

10th of July SG17 Workshop in Geneva during AI for Good
Designing the Trust Management for Agentic AI

This is for you

Enjoy

Thank you