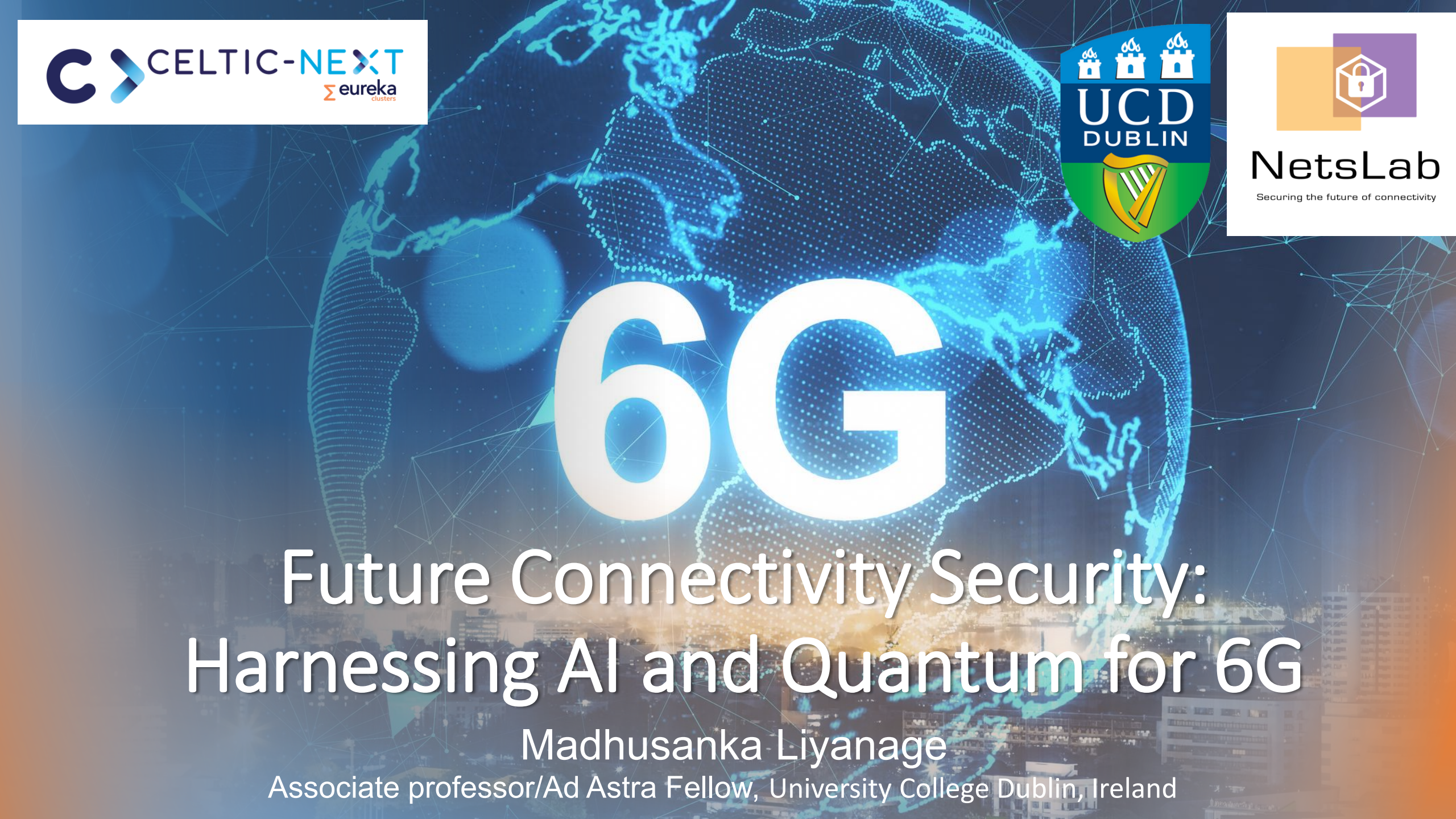


Future Connectivity Security: Harnessing AI and Quantum for 6G

Madhusanka Liyanage
Associate professor/Ad Astra Fellow, University College Dublin, Ireland

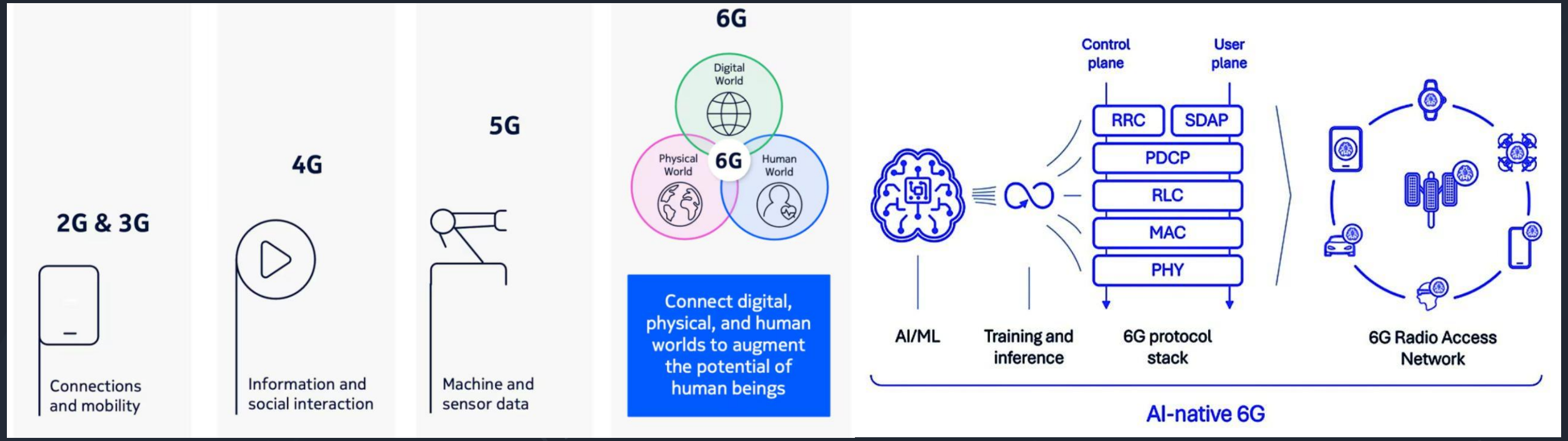
Madhusanka Liyanage

Associate professor/Ad Astra Fellow

University College Dublin, Ireland

Research.com Rising Stars 2025 | Research.com Electronics and Electrical Engineering Ireland 2025 LEADER | Highly Cited Researcher 2025 Clarivate | UCD DUBLIN | NetsLab

- **Director** of Network Softwarization and Security Labs (NetsLab) at the UCD School of CS
- Secure funding for more than **13 Million** Euros and currently PI for Seven large EU level 6G/AI Security related projects
- Co-authored over **300 publications**, including seven books with Wiley and two patents (Google Citations: **22000**+, h-index: **63**+).
- **Expert consultant** at European Union Agency for Cybersecurity (ENISA) **"2020 IEEE ComSoc Outstanding Young Researcher"** award by IEEE ComSoc EMEA
- **Highly Cited Researcher 2025 by Clarivate in the field of Computer Science - Top 0.1% Scientists**
- **World's Top 2% Scientists (2020, 2021, 2022, 2024 and 2024)**
- Ranked among **Best (Top 1000) Rising Stars of Science in 2024 and 2025** by Research.com
- Research Interest: **5G/6G Security, Blockchain for 5G/6G Networks, AI/FL/XAI Security**



The 6G Vision: More Than Speed

- 6G = Intelligence, Autonomy, and Global Integration.

"6G is not just about connectivity; it's about confidence in what connects us."

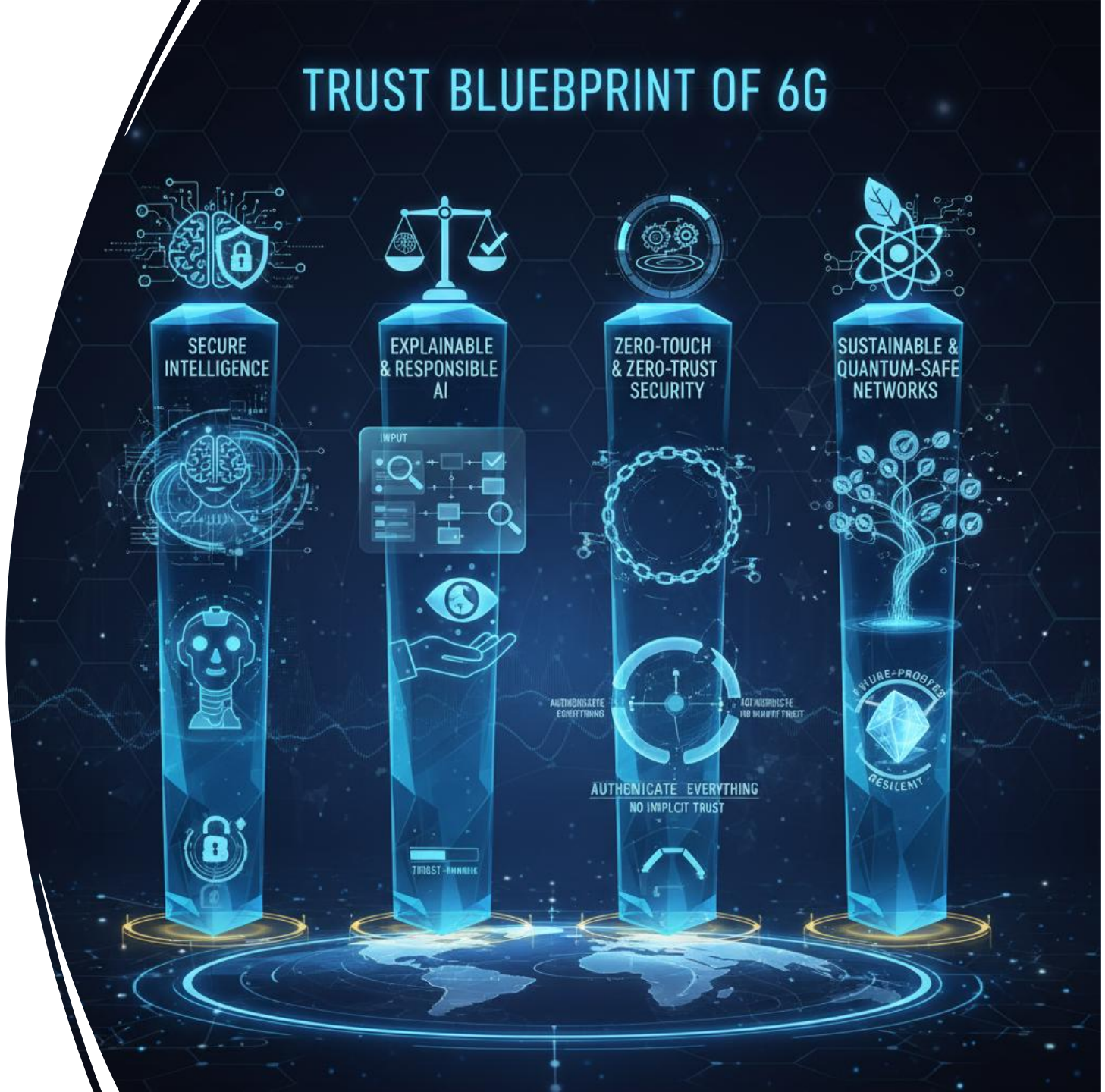
Why Trust Is the New Currency

- Cyber threats, misinformation, generative AI—undermining digital trust.
- 6G will connect **everything**, including autonomous systems and critical infrastructure.
- Each node = both an opportunity and a risk.

Connectivity without trust is like speed without control—powerful, yet fatally risky

The 6G Trust Blueprint

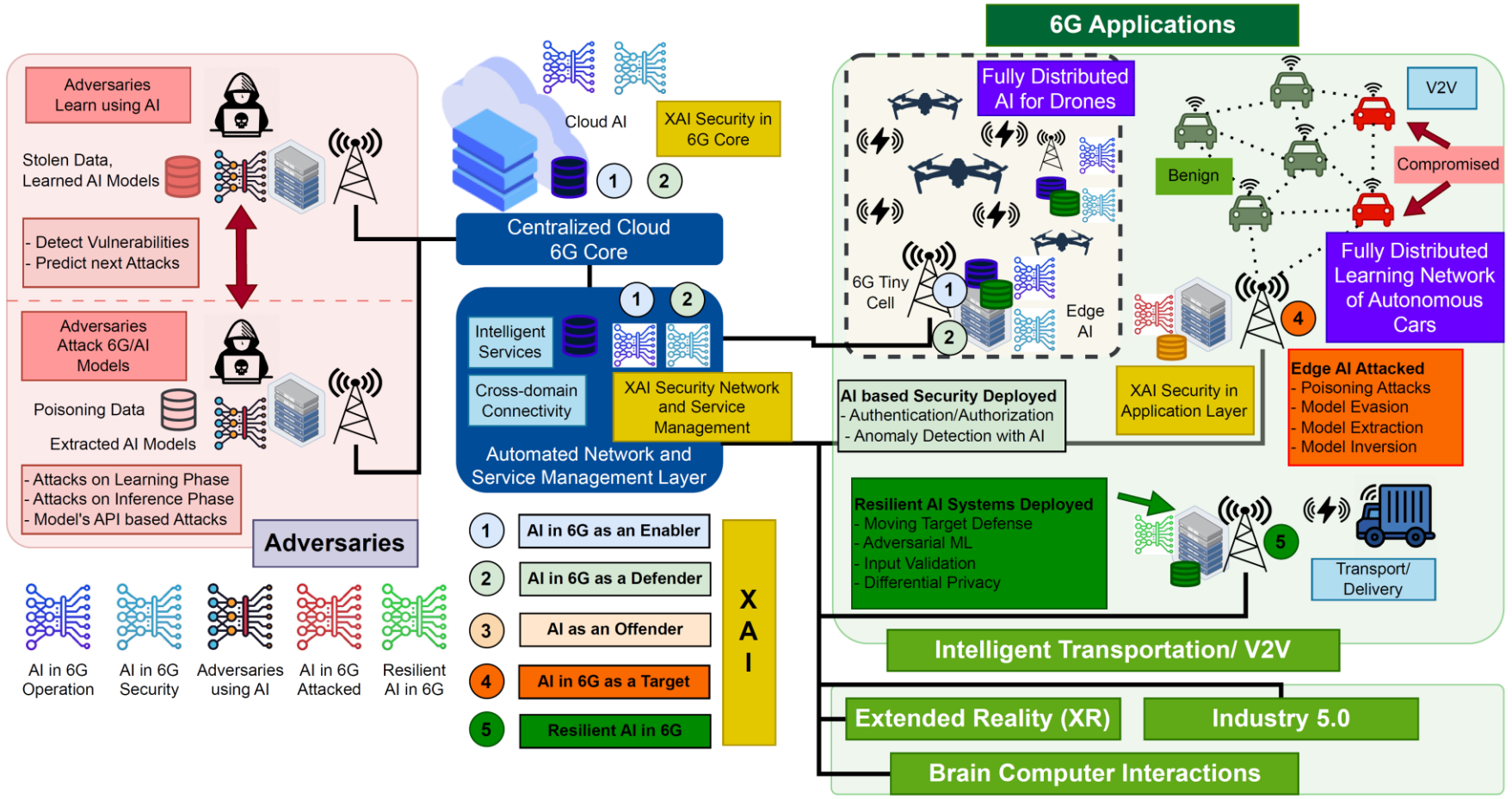
- **Four foundational pillars:**
  - **Secure Intelligence:** Protecting AI-driven decisions.
  - **Explainable & Responsible AI:** Transparency for machine reasoning.
  - **Zero-Touch & Zero-Trust Security:** Autonomic protection.
  - **Sustainable & Quantum-Safe Networks:** Long-term resilience.



UCD DUBLIN | NetsLab

Secure Intelligence: Protecting AI-driven decisions

- AI has multiple roles in 6G Security
  - AI in 6G as a **Defender**
  - AI in 6G as a **Resilient Enabler**
  - AI in 6G as an **Offender**
  - AI in 6G as a **Target**



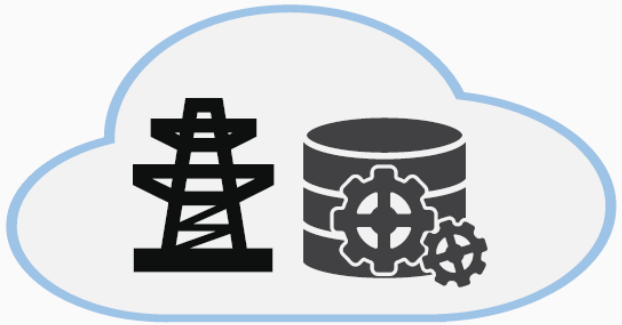
"AI will defend 6G—but only if we defend AI first."

AI-Assisted (5G)

Enhanced 5G Applications

Non-Real-Time

Human-in-the-Loop



RAN & Core Network

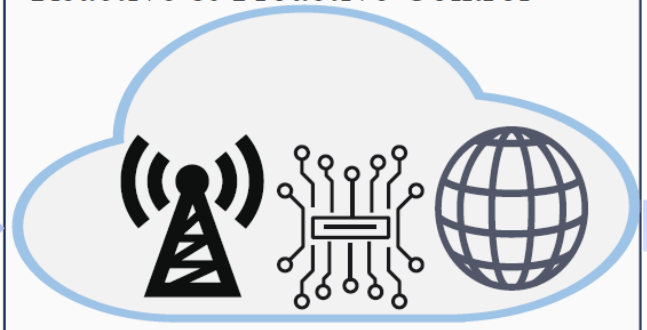
5G Applications

AI-Native (6G)

AI-Native Control Plane

Digital Twins & Continuous Learning

Reactive & Proactive Control



Intelligent RAN & Core

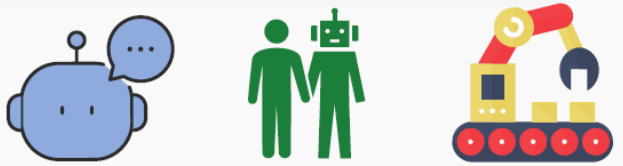
AI-Driven Services

Agentic Autonomous 6G Networks (6G Advanced)

Adaptive AI Agents

Self-Adapt & Self-Coordinate

Retain Memory & Pursue Long-Term



Autonomous AI Agents

Perception Attacks

- Telemetry Poisoning
- Sensor Spoofing

Cognition Attacks

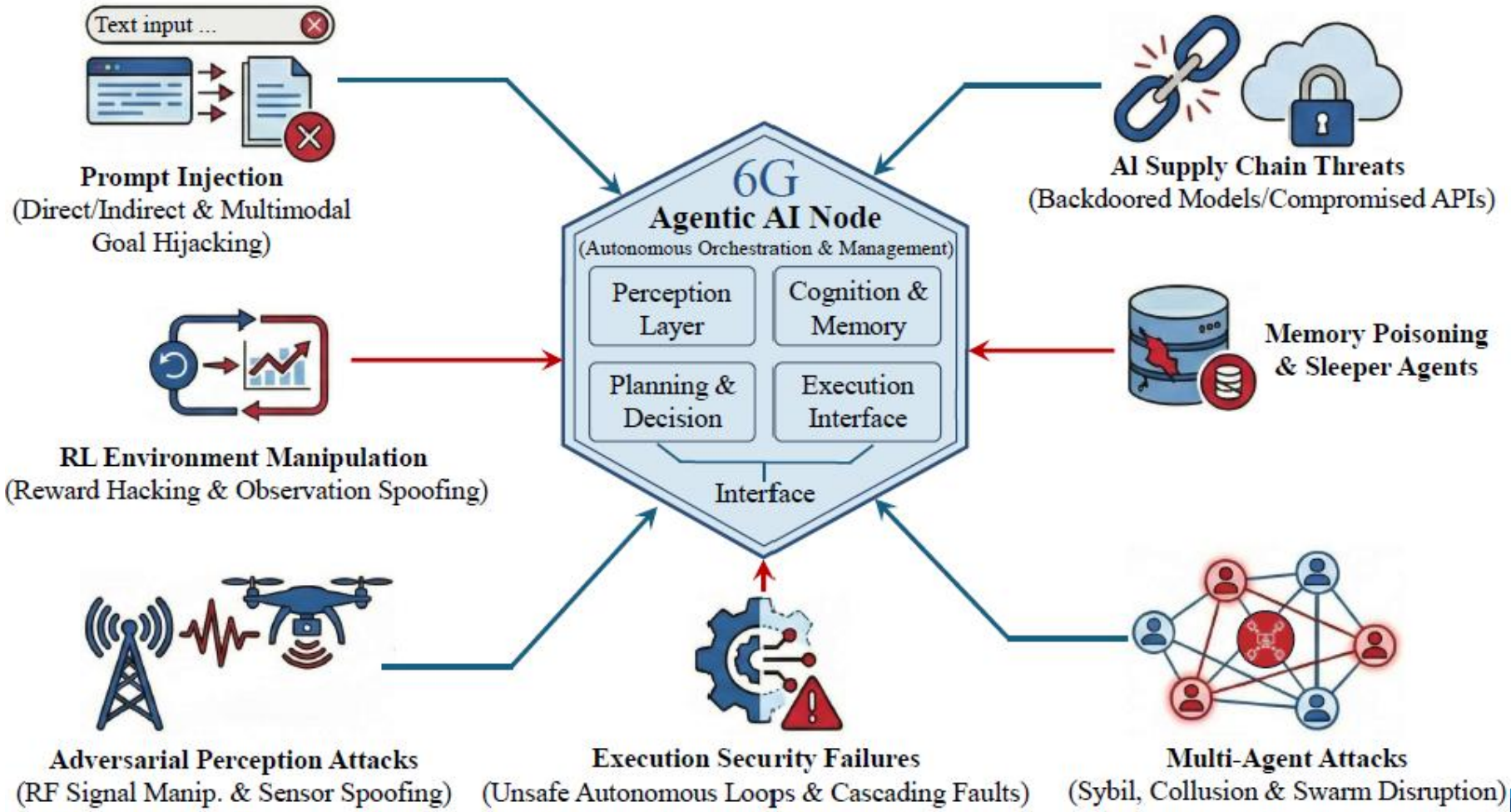
- Memory Poisoning
- Goal Hijacking
- Policy Manipulation
- Reward Shaping

Actuation Attacks:

- Misconfiguration Cascades
- Autonomous Policy Conflicts
- Self-Reinforcing Failures

AI-Assisted → **AI-Native** → **Agentic Autonomous**

Threat Surface for Agentic AI in 6G



NetsLab

How we Trust AI?

Explainable & Responsible AI: Transparency for machine reasoning

- Specially, in critical systems - AI decisions must be **understandable, verifiable, and reliable**.

"If we cannot explain what our AI decides, we cannot trust what our AI defends."

UCD DUBLIN | NetsLab

Before: Traditional Compliance

Forbes

TikTok Sets Aside $1 Billion To Cover Future European Data Privacy Fines

Social Media

BBC

Home News Sport Business Innovation Culture Arts Travel Earth Audio Video Live

Facial recognition: School ID checks lead to GDPR fine

Enterprise Software

FINANCIAL TIMES Subscribe Sign In

Letter + Add to myFT

Letter: Monzo fine exposes fintech compliance gaps

From Marit Rødevand, CEO & Founder, Strise, Oslo, Norway

Save

Published JUL 14 2025

Fintech

SME Today About Advertise Events Calendar Business Wall

SMEs are risking fines of up to £17.5 million for serious breaches of GDPR principles.

BY SME-ADMIN ON JULY 30, 2024

SME

Now: AI Regulations Emerging!

TECH

EU kicks off landmark AI law enforcement as first batch of restrictions enter into force

PUBLISHED MON, FEB 3 2025·2:24 AM EST | UPDATED MON, FEB 3 2025·9:41 AM EST

BLUEPRINT FOR AN AI BILL OF RIGHTS

MAKING AUTOMATED SYSTEMS WORK FOR THE AMERICAN PEOPLE

OSTP

UK Parliament

Parliamentary Bills

HOUSE OF LORDS

UK Parliament > Parliamentary Bills > Artificial Intelligence (Regulation) Bill [HL] Bill feed

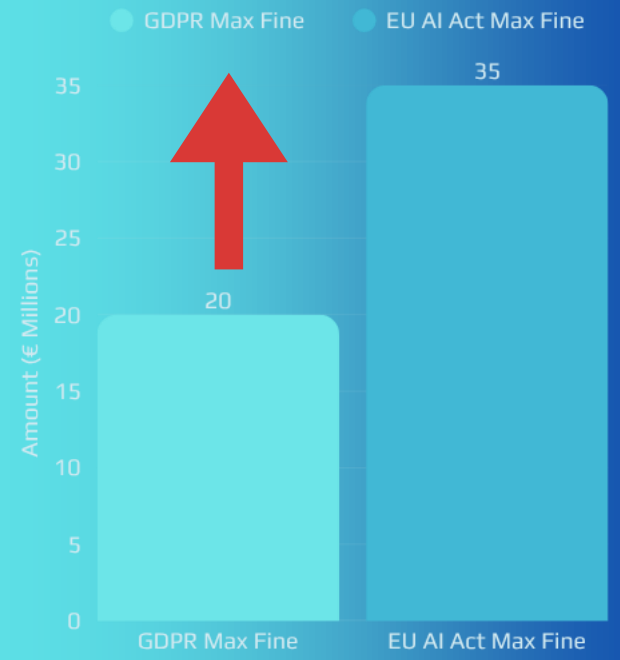
Artificial Intelligence (Regulation) Bill

SOUTH KOREA'S NEW AI FRAMEWORK ACT: A BALANCING ACT BETWEEN INNOVATION AND REGULATION

APRIL 18, 2025

Next?

EU AI Act: Upto €35 M fines non-compliance in AI use



Compliance Hasn't Caught Up with AI

STATIC LEGACY COMPLIANCE

ISO 27001 NIS2 GDPR

YEARLY AUDITS & STATIC POLICIES:
- TOO SLOW FOR AI CHANGES.

PROCESS, NOT PRODUCT:
- FAILS TO ASSESS AI BEHAVIOUR DIRECTLY

REACTIVE:
- ISSUES FOUND AFTER DAMAGE IS DONE

DYNAMIC AI REALITY

AI DRIFTS & CHANGES DAILY:
- NEED FOR IN-HOUSE SOLUTIONS FOR DYNAMIC AI REQUIRMENTS

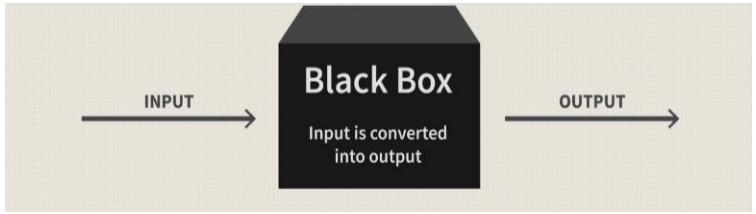
PRODUCT-LEVEL COMPLIANCE:
- REQUIRES REAL-TIME, GRANULAR VALIDATION

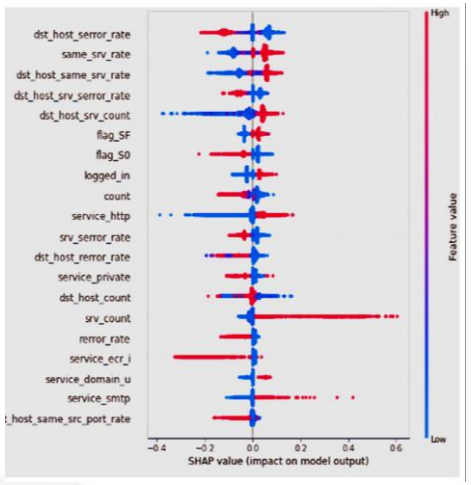
PROACTIVE:
- MUST DETECT VULNERABILITIES BEFORE DEPLOYMENT

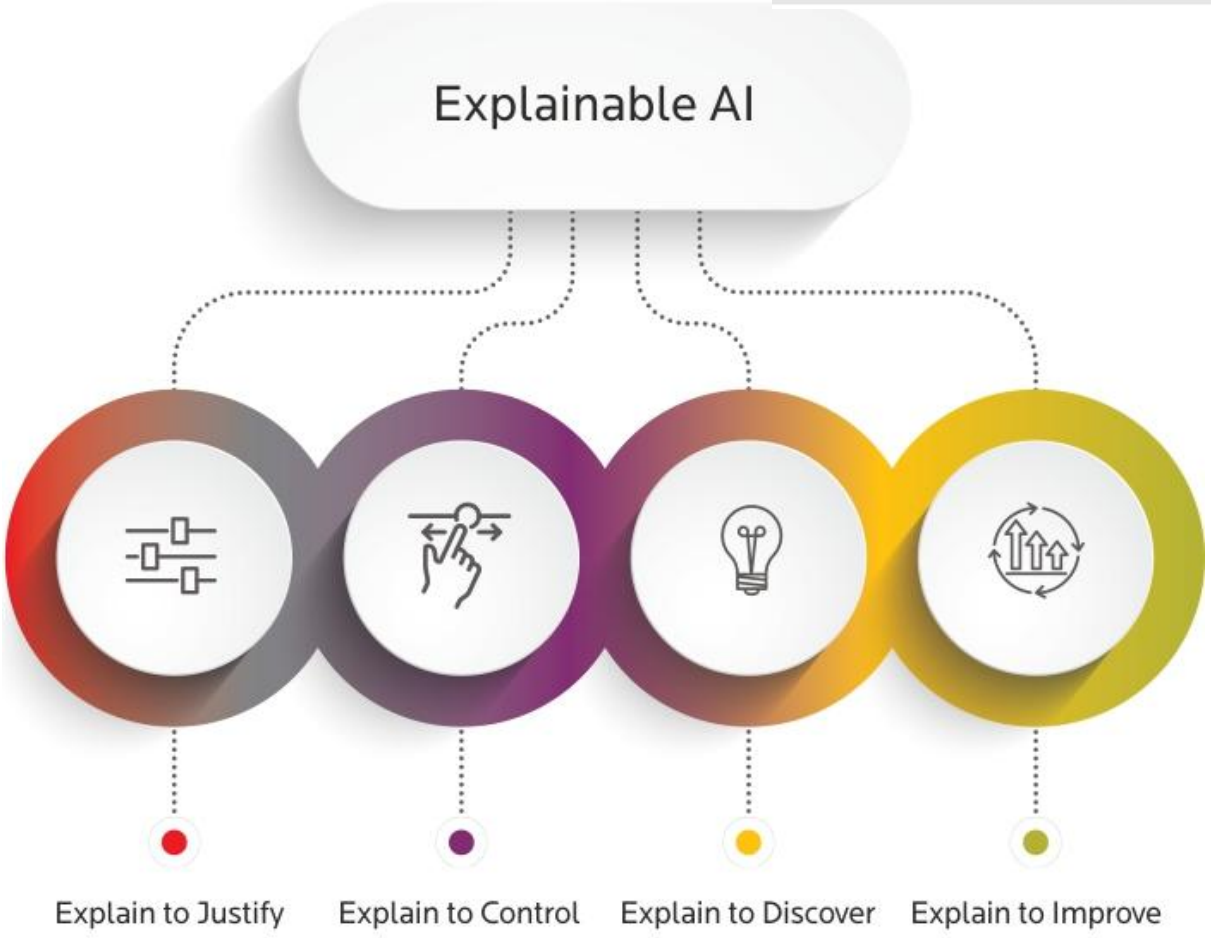
AI Makes Static Compliance **OBSOLETE!**

Static Rules cannot govern dynamic Intelligence!

UCD DUBLIN | NetsLab | Genshield-AI







Explainable AI: Transparency for machine reasoning

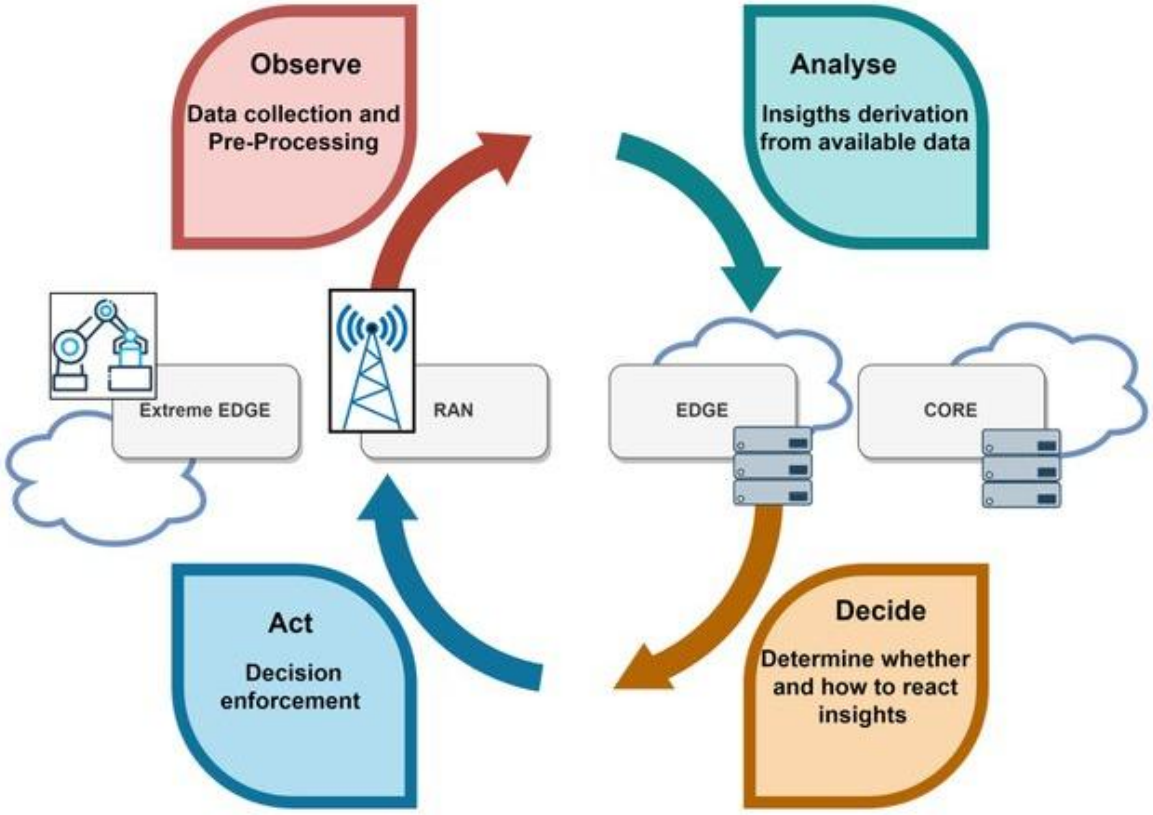
- Role of XAI in 6G security
  - Improving the accountability and explainability of AI-based security Systems
  - Helps to real-time fine-tune models to improve detection accuracy and reduce false positives.
  - Improve the attack detection and mitigation
    - E.g Zero-day attack detection and Poisoning attack detection
  - Improve accuracy and reduce the cost
    - Reduce the number of features for fast training and inference

"If we cannot explain what our AI decides, we cannot trust what our AI defends."

SPATIAL UCD DUBLIN | NetsLab

Automated Security in 6G:
Zero-Touch, Zero-Trust Architecture

- Zero Touch Security automates threat detection and response in 6G networks using AI, reducing human error and ensuring rapid, scalable protection.
- **AI-driven predictive cybersecurity algorithms**
- **AI/ML-driven security orchestration**
- Zero-Trust: “never trust, always verify.”
- **Enable Zero Trust Architecture for 6G:** Continuous verification of all connections.



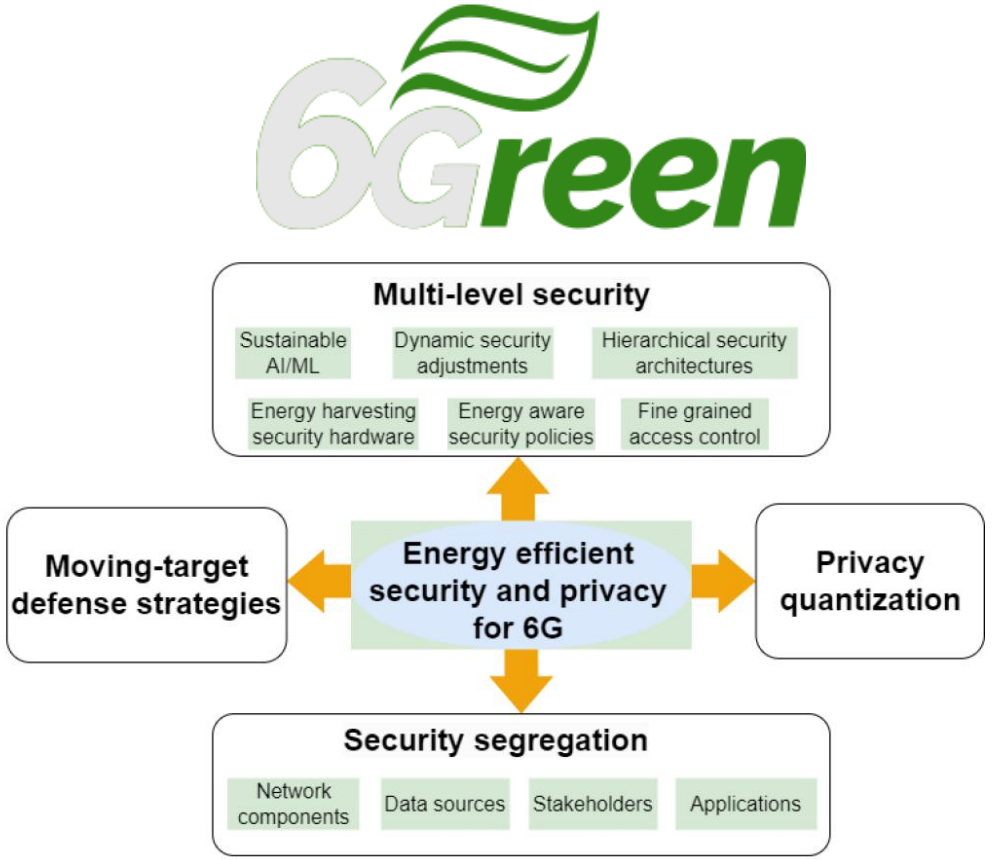
“In 6G, trust is continuous—not a one-time certificate. And Only automation can secure continuous trust in a billion-device 6G world.”

ROBUST-6G

UCD DUBLIN | NetsLab

Energy-Efficient and Responsible Security

- **Why It Matters in 6G**
  - 6G connects billions of devices — security must stay energy-smart.
  - Traditional methods drain power and don't scale to edge systems.
  - Sustainable security aligns trust with energy efficiency.
- **How to Achieve It**
  - **Energy-aware cryptography:** Minimize computation and transmission.
  - **Adaptive security:** Adjust protection by context and energy.
  - **Efficient privacy:** Lightweight noise in Differential Privacy, low-cost FL models.
  - **Edge–cloud collaboration:** Multi-level security by offloading heavy tasks to green data centers.



"In 6G, security that wastes energy is itself a threat."

ROBUST-6G

UCD DUBLIN | NetsLab

Quantum-Resilient 6G

- Securing 6G communications should be targeting on integrating Quantum key distribution and post-quantum cryptography for long-term network security, including challenges that could arise in a post-quantum era.

"6G must be ready for a world where quantum power can break today's trust."

ENSURE-6G

UCD DUBLIN | NetsLab

Hexa-X-II 6G E2E system blueprint

Security is a Pervasive Function in 6G

Application enablement platform & Application layers:

- a unified platform for developers and third-party applications to leverage 6G capabilities.

Network functions layer

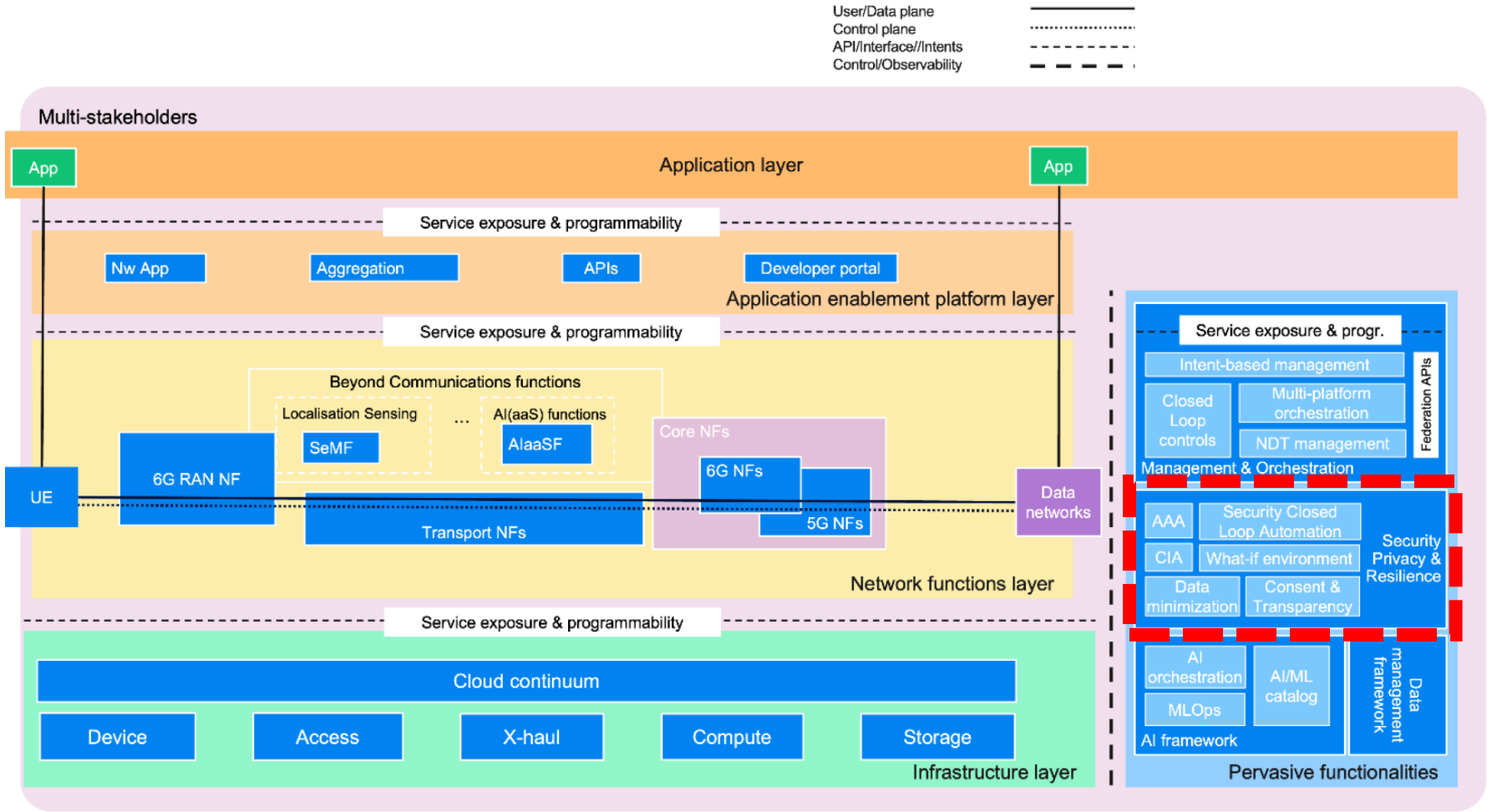
- a single radio access technology, an extended core, and beyond communications capabilities

Infrastructure layer

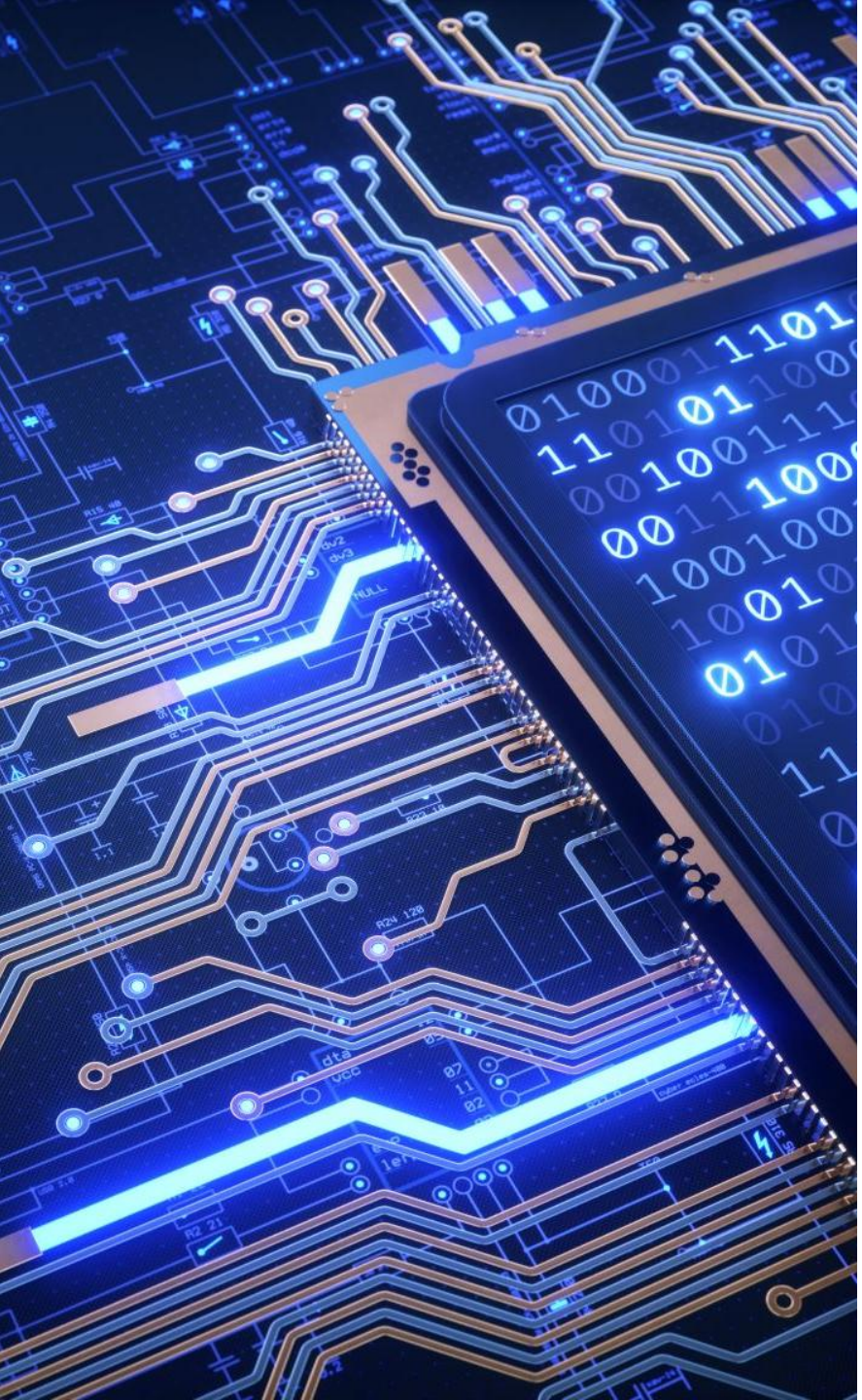
- delivering a cloud continuum

Pervasive functionalities

- enabling AI/ML, data, security, and automation across all layers



Courtesy to Dr. Pawani Porambage, VTT, Finland



Conclusion

- 6G will redefine connectivity.
- Trust is not optional—it is the blueprint for its survival.
  - Four foundational pillars: Secure Intelligence, Explainable & Responsible AI, Zero-Touch & Zero-Trust Security, Sustainable & Quantum-Safe Networks

"Trust isn't a layer in 6G—it's the core that enables reinvention."

UCD DUBLIN | NetsLab

Network Softwarization and Security Laboratory (NetsLab)

NetsLab
Securing the future of connectivity

UCD DUBLIN

https://netslab.ucd.ie/

NETSLAB is a research group at the UCD School of Computer Science that mainly focuses on **the security and privacy of future mobile networks, including 5G and 6G**.

- Director: **Dr. Madhusanka Liyanage**
- Over **30 members** including 2 Senior Researchers, 6 Post-docs, 16 PhD Students, 3 RAs
- Published over 300 publications in **5G/6G Security and Blockchian Topics**
- Contribute to **ESTI, 6G-IA, ITU, ENISA, IEEE** etc

AI Security and Privacy

Implementing Blockchain in 5G/6G Networks

Network Softwarization and Security Automation

6GSNS

fidal field trials beyond 5G

SAND BOX

C6G

ROBUST-6G

6G BRICKS

SPATIAL

ENSURE-6G

dAIEDGE

GenShield AI

6G FLAGSHIP UNIVERSITY OF OULU

5G CURE

CONNECT SFI Research Centre for Future Networks

ML Labs

Follow us
in Linkedin:

NetsLab

Thank you!!

Contact email: madhusanka@ucd.ie
Web: https://netslab.ucd.ie/