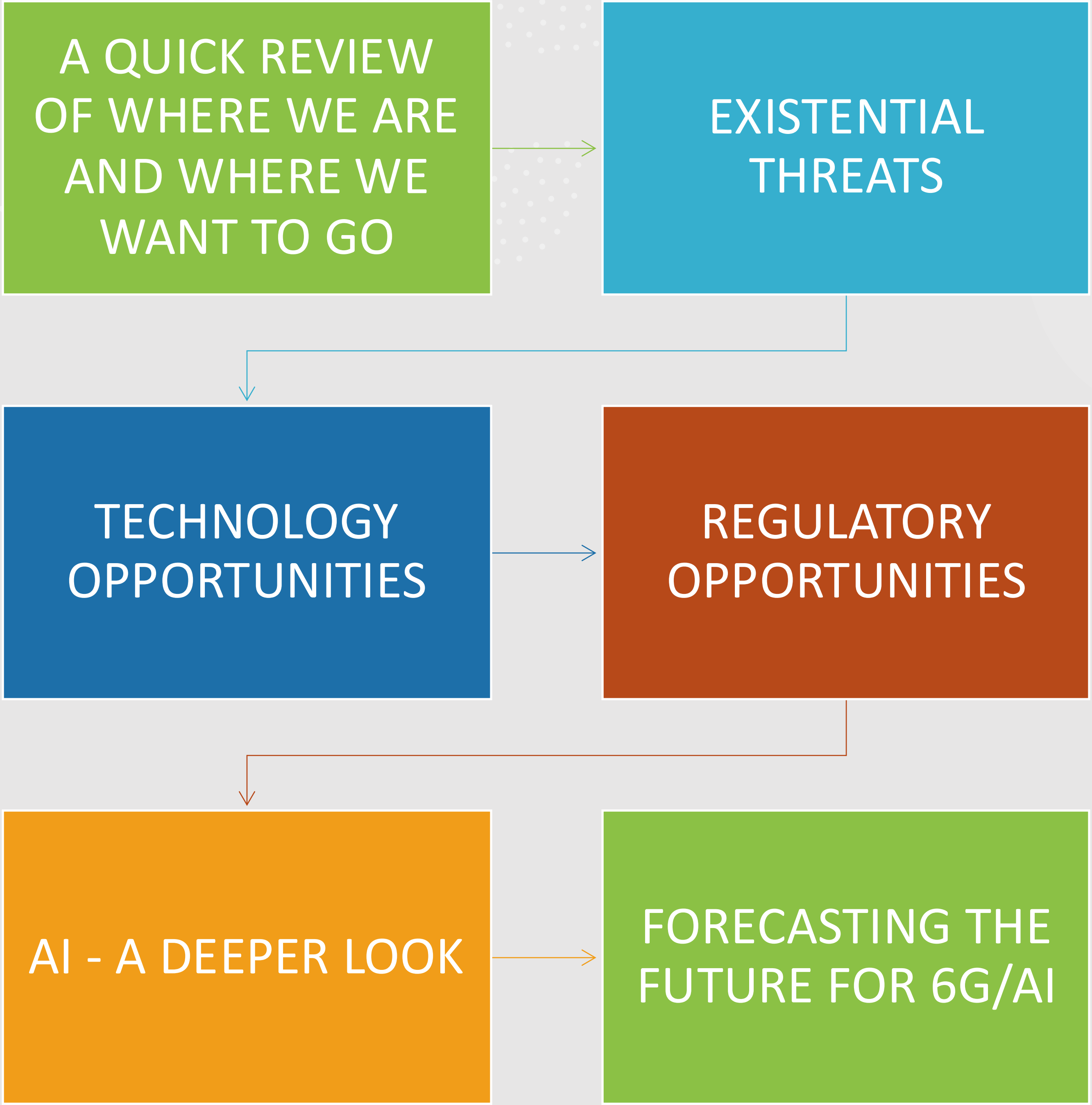
6G and Security and AI

How does AI influence 6G

About me …

- Scott CADZOW
  - Scottish, lives in England, has lived in The Netherlands and for about 25 years has spent 75% of his time in France
  - Engineer by education, instinct and profession
  - Somewhat varied work history: Advanced radio, software defined radio, III-V materials development for mechanically active devices, database design and access, radio standards and security standards in public safety, Intelligent Transport, Health, Networks, methods for risk analysis and security frameworks
  - Standards leadership: has written about 100 standards in ETSI, has chaired or been vice chair in TETRA, LI, ITS, eHealth, SAI, ETI and rapporteur in many others including ESI, CYBER, CDM …

Outline of content – an agenda of sorts



A QUICK REVIEW OF WHERE WE ARE AND WHERE WE WANT TO GO

EXISTENTIAL THREATS

TECHNOLOGY OPPORTUNITIES

REGULATORY OPPORTUNITIES

AI - A DEEPER LOOK

FORECASTING THE FUTURE FOR 6G/AI

Why the background?

- Silly question - history informs our outlook on the future
- We should not second guess what people want but we need to be aware of why things have succeeded or failed.

A quick review …

Where we are

We've achieved recognition that security is good and essential and that it's difficult

Cryptography is now mainstream and expected

Why we are in a bit of a rut

We're still stuck with security being considered as a synonym of safety

We're still stuck with security being confused with privacy

Where we want to go

Effective deployment of security technology to manage risk to reasonable levels

Some review points

2G security through 3G, 4G and 5G

- Strong and state of the art
- Evolving with added functionality over time:
  - Authentication of the phone, added authentication of the network, added longer keys for authentication (including a CMAC for the mutual element) and encryption, added in keying for higher layer functions, merging WiFi and cellular security models, moving from circuits to sessions

IoT and ICT towards an Internet of Everything

- Rooted in IP but extending way beyond

Better understanding of ephemeral keying

- Not just TLS1.3 but building out from session keys in 2G

A bit more review

We're pushing security at the heart of most standards work

In AI

In IoT

In smart cities

In Intelligent Transport

We are recognising privacy assurances aren't the same as security assurances

Assurance schemes are evolving to be suited for all device types and services

A last review point

- We’ve achieved convergence (in the standards domain)
- Speed is available most of the time
- Digital citizens and digital society exist
- Smart cars, smart cities, smart homes exist

Existential threats

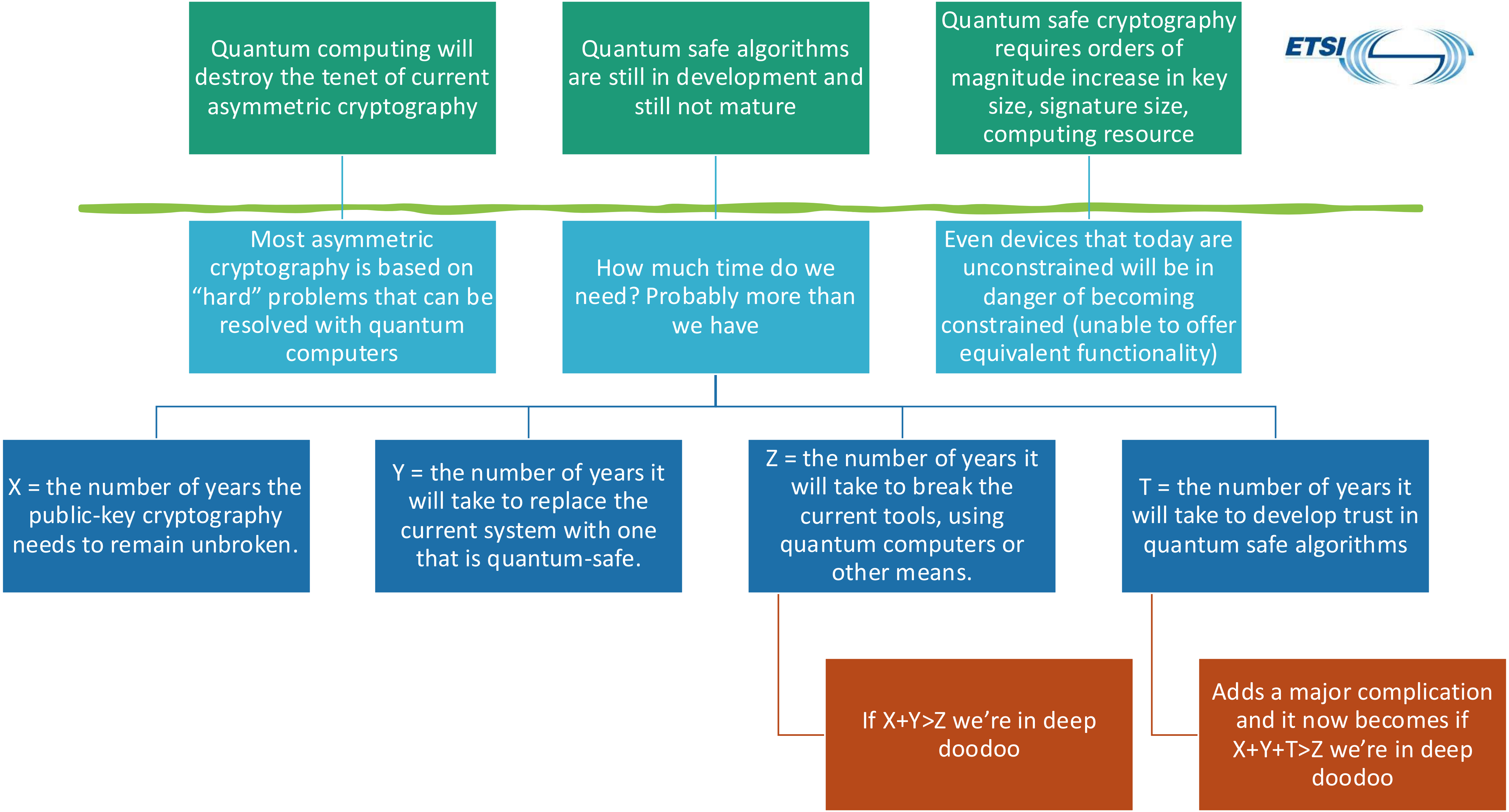
(things we need to worry about (a lot))

- Quantum
- Pervasive encryption
- Bad guys
- Good guys with good intent but no knowledge
- Crypto
- Energy costs
- AI and its cousin ML

Existential threats

(things we need to worry about (a lot))

- **Quantum**
- ~~Pervasive encryption~~
- ~~Bad guys~~
- ~~Good guys with good intent but no knowledge~~
- ~~Crypto~~
- ~~Energy costs~~
- ~~AI and its cousin ML~~



Quantum computing will destroy the tenet of current asymmetric cryptography

Quantum safe algorithms are still in development and still not mature

Quantum safe cryptography requires orders of magnitude increase in key size, signature size, computing resource

Most asymmetric cryptography is based on “hard” problems that can be resolved with quantum computers

How much time do we need? Probably more than we have

Even devices that today are unconstrained will be in danger of becoming constrained (unable to offer equivalent functionality)

X = the number of years the public-key cryptography needs to remain unbroken.

Y = the number of years it will take to replace the current system with one that is quantum-safe.

Z = the number of years it will take to break the current tools, using quantum computers or other means.

T = the number of years it will take to develop trust in quantum safe algorithms

If $X+Y>Z$ we’re in deep doodoo

Adds a major complication and it now becomes if $X+Y+T>Z$ we’re in deep doodoo

Countering the quantum threat

Quantum Safe Cryptography

Led by NIST and ETSI's CYBER-QSC groups

Identifying new algorithms and models for signature and encryption

Post quantum cellular

Work in 3GPP SA3 and ETSI SAGE

There is a way to overcome the threat – it will just take time

Quantum crypto approaches

- Quantum Safe Cryptography
  - Attempting to defeat the impact of specific quantum computing models against “classical” cryptography
  - Rethinking the model of Ellis and others to achieve security without secrecy (asymmetric cryptographic model)
  - Lattice frameworks, learning with errors and such
- Quantum mechanical application
  - Exploiting knowledge of quantum effects (superposition, teleportation and so on)
  - Seen in Quantum Key Distribution as a method for exchanging a key across a public network immune to attack

ETSI’s CYBER-QSC scope

- Quantum safe cryptography
  - Refining the work done in the NIST quantum algorithm not a competition process to select/design algorithms
  - Lattices, Learning with Errors, … lots of number theory and maths
- Addresses several application areas of cryptography
  - Signature
  - Key encapsulation
  - Encryption
- Migration and mitigation
  - Developing guides that address the migration problem driving other groups including smart-elements (TC SEC), transport (TC ITS), health (TC eHEALTH), frameworks (TC ESI)

Existential threats

(things we need to worry about (a lot))

- ~~Quantum~~
- **Pervasive encryption**
- ~~Bad guys~~
- ~~Good guys with good intent but no knowledge~~
- ~~Crypto~~
- ~~Energy costs~~
- ~~AI and its cousin ML~~

Pervasive encryption

Encryption is good, as is cryptography. The role of encryption of information being transported between two end-points has three widely recognized positive purposes depending on the context:

- confidentiality protection of the transferred content;
- enhanced trust in the identity of the parties associated with the information; and
- enhanced trust in the integrity of the information during transport.

End-to-end encryption = good, is a marketing mantra that isn't all it seems, if it means everything is encrypted

- It removes pre-emptive filtering of malicious content
- It means networks are just pipes with no added value – can routing work if everything is encrypted with keys known only to the end points?
- Regulatory bypass (no oversight, operators are like rabbits caught in the headlights)

Countering threats of pervasive encryption

- Adoption of Zero Trust Architectures
    - Moves from Implicit to Explicit trust
- Require explicability and transparency of where encryption is used
    - Don’t assume – prove
- Work being addressed at ETSI ISG ETI

Zero trust - what it means and why it’s important

It doesn’t mean we can’t trust things

It means we can’t assume trust, we need to prove trust

Why? Trust is contextual, trust is mutable, trust is not-transferable

Existential threats

(things we need to worry about (a lot))

- ~~Quantum~~
- ~~Pervasive encryption~~
- **Bad guys**
- **Good guys with good intent but no knowledge**
- ~~Crypto~~
- ~~Energy costs~~
- ~~AI and its cousin ML~~

Bad guys, good guys

Bad guys will spend €s to make cents – it's a profit thing

The risk of penalty is built into their profit motive

Good guys don't have profits to justify their existence, they're always a cost item (an expense)

If you've not suffered from attack is it because your defence is good or you're not a target (yet)? How much should I spend on defence?

Good guys sometimes make bad decisions:

Encryption enables criminal activity to be hidden → let's ban encryption

Functionality comes first so let's get the code working and then secure it later

That webcam in the child's toy could be used to spy on me. Nobody would do that surely? It's just a toy

Making good guys better …

- Education, education, education …
- Specialists and generalists working together
  - Teams not individuals
  - Board level responsibility - it should not be the IT guys' fault
- Thinking "outside the box"
  - Side channel attacks
  - Understanding the motivation of the attacker
  - Thinking bad and acting good
  - Using intelligence intelligently

Understanding risk

- Risk is the product of impact and likelihood of an attack
- Risk is what is mitigated in one of two ways:
  - Redesign
  - Masking
- Redesign is hard and from a security perspective achieves two things - reducing the impact (really hard) and reducing the likelihood of an attack
- Masking only makes likelihood smaller - it makes no attempt to reduce the impact

Risk management is a process

Risk assessment is too often never done or only ever done at the start of a project ---- WRONG!!!!

Attacks and attackers learn daily so the risk of an attack changes daily hence the risk assessment has to be continuous

Building risk and threat awareness into normal business practice

It’s normal practice for supply chains, for pricing, to be competitive, it has to be for cybersecurity

Share knowledge and best practice with your competitors

If your competitors are attacked you’ll be next - share knowledge

Standards bodies share knowledge, expertise, experience and develop best practice - use them as core to the business

Existential threats

(things we need to worry about (a lot))

- ~~Quantum~~
- ~~Pervasive encryption~~
- ~~Bad guys~~
- ~~Good guys with good intent but no knowledge~~
- **Crypto**
- ~~Energy costs~~
- ~~AI and its cousin ML~~

Crypto

- As in currency
  - ”I work in crypto” could give the impression to a layperson that you’re in banking or finance
- It’s not a security in the ICT sense but may be a financial security
- Crypto (currency) may divert expertise from everyday ICT security
- Crypto (currency) could be killed off by quantum threats
  - Where does my money go?
  - If there’s no central authority to endorse money does it exist?

The lure of blockchain …

Cynical view: A solution in search of its problem

- Not everything is a ledger or can be “ledgerised”
- Other security models achieve similar results with less overhead

Trust model view: Trust nobody by trusting in the collective - democracy in action

Security model view: It’s got everything - immunity to change, cryptographically timestamped, reasonable confidentiality, distributed and open, signed and sealed, extensible, crypto-agility built-in

Away from digital currency though …

Smart contracts

Codifying business then distributing agreement that contracts have been fulfilled

Supply chains

Software bills of material

Patch management

…

Cynical view? Not everything in life can be codified and automated, sometimes rules are guidelines (slap bass? Test dept (the band)?)

Existential threats

(things we need to worry about (a lot))

- ~~Quantum~~
- ~~Pervasive encryption~~
- ~~Bad guys~~
- ~~Good guys with good intent but no knowledge~~
- ~~Crypto~~
- **Energy costs**
- ~~AI and its cousin ML~~

Energy costs

Cryptography consumes a lot of processing cycles

The longer the key, the more rounds, the more power that is needed

Same with memory

Needed to store keys, to process the crypto functions

Same with communications resource

Sending keys, overhead of signature

Today's crypto when used in new processes often becomes energy intense (in a bad way)

Bitcoin consensus protocols are notoriously energy inefficient

Existential threats

(things we need to worry about (a lot))

- ~~Quantum~~
- ~~Pervasive encryption~~
- ~~Bad guys~~
- ~~Good guys with good intent but no knowledge~~
- ~~Crypto~~
- ~~Energy costs~~
- **AI and its cousin ML**

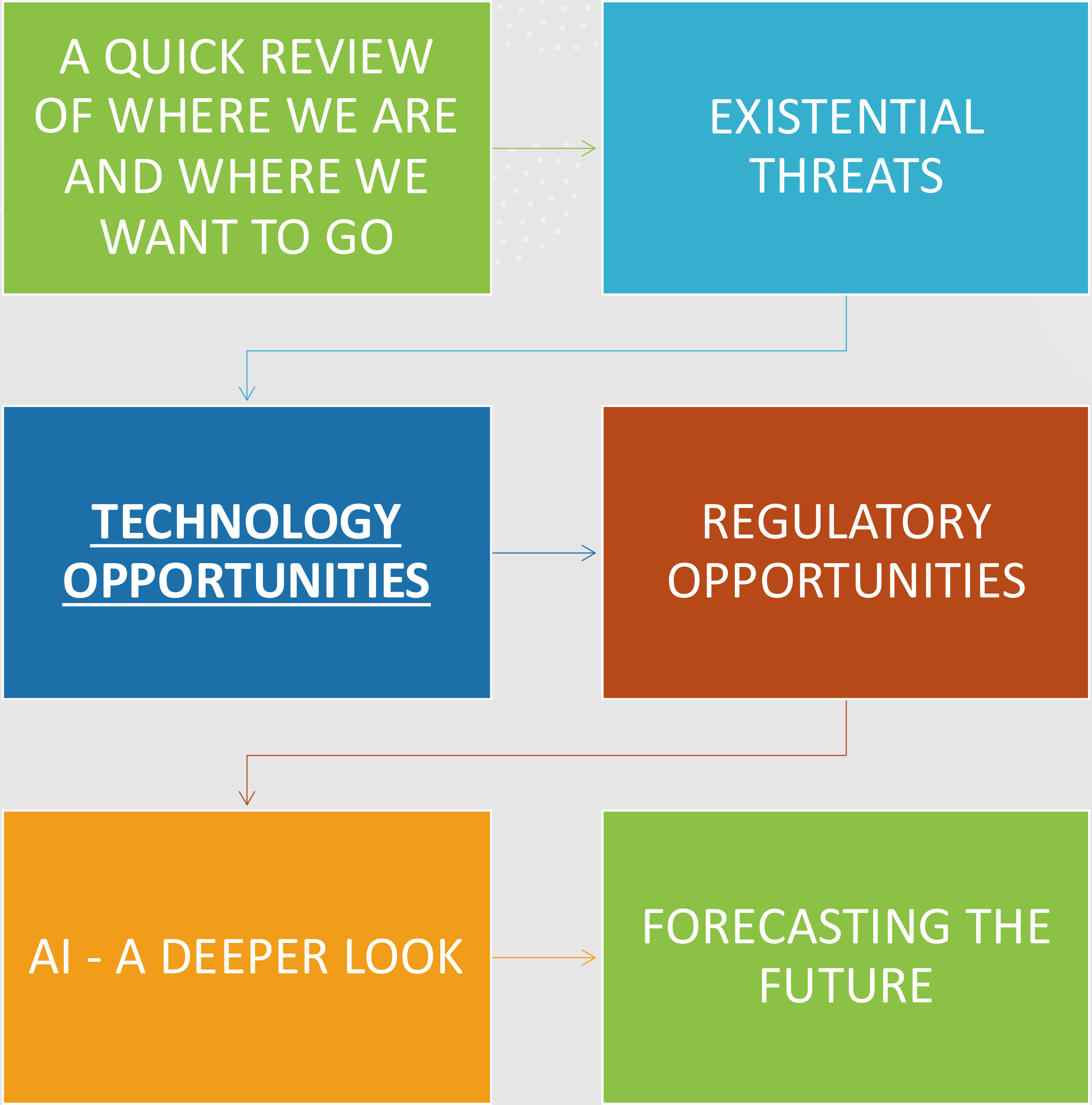
Artificial Intelligence

- In general terms more intelligence applied to a “hard” problem, and more intelligence power, cracks the problem or prevents the problem ever arising
- AI, and Machine Learning, offer a couple of things to worry base ICT security:
  - Lots of effort to uncover weaknesses in core crypto-systems compressed in time by algorithms finding weak correlations and multiplying them to be causations
  - Patterns unknown as weaknesses discovered by all out machine driven attack – botnets on steroids
- AI at the application level may be even worse – deep fakes destroy trust
  - Uncertainty breeds doubt and doubt destroys trust

AI in more detail later …

- As an existential threat AI impacts humanity in lots of ways in much the same way that the industrial revolution did
  - Jobs **will** change
  - Economic balances **will** shift
  - Nation states **will** lose or gain power
- The argument that ”it’s just software” is misguided and misleading

Outline of content – an agenda of sorts



A QUICK REVIEW OF WHERE WE ARE AND WHERE WE WANT TO GO

EXISTENTIAL THREATS

TECHNOLOGY OPPORTUNITIES

REGULATORY OPPORTUNITIES

AI - A DEEPER LOOK

FORECASTING THE FUTURE

Opportunities do exist

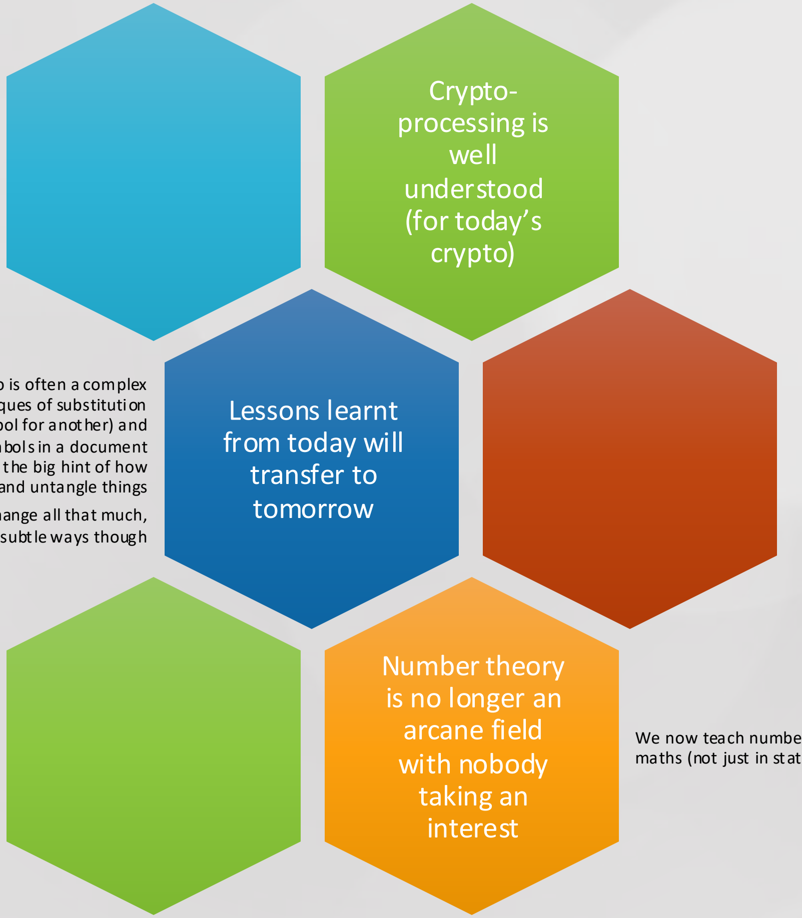
Technological

- More processing power, more bandwidth, more maths

Regulation

- Understanding the need for ICT security in society
  - Waking up to the 21st century being an ICT connected society
  - Recognising the threat to nation state security of ICT threats to institutions, industry, individuals (the 3i’s)
- Mandating for security breaches to be treated criminally (breaches can mean jail time)

Technology is on our side



Crypto-processing is well understood (for today's crypto)

Lessons learnt from today will transfer to tomorrow

Number theory is no longer an arcane field with nobody taking an interest

Modern symmetric crypto is often a complex mix of centuries old techniques of substitution (changing one symbol for another) and transposition (moving symbols in a document around) with a key giving the big hint of how to tangle and untangle things

These roots will not change all that much, they will be extended in subtle ways though

We now teach number theory and algorithms in maths (not just in statistics classes)

Technology, a good companion

- Good guys can use it to thwart the bad guys
  - Harness the power of AI/ML to identify attacks and attackers before they become an issue
  - Use Quantum to give an edge – alongside new processor designs use quantum mechanics to work on new algorithms, use QKD as an extension to more conventional key management schemes, explore the role of superposition and teleportation and entanglement in enabling security
  - Holographic processing (not holostate but multi-path processing in crystalline structures), multi-state processing, neural nets, all have a role to play

Risk management technologies?

- Risk is what we’re trying to manage
- Risk assessment needs clear understanding of what we have (components) and how they fit together (interfaces)
- Modern systems are challenging for risk analysis as the components and their interfaces are auto-mutating, auto-evolving
  - We need to improve our ability to track risk in live systems
  - We can harness AI/ML to help us here

Regulation is going to help us

Security of users is at the core of many new regulatory initiatives:

The Cybersecurity Act in the EU

The Privacy directives and data protection directives

The Radio Equipment Directive

The proposed AI Act

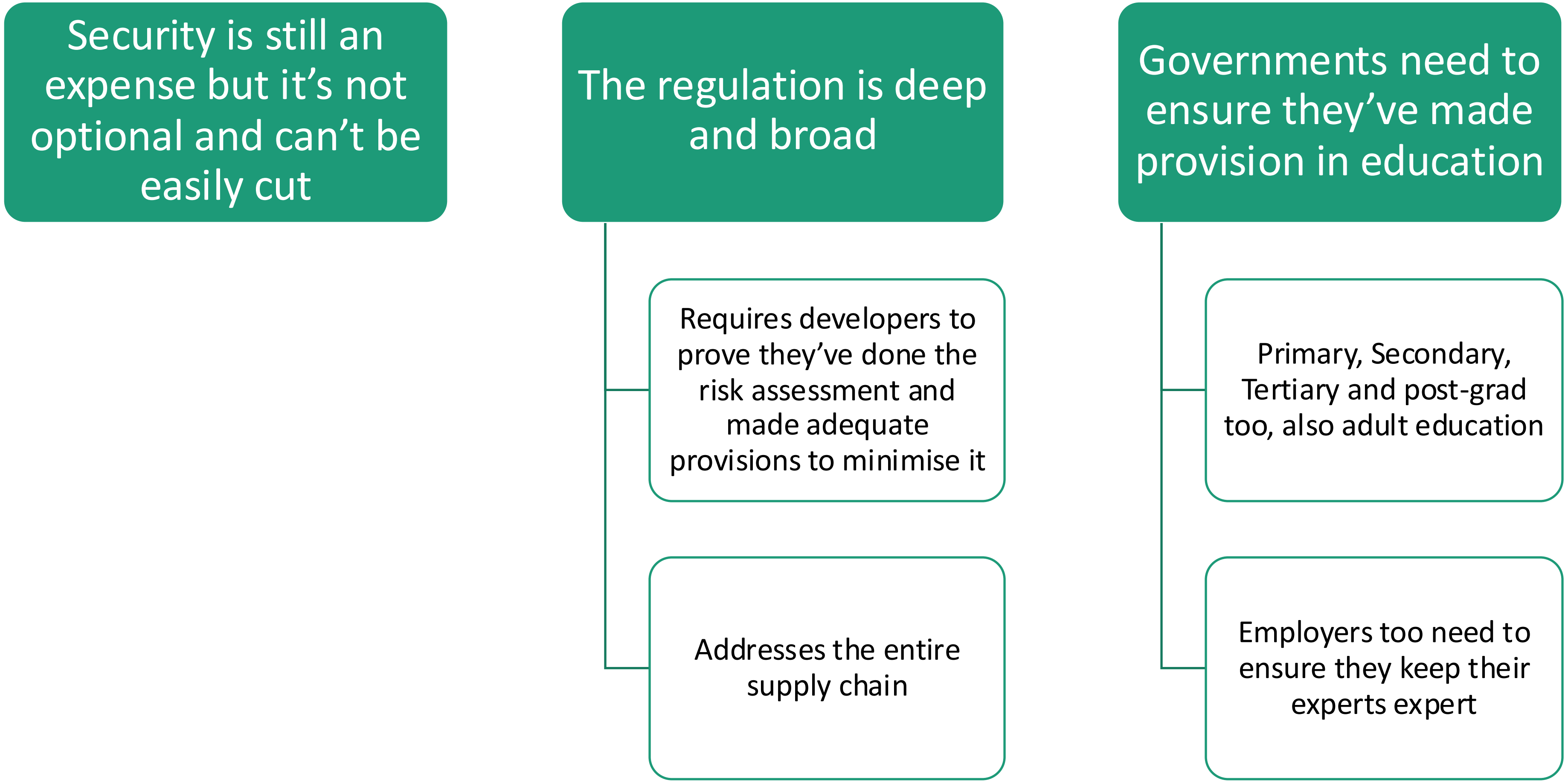
All of the above (and many others) make it clear that poor security which leads to harm is unacceptable

Security provisions, commensurate to the risk, are mandated by law

Penalties for failure are significant (The UK GDPR and DPA 2018 set a **maximum fine of £17.5 million or 4% of annual global turnover – whichever is greater** – for infringements. Th EU GDPR sets a maximum fine of €20 million (about £18 million) or 4% of annual global turnover – whichever is greater – for infringements)

Similar levels of penalty are expected from the other acts

Regulation helps but how?



Security is still an expense but it's not optional and can't be easily cut

The regulation is deep and broad

- Requires developers to prove they've done the risk assessment and made adequate provisions to minimise it
- Addresses the entire supply chain

Governments need to ensure they've made provision in education

- Primary, Secondary, Tertiary and post-grad too, also adult education
- Employers too need to ensure they keep their experts expert

Regulation and technology work together

- Trust is not just personal but it's still couched in society as if it were
  - Trusted institutions – government, school, church?
    - Why do we trust institutions? Are we simply educated to trust them?
  - Trusted roles – doctors, lawyers, accountants, engineers?
    - Do we trust them because of the steps they go through to become qualified?
  - Trusted technology – Operating systems, applications, hardware, comms
- New trust frameworks for ICT driven societies?
  - ICT led change has moved faster than many of our key institutions and roles
- We need to get to a point where trust is explicit, explicable and transparent in our ICT worlds

Time for a break - more AI later

Scott CADZOW, scott at cadzow dot com, somewhere in England

Existential threats

(things we need to worry about (a lot))

- ~~Quantum~~
- ~~Pervasive encryption~~
- ~~Bad guys~~
- ~~Good guys with good intent but no knowledge~~
- ~~Crypto~~
- ~~Energy costs~~
- **AI and its cousin ML**

Artificial Intelligence and Machine Learning

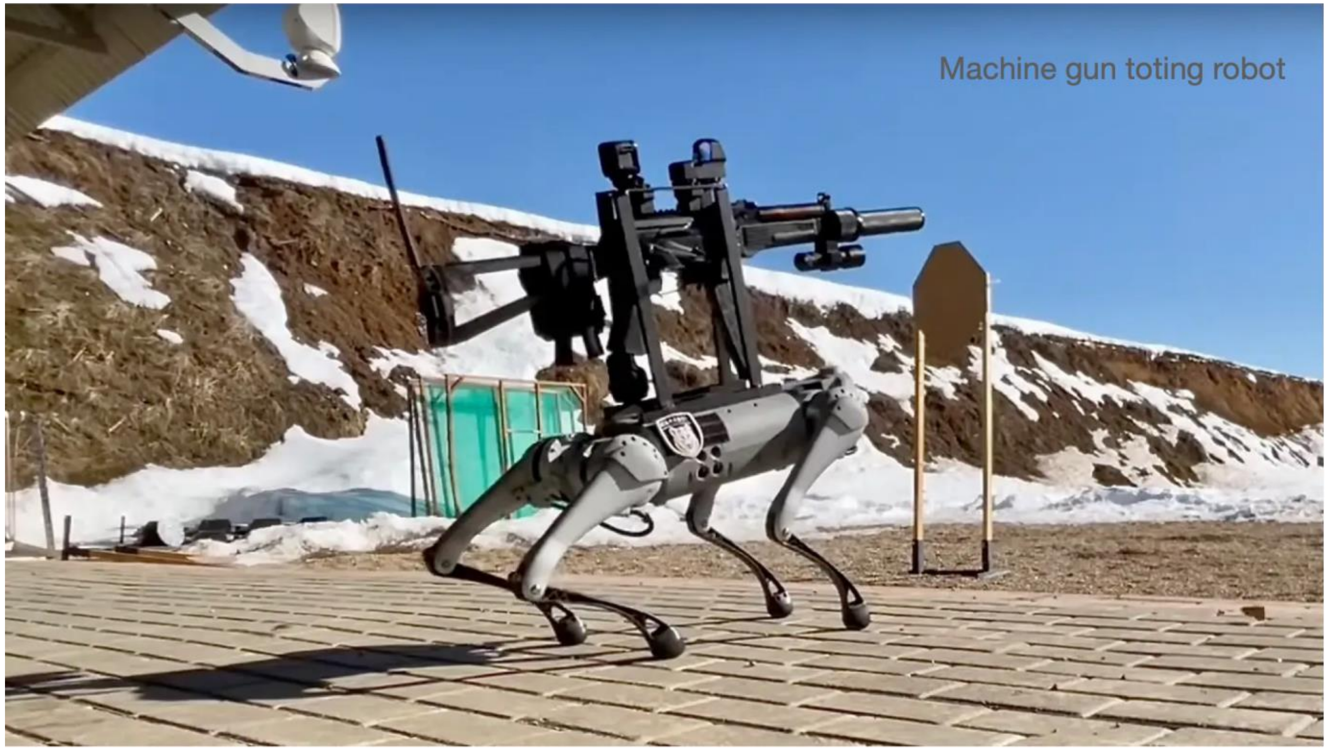
- What the OECD says:
  - An AI system is a machine-based system that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environment
- What Arthur C Clarke said:
  - Any sufficiently advanced technology is indistinguishable from magic
- What ETSI says:
  - [the] ability of a system to handle representations, both explicit and implicit, and procedures to perform tasks that would be considered intelligent if performed by a human

The public worry about AI

- Dystopian visions of a future world run by robots
  - Terminator to the extreme
  - Politics by machine to become a machine driven autocracy
  - Taught by robots and suppression of emotion as illogical
  - Rogue machines killing our children

Bad loser chess robot

Robot car used steel rod to change lane?



Machine gun toting robot

Robot surgery?

Why AI standards are necessary

- AI is a complex software and rationalising complexity is always good
- Standards often open up complex systems into interoperable subsystems with standardised (and open) interfaces between them
- Standards though don’t really touch on content but do touch on process
- AI is an “existential threat” and if standards can make its application both more transparent and more explicable it defuses the threat and allows us to manage the risk

AI - intelligent or smart?

- AI is just software, acting on big data, to achieve a result
  - It is not really “intelligent”
  - Some applications of AI can pass the Turing test
- Most AI is at the component level
  - Micro decisions at a local level
  - Semi-autonomous but co-operative in the wider system,

TC SAI – from our terms of reference

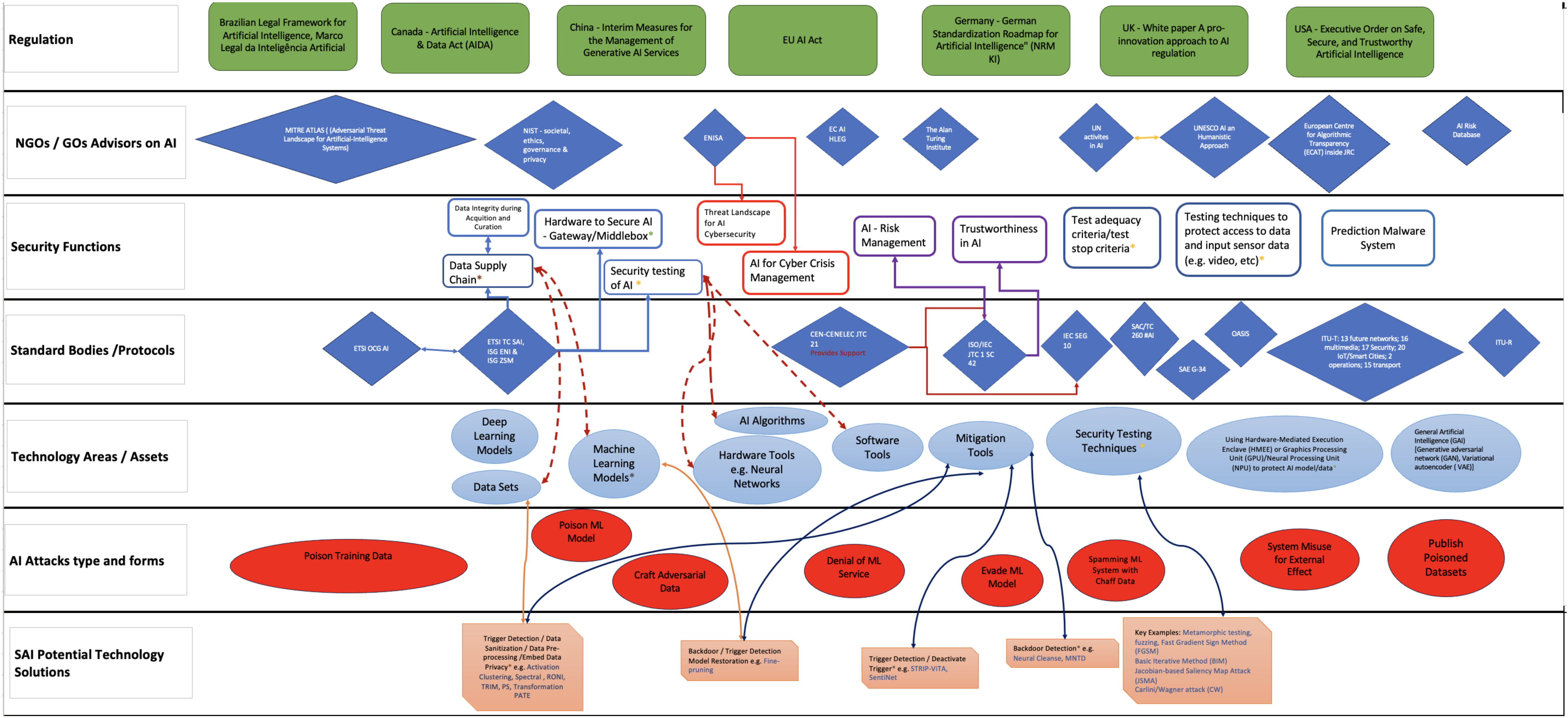
- Terms of Reference
- The aim of Technical Committee Securing Artificial Intelligence (TC SAI) is to develop technical specifications that mitigate against threats arising from the deployment of AI, and threats to AI systems, from both other AIs, and from conventional sources. Whilst in the short to medium term the focus of TC SAI will be on the application of Machine Learning (ML) the group shall also give guidance and evaluation reports to ETSI and its stakeholders on the wider developments of AI
- AI is becoming an increasing element of the ICT world thus it is essential that it is made secure, safe and societally responsible.
    - The word "securing" in the name of TC SAI is intended to address all of those aspects: AI has to be secure but it cannot only be secure - it has to be safe, it has to be societal, it has to be suitable. Thus the “S” in SAI is expanded to have all of these meanings.

Not ethics -- see supplementary slides

TC SAI – Our place in the EU

- TC SAI has the opportunity to lead on the standards that fit to Europe and wider afield and will take it
  - Article 8 of the proposed final draft of the Cyber Resilience Act (CRA) addresses High Risk AI as a digital element
    - There is a proposal for an AI Act to regulate the use of AI to be safe and secure, and socially accountable in addition to considerations of AI as a digital element in the CRA
  - There are multiple initiatives by EU and partner governments to regulate or guide the use of AI and all of them will require standards to guide the market's best practice

TC SAI - a view on our world



Regulation

Brazilian Legal Framework for Artificial Intelligence, Marco Legal da Inteligência Artificial

Canada - Artificial Intelligence & Data Act (AIDA)

China - Interim Measures for the Management of Generative AI Services

EU AI Act

Germany - German Standardization Roadmap for Artificial Intelligence" (NRM KI)

UK - White paper A pro-innovation approach to AI regulation

USA - Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence

NGOs / GOs Advisors on AI

MITRE ATLAS ((Adversarial Threat Landscape for Artificial-Intelligence Systems)

NIST - societal, ethics, governance & privacy

ENISA

EC AI HLEG

The Alan Turing Institute

UN activites in AI

UNESCO AI an Humanistic Approach

European Centre for Algorithmic Transparency (ECAT) inside JRC

AI Risk Database

Security Functions

Data Integrity during Acquition and Curation

Hardware to Secure AI - Gateway/Middlebox*

Threat Landscape for AI Cybersecurity

Data Supply Chain*

Security testing of AI *

AI for Cyber Crisis Management

AI - Risk Management

Trustworthiness in AI

Test adequacy criteria/test stop criteria*

Testing techniques to protect access to data and input sensor data (e.g. video, etc)*

Prediction Malware System

Standard Bodies /Protocols

ETSI OCG AI

ETSI TC SAI, ISG ENI & ISG ZSM

CEN-CENELEC JTC 21 Provides Support

ISO/IEC JTC 1 SC 42

IEC SEG 10

SAC/TC 260 #AI

SAE G-34

OASIS

ITU-T: 13 future networks; 16 multimedia; 17 Security; 20 IoT/Smart Cities; 2 operations; 15 transport

ITU-R

Technology Areas / Assets

Deep Learning Models

Data Sets

Machine Learning Models*

AI Algorithms

Hardware Tools e.g. Neural Networks

Software Tools

Mitigation Tools

Security Testing Techniques *

Using Hardware-Mediated Execution Enclave (HMEE) or Graphics Processing Unit (GPU)/Neural Processing Unit (NPU) to protect AI model/data*

General Artificial Intelligence (GAI) [Generative adversarial network (GAN), Variational autoencoder (VAE)]

AI Attacks type and forms

Poison Training Data

Poison ML Model

Craft Adversarial Data

Denial of ML Service

Evade ML Model

Spamming ML System with Chaff Data

System Misuse for External Effect

Publish Poisoned Datasets

SAI Potential Technology Solutions

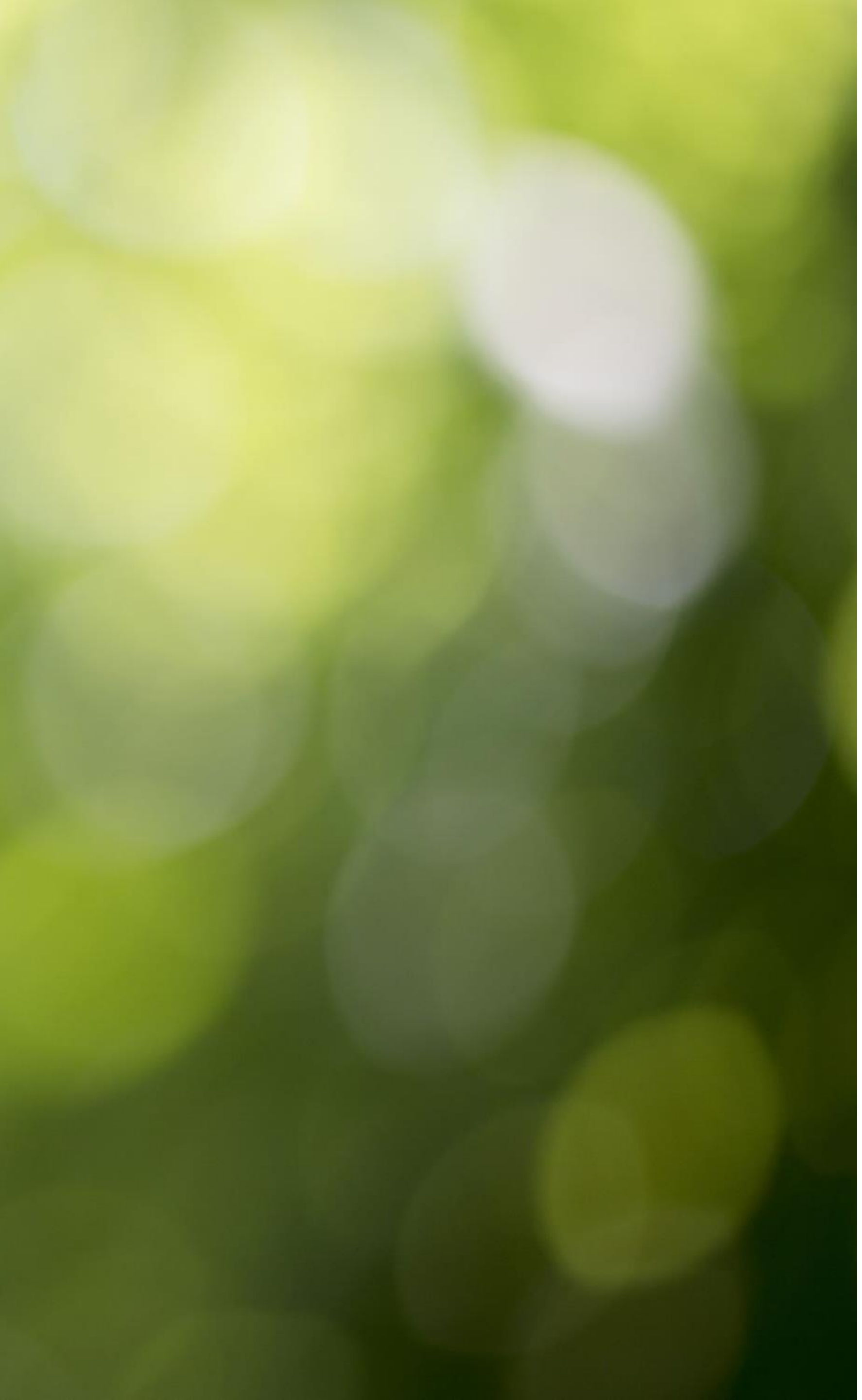
Trigger Detection / Data Sanitization / Data Pre-processing /Embed Data Privacy* e.g. Activation Clustering, Spectral , RONI, TRIM, PS, Transformation PATE

Backdoor / Trigger Detection Model Restoration e.g. Fine-pruning

Trigger Detection / Deactivate Trigger* e.g. STRIP-ViTA, SentiNet

Backdoor Detection* e.g. Neural Cleanse, MNTD

Key Examples: Metamorphic testing, fuzzing, Fast Gradient Sign Method (FGSM)
Basic Iterative Method (BIM)
Jacobian-based Saliency Map Attack (JSMA)
Carlini/Wagner attack (CW)



TC SAI – the attack cycle

Attacks & Defences to AI Systems	Discover security vulnerabilities and attacks to AI systems or systems with AI components and develop effective defensive techniques to address the attacks
AI for Attacks	Attackers leverage the ability of AI to auto launch or speed up attacks, typically with serious impacts
AI for Defence	The ability of AI is benignly used to develop better and automatic security technologies to defend against cyberattacks.

Attacks & Mitigations of AI component, aka, AI self-security

Securing AI component from attacks

Mitigate AI component vulnerability

AI -- Takeaways and suggestions

- AI practitioners and users need guidance
- AI is an emerging technology that builds on a long history of computer assistance to industry, to social activity, to business activity, to leisure
- A lot of what AI does is evolutionary
- A lot of what AI can do is revolutionary
- The speed at which AI can become revolutionary is faster than we are really ready for
- A lot of the societal concerns are rooted in fear of the unknown and untested
- SDOs (like ETSI and ITU-T) can bring rationality to the AI debate

Why not ethics?

- The following characteristics (or tests) set out in ETSI’s guide to developing standards should be embedded into the development of any contribution to a standard:
  - **Necessary**: it (a standard) should specify only what is required to meet its objectives, and not impose a particular approach to implementation.
  - **Unambiguous**: it should be impossible to interpret the normative parts of the standard in more than one way.
  - **Complete**: the requirement should contain all the information necessary to understand that requirement, either directly or by reference to other documents. The reader of a standard should not need to make assumptions about the implementation of any requirement.
  - **Precise**: the requirement should be worded clearly and exactly, without unnecessary detail that might confuse the reader.
  - **Well-structured**: the individual elements of the requirement should all be included in an appropriate and easy-to-read manner.
  - **Consistent**: there should be no contradiction between different requirements within the standard, nor with other related standards.
  - **Testable**: there should be clear and obvious means of demonstrating that an implementation complies with the requirement.
- It is unlikely to be able to write a requirement for Ethics, of AI or in general, that satisfies these criteria.

The Lintilla problem in ethics (from Douglas Adam’s HHGTTG)

- While initially creating six clones of Lintilla, the machine used to clone her had a slight break down. The machine got stuck in a loop, and by the time one Lintilla clone had been created, a half clone had been started. Therefore, the machine could not be shut off without committing murder and would thus go on creating Lintillas indefinitely.
- Can you stop the machine without committing murder? Can you stop the indefinite supply of Lintillas without committing murder?
- This problem taxed the minds first of the cloning engineers, then of the clergy, then of the letters page of Siderial Record Straightener, and finally of the cloning machine company's lawyers. The lawyers experimented vainly with various ways of redefining murder, reevaluating it, and in the end even respelling it in the hope that no one would notice. Of course, they did, and in a final attempt to stem the tide of Lintillas, a group of Allitnils have been deployed: anti-clones designed to eliminate the Lintillas in the most humane and legally defensible way possible.
- The ”solution” makes a Lintilla and an Allitnil fall in love and immediately agree to a “marriage” with the fraud that their marriage certificates are actually cloning machine company "Agreements to Cease to Be”.
- Is the solution ethical? Obviously not, probably not, maybe.

Role of standards in innovation

A short summary

Standards can lead innovation

- Standards makers react well (as engineers) to challenges
- Simple statements of policy may have far reaching impact
  - Only digital cell phones allowed to access the 900MHz band spurred the development of GSM and that in turn has led to our always on 5G world
  - All cars have to have passenger restraint systems led to a massive improvement in the structural integrity of cars
  - Taxation based on CO2 emissions, and the various fuel/oil crisis, encouraged ever more efficient engines - tightened further requires building of EVs as the primary fleet

What are standards?

- As defined: “a required or agreed level of quality or attainment”
- The highest reasonable level of technical achievement that gives assurance of
  - Interoperability - opens the market to multiple players and gives assurance that widget-A can operate alongside widget-B
  - Interconnectivity - assurance that widget-A connects to widget-B

Who develops standards?

- The stakeholders
  - Regulators
  - Manufacturers
  - Deployers
  - Integrators
  - Users
  - Society

Forecasting

- Alice’s world

The crystal ball bit …

- Disclaimer: Forecasts are by nature unreliable, only hindsight is reliable (with the right analyst anyway)
- The easy bit:
  - Technology will continue to improve (Moore's law downscaled to different levels of efficiency)
  - Software will become more testable
  - Users will expect secure systems by default
- The hard bit:
  - When things will happen is not an easy prediction

Commercial reality of forecasting

Processor architectures will change and the software they support will change

EXAMPLE: Apple have moved into SoCs for all platforms

… but only Apple know when actual changes will get to market

Software developments, and hardware developments, will be driven by sales pressure

EXAMPLE: a new OS demands new hardware and the market demands new every year

… but this suggests fashion and not novelty

Society will adopt and mould technology – not the developers

EXAMPLE: Facebook and Twitter are quite different as their use became mainstream

… but the destination is never certain when we start

Some remarks #1

A system without security will not be viable to enter the market

Society will demand it, and vendors/developers/providers will have to provide it to survive

Regulators and nation states have to defend their citizens

If ICT is a source of threats then regulators and nation states have to ensure that ICT is secure in order to protect and defend their citizens

… and their sovereign wealth

… and their borders

Some remarks #2

- Standards as drivers for interoperability will remain critical
  - The purpose of standards hasn’t changed – they open markets to more players
  - One player can only serve a limited number of customers, a standard could allow 100s of players to serve the market, and that market could be 1000s of times bigger that a single player could serve.
  - One player can only evolve the market at their pace, 100s of players means there is a race for market share and market evolution

A take-away …

- *“Standardization does not mean that we all wear the same color and weave of cloth, eat standard sandwiches, or live in standard rooms with standard furnishings. Homes of infinite variety of design are built with a few types of bricks, and with lumber of standard sizes, and with water and heating pipes and fittings of standard dimensions",*
  W. Edwards Deming

6G → What is it? When will it come? What role will AI play?

A very broad look into the crystal ball

Disclaimer

6G does not exist

6G is going to be an evolution and a revolution together

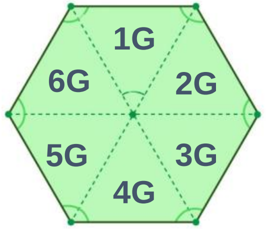
6G is going to try and address all of the existential risks already discussed but will introduce different ones

What Wikipedia says …

- The frequency bands for 6G are undetermined
    - Somewhere in the Terahertz and millimetre ranges (100GHz to 3THz)
    - Vortex or spinning radio waves are being considered
- Data rates are somewhat undetermined
    - Several Gigabits per second are anticipated
        - Research results are suggesting 200+ Gb/s, with vortex approaches 1+ Tb/s
    - Data rate is likely to be very volatile as noise sources are much more complex and with complex interactions
- AI will play a significant role
    - In operation and in design

Consequences ????

- The attack surface of 6G is unknown
  - And is likely to be unknown throughout its deployment
- 6G is an unknown enigma that fits to what Rumsfeld suggested are in the gap between known unknowns and unknown unknowns
  - “There are known knowns; there are things we know we know. We also know there are **known unknowns**; that is to say we know there are some things we do not know. But there are also **unknown unknowns**—the ones we don't know we don't know”



Mobile Generations, 3GPP Releases

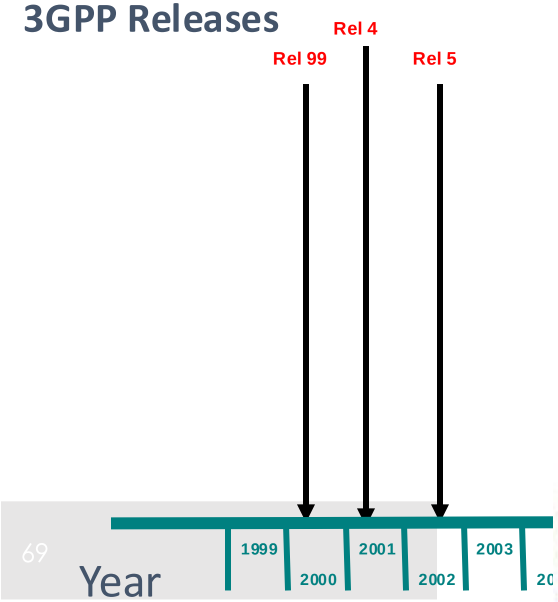
Mobile ‘Generations’

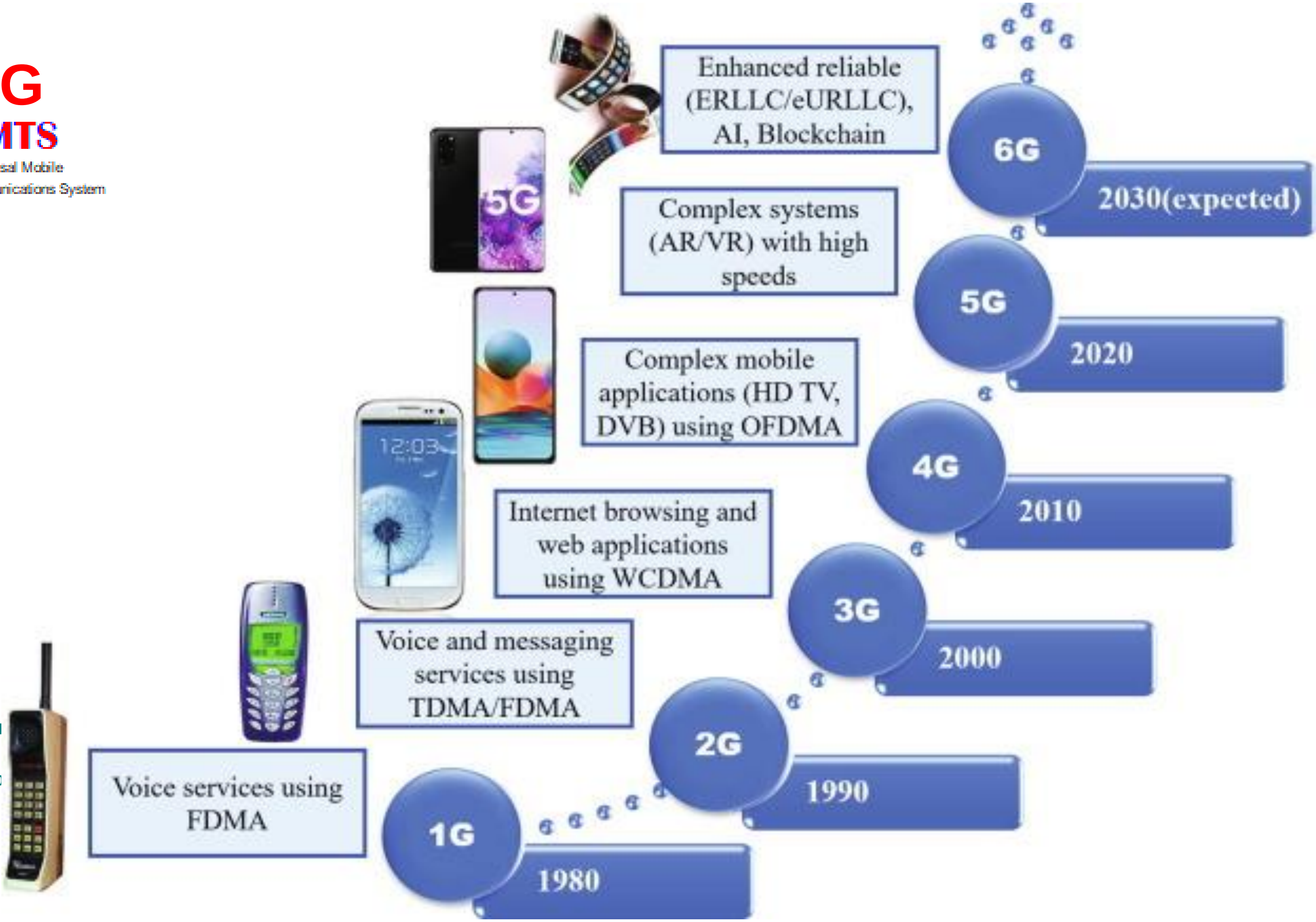
3G

UMTS

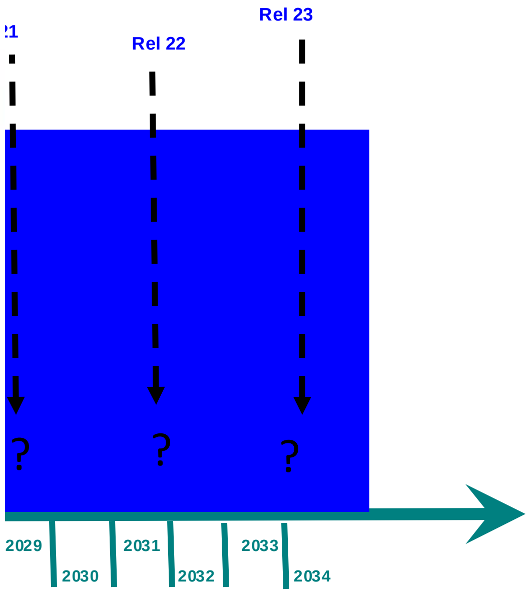
Universal Mobile Telecommunications System

3GPP Releases



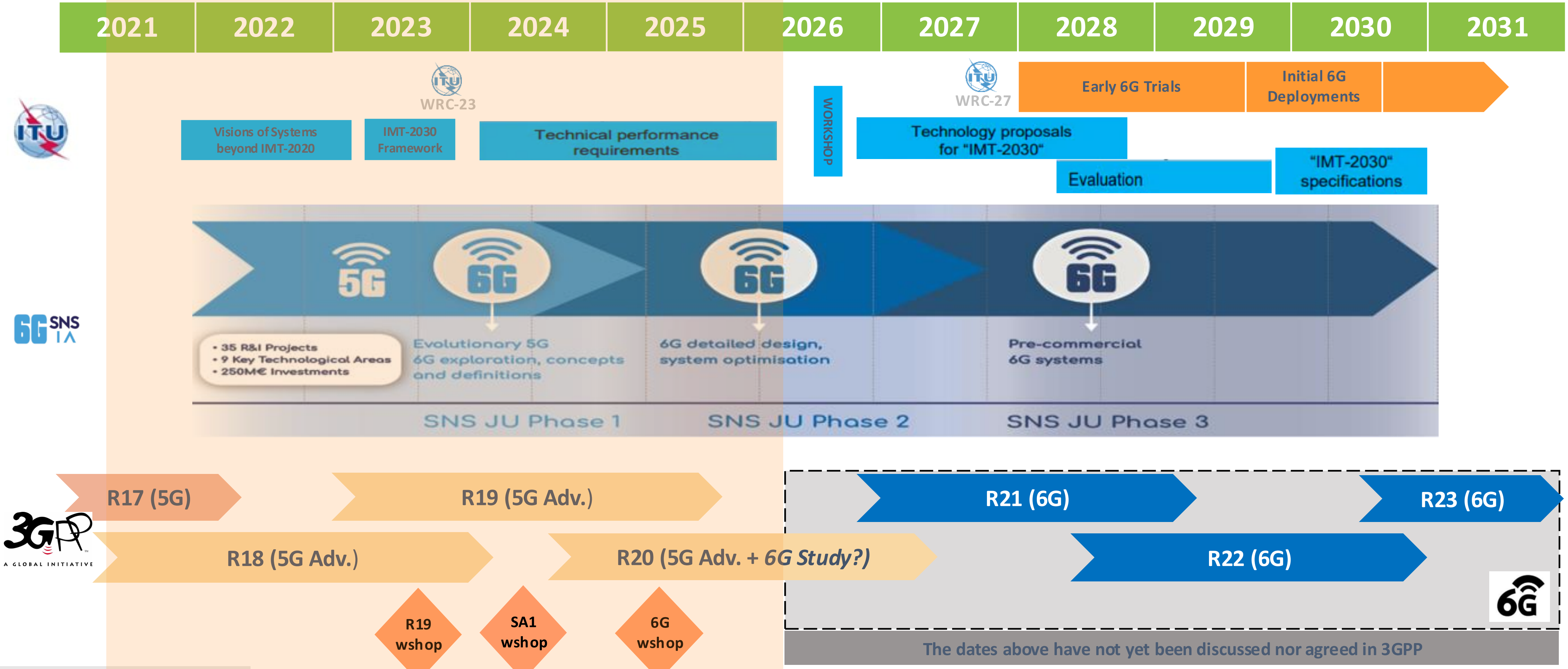

Enhanced reliable (ERLLC/eURLLC), AI, Blockchain
6G
2030(expected)
Complex systems (AR/VR) with high speeds
5G
2020
Complex mobile applications (HD TV, DVB) using OFDMA
4G
2010
Internet browsing and web applications using WCDMA
3G
2000
Voice and messaging services using TDMA/FDMA
2G
1990
Voice services using FDMA
1G
1980
5G
12:03

6G



Source: https://doi.org/10.1016/j.jksuci.2022.03.019

6G, Window of Opportunity (for pre-standards work)



2021 | 2022 | 2023 | 2024 | 2025 | 2026 | 2027 | 2028 | 2029 | 2030 | 2031

ITU
WRC-23
WRC-27
Visions of Systems beyond IMT-2020
IMT-2030 Framework
Technical performance requirements
WORKSHOP
Technology proposals for "IMT-2030"
Evaluation
"IMT-2030" specifications
Early 6G Trials
Initial 6G Deployments
6G SNS IA
5G
6G
• 35 R&I Projects
• 9 Key Technological Areas
• 250M€ Investments
Evolutionary 5G 6G exploration, concepts and definitions
6G detailed design, system optimisation
Pre-commercial 6G systems
SNS JU Phase 1
SNS JU Phase 2
SNS JU Phase 3
3GPP A GLOBAL INITIATIVE
R17 (5G)
R19 (5G Adv.)
R18 (5G Adv.)
R20 (5G Adv. + 6G Study?)
R21 (6G)
R23 (6G)
R22 (6G)
R19 wshop
SA1 wshop
6G wshop

The dates above have not yet been discussed nor agreed in 3GPP

6G, are we there yet?

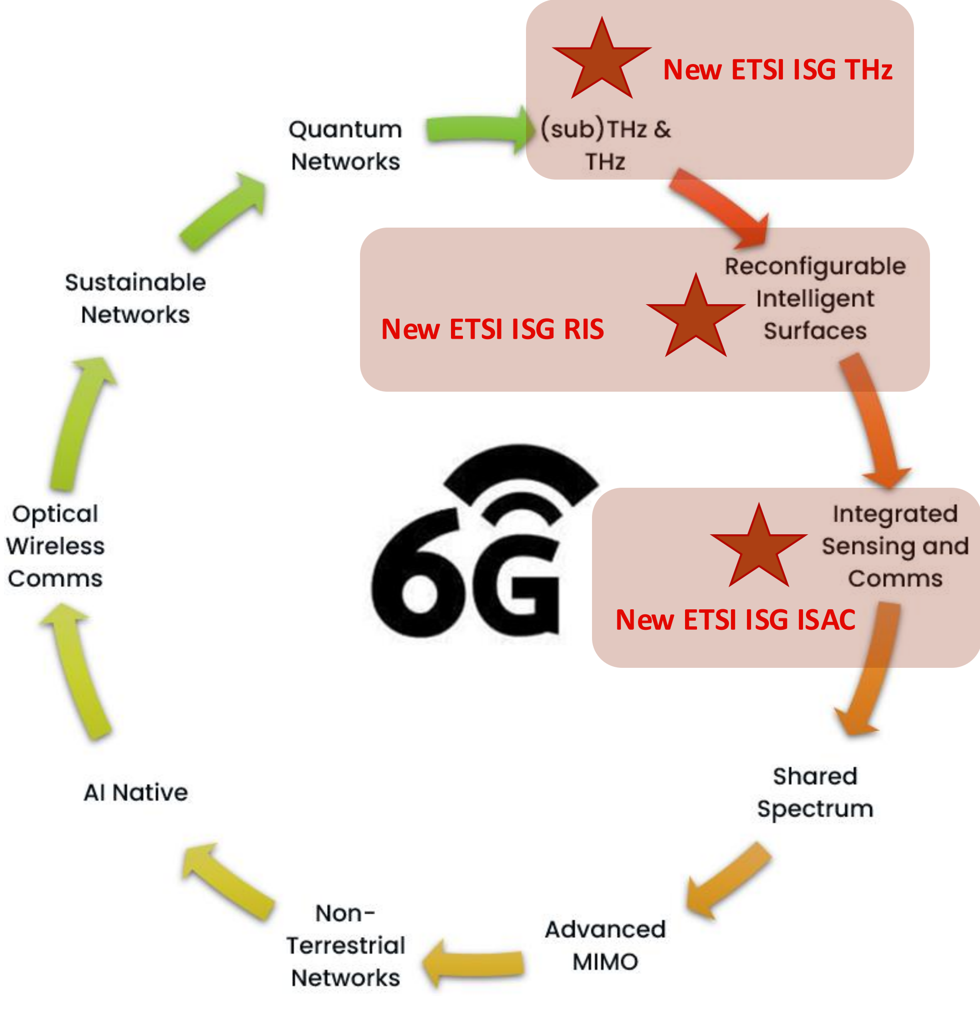
Current assumption is the first 6G services *may* be deployed in 2030, but of course expectations may change due to market pressures

6G is currently only at the Research & Vision phase, investigating potential technologies. More formal standards for 6G will follow later

We see many announcements of national, regional, corporate 6G programmes & visions with large investments in global 6G research

6G is expected to begin in 3GPP in Rel-20 (6G initial studies) and Rel-21 (6G service requirements), starting around 2024 -> 2025 ***

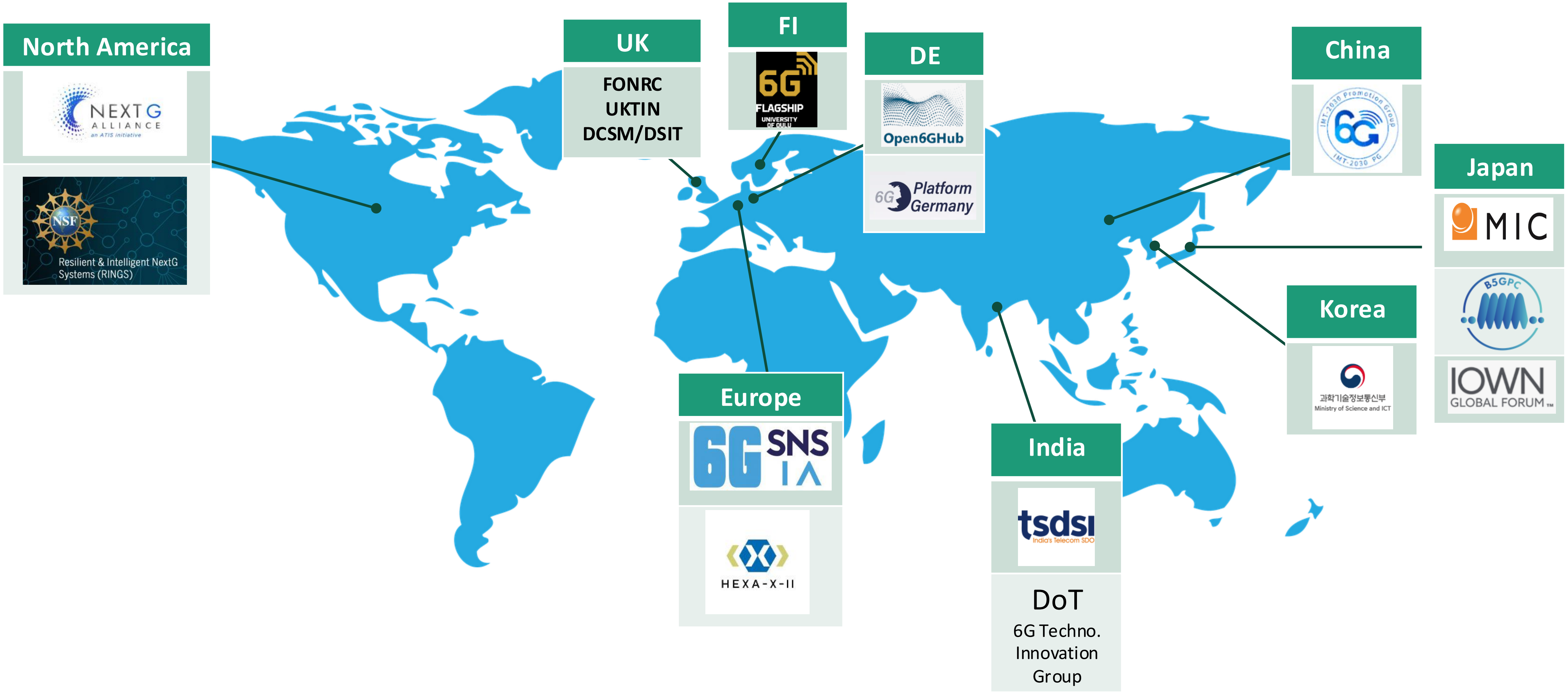
Recent consensus on "what is 6G" – a mixture of gradual technology **evolutions** from 5G with some **revolutionary** new concepts



Potential candidate B5G / 6G Technologies

***
NOTE: BEYOND R19, These are "indicative and estimated" dates only

(some of the) 6G Initiatives Worldwide



North America

NEXT G ALLIANCE an ATIS initiative

NSF Resilient & Intelligent NextG Systems (RINGS)

UK

FONRC
UKTIN
DCSM/DSIT

FI

6G FLAGSHIP UNIVERSITY OF OULU

DE

Open6GHub

6G Platform Germany

Europe

6G SNS IA

HEXA-X-II

India

tsdsi India's Telecom SDO

DoT
6G Techno. Innovation Group

China

IMT-2030 Promotion Group 6G

Korea

과학기술정보통신부 Ministry of Science and ICT

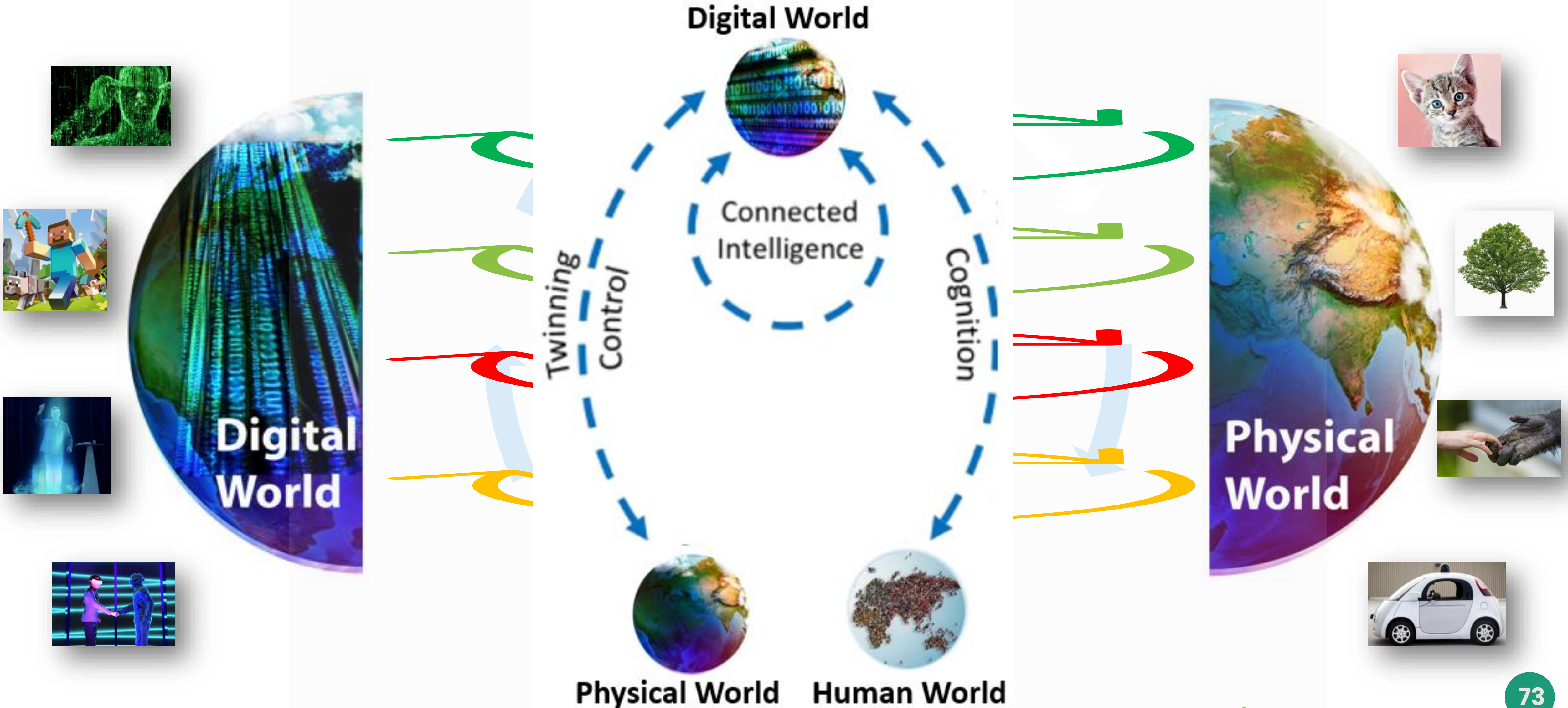
Japan

MIC

B5GPC

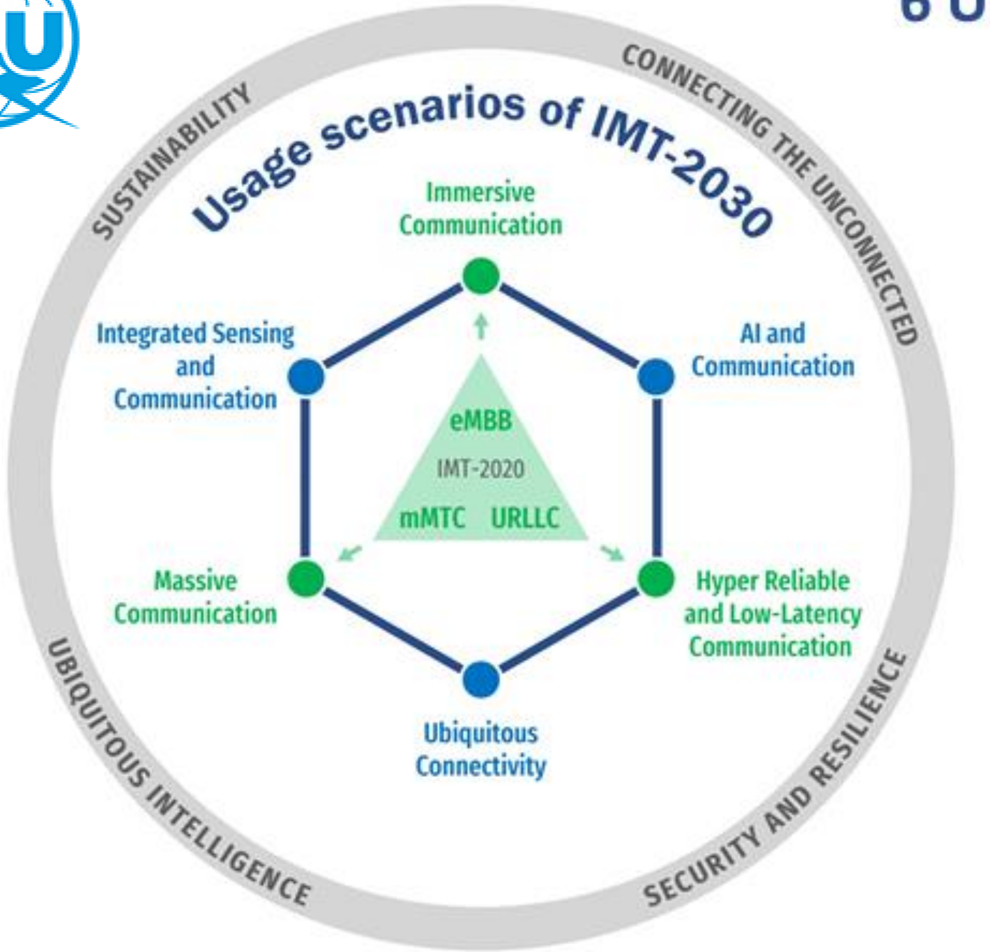
IOWN GLOBAL FORUM

Common Vision emerging from early 6G research



Redrawn from Nokia / HEXA-X inspired figures

IMT-2030 Usage scenarios and overarching aspects



So called "Wheel diagram"
Source: Document 5/131 and edited in SG 5

6 Usage scenarios

Extension from IMT-2020 (5G)

eMBB	➡	Immersive Communication
mMTC	➡	Massive Communication
URLLC	➡	HRLLC (Hyper Reliable & Low-Latency Communication)

New

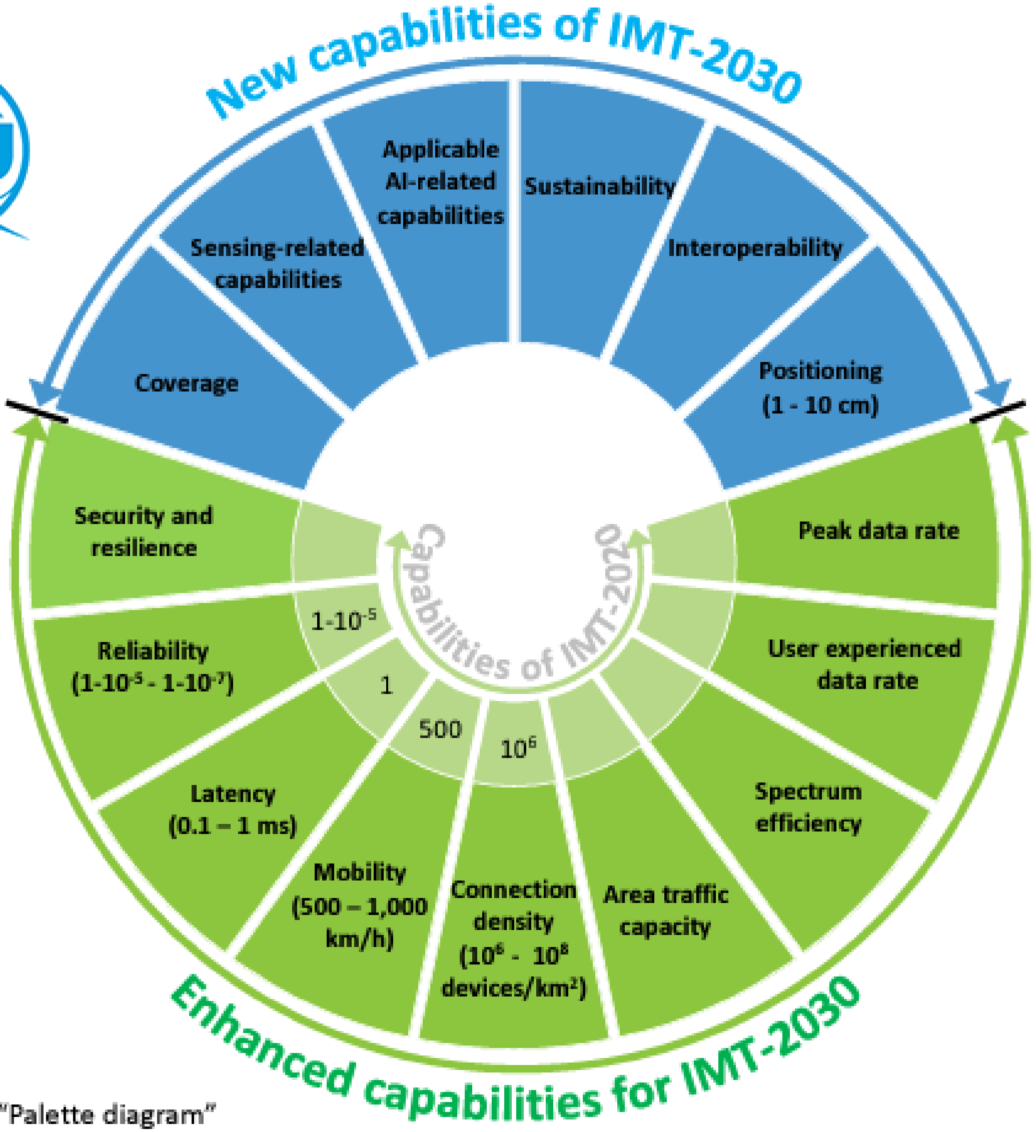
- Ubiquitous Connectivity
- AI and Communication
- Integrated Sensing and Communication

4 Overarching aspects:

act as design principles commonly applicable to all usage scenarios

Sustainability, Connecting the unconnected,
Ubiquitous intelligence, Security/resilience

IMT-2030 Capabilities


New capabilities of IMT-2030
Applicable AI-related capabilities
Sustainability
Sensing-related capabilities
Interoperability
Coverage
Positioning (1 - 10 cm)
Security and resilience
Peak data rate
Capabilities of IMT-2020
1-10-5
Reliability (1-10-5 - 1-10-7)
User experienced data rate
1
500
10^6
Latency (0.1 – 1 ms)
Spectrum efficiency
Mobility (500 – 1,000 km/h)
Connection density (10^6 - 10^8 devices/km²)
Area traffic capacity
Enhanced capabilities for IMT-2030

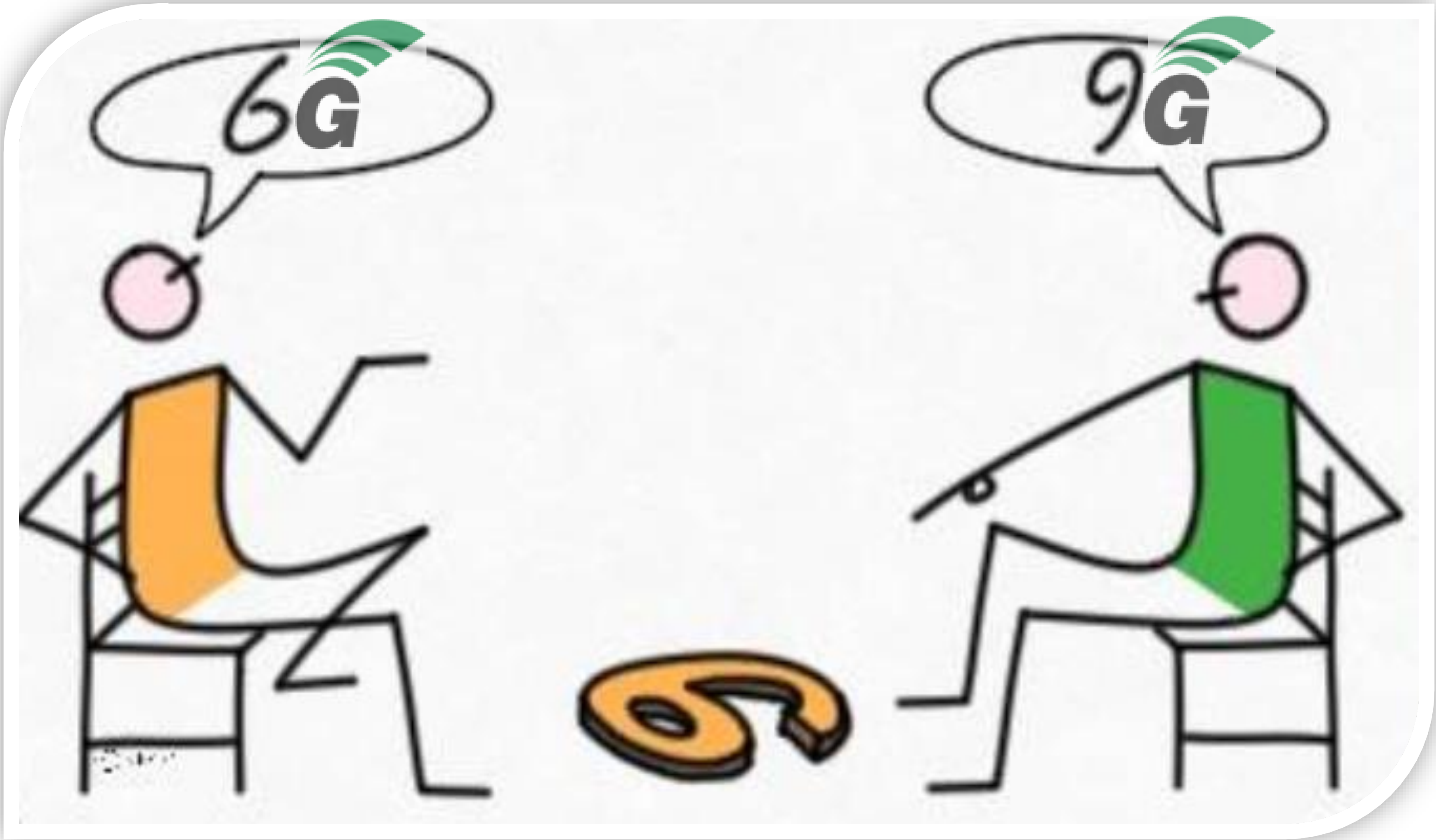
So called "Palette diagram"

The range of values given for capabilities are estimated targets for research and investigation of IMT-2030.

All values in the range have equal priority in research and investigation.

For each usage scenario, a single or multiple values within the range would be developed in future in other ITU-R Recommendations/Reports.

Future Mobile Generations – It’s just a question of perspective



So - 6G and AI?

AI in the design phase

AI in operations

Behaviour

- In an ideal world we always act altruistically (as individuals, as societies)
  - disinterested and selfless concern for the well-being of others
  - the 6G system should be altruistic by default (and equitable too)
- In the real world we tend to be act selfishly
  - In transport (driving)
    - Hogging lanes, harassing other road users, my car, my privilege, and so on
    - Our mode of transport seems to change our personality too

Intelligence vs logic

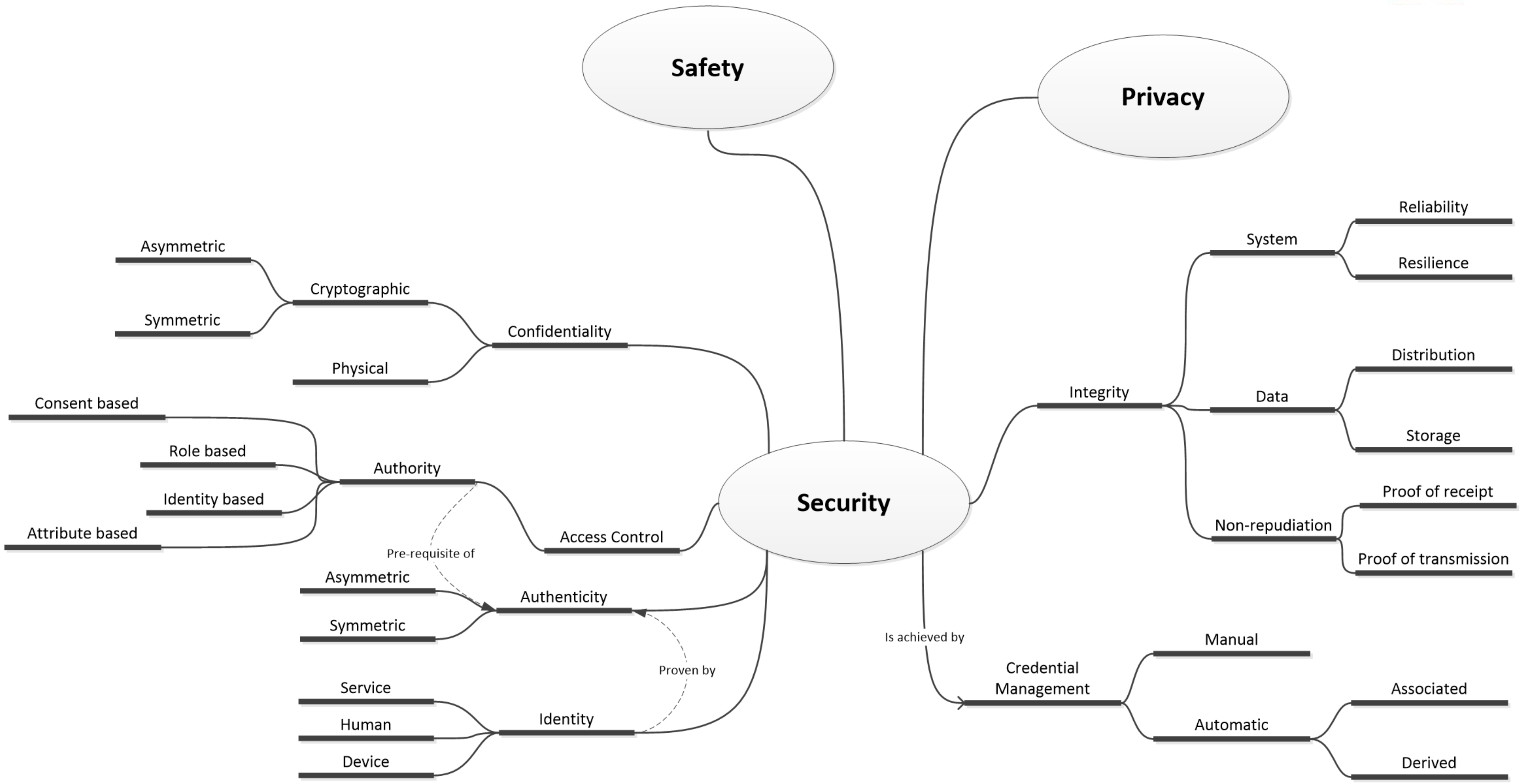
- A well designed logical system is not intelligent but may appear to be
  - In other words a set of logically consistent steps captures intelligence from the designer but has no intelligence of its own
    - Examples exist in IF .. THEN .. ELSE trees (IF Vehicle-Speed is greater than the cruise-control-speed THEN reduce speed, ELSE IF Vehicle-Speed is less than or cruise-control-speed THEN increase speed ELSE IF Vehicle-Speed is equal to cruise-control-speed THEN maintain speed)
- However an intelligent system is often selected where the decision trees are more complex, deal with more variables, and have an indeterminate state
  - “Intelligent cruise control” will default to appearing to have the same behaviour as normal cruise control

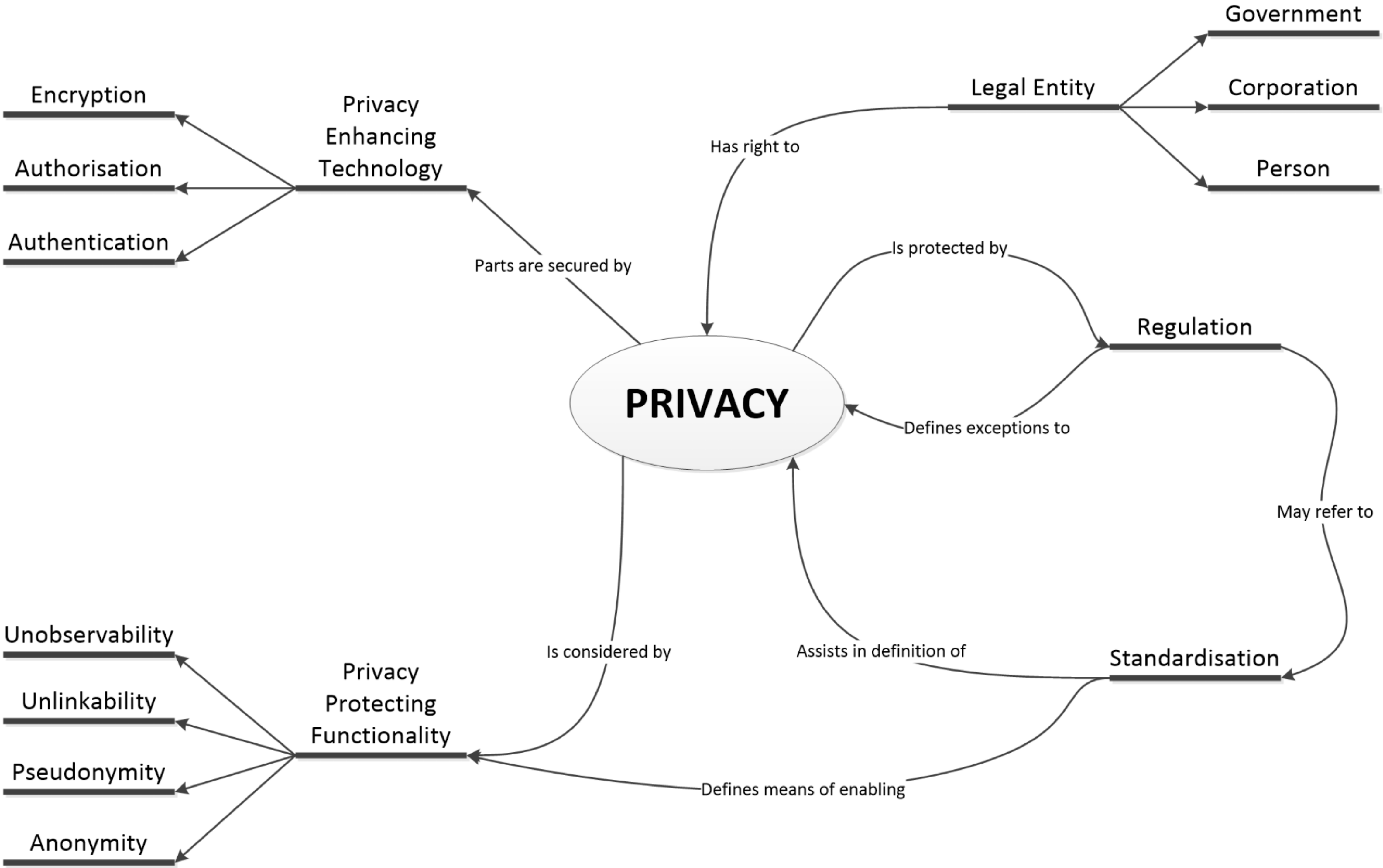
AI in design

- The problem
  - 6G is complex with an error prone radio interface, with handling multiple concurrent services, broadcast, unicast, multicast, protected (VPNs and public safety provisions), unprotected (consumer?), linking users to local and remote services, edge and core routing divergence, anticipatory design
- The opportunity
  - Lots of meta-data on how cellular has evolved exists → LLMs for design?
  - Simulation to drive design decisions → Common industry practice

The AI Act?

- Areas which relate to the security of AI:
  - Article 9 Risk Management System
  - Article 10 Data and Data Governance
  - Article 11 Technical Documentation
  - Article 12 Record-keeping.
  - Article 13 Transparency & Provision of Info to Users
  - Article 15 Accuracy, Robustness & Cybersecurity
  - Article 17 Quality management system.
  - Article 40 States that conformance to harmonised standards cited in the Official Journal (OJ) give presumption of conformity.
  - Articles 41 to 50. Testing and Certification - Part of Conformity assessment activities.


Safety
Privacy
Security
Confidentiality
Cryptographic
Asymmetric
Symmetric
Physical
Access Control
Authority
Consent based
Role based
Identity based
Attribute based
Pre-requisite of
Authenticity
Asymmetric
Symmetric
Proven by
Identity
Service
Human
Device
Integrity
System
Reliability
Resilience
Data
Distribution
Storage
Non-repudiation
Proof of receipt
Proof of transmission
Is achieved by
Credential Management
Manual
Automatic
Associated
Derived


PRIVACY
Privacy Enhancing Technology
Encryption
Authorisation
Authentication
Parts are secured by
Has right to
Legal Entity
Government
Corporation
Person
Is protected by
Regulation
Defines exceptions to
May refer to
Standardisation
Assists in definition of
Defines means of enabling
Is considered by
Privacy Protecting Functionality
Unobservability
Unlinkability
Pseudonymity
Anonymity

Consequences …

- AI Act requires combined approach to safety, privacy and security
- AI Act works hand in hand with other instruments: RED, CRA, CSA, NIS2, eIDAS, EU Digital Wallet, “Blue book”, …
- A crude estimate of the AI Act suggests that 6G networks are going to be high risk (because of the customers and business it supports)

- AI can work to determine casual and causal links in behaviour to break privacy, bypass security, and defeat safety

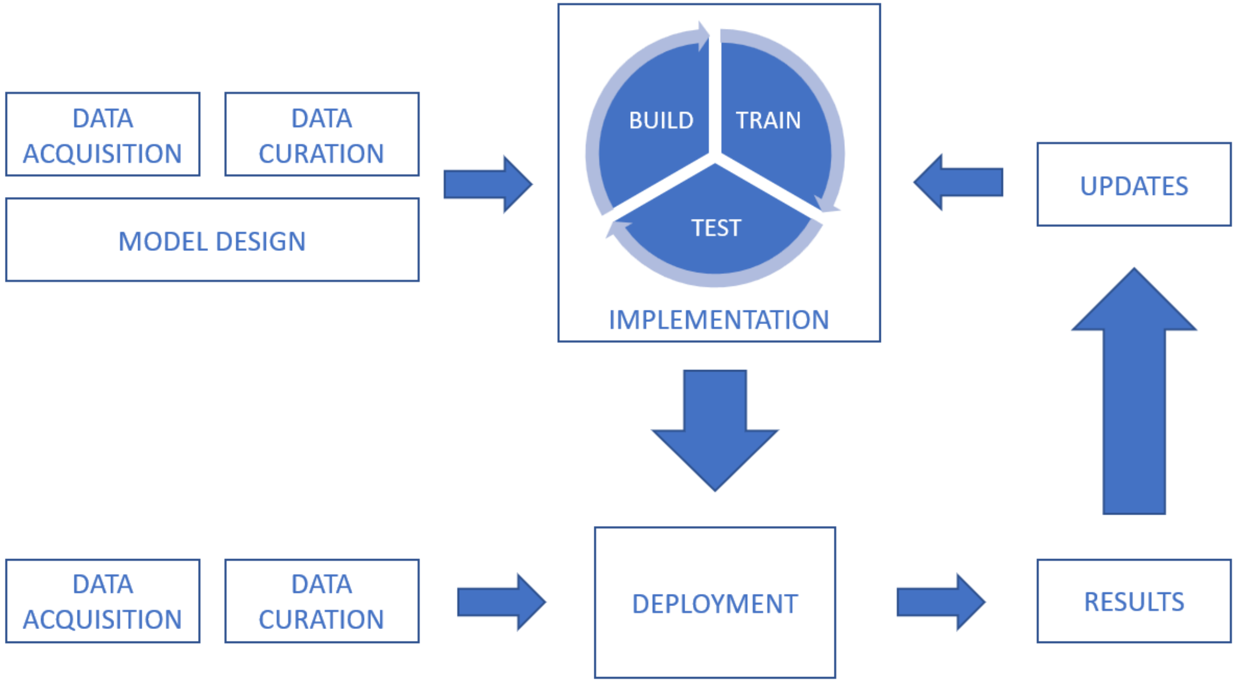
What is the 6G problem AI solves?

- It doesn’t as there is no problem yet
- What we can anticipate:
  - 6G will be massively mutable compared to any other generation of network
  - The speed and rate of mutation will be such that it cannot be managed by human administrators
  - Micro-mobility will require real time modification of the network connection

Machine learning cycle

- Lots of points of attack (every arrow, every box)

Lifecycle Phase	Issues
Data Acquisition	Integrity
Data Curation	Integrity
Model Design	Generic issues only
Software Build	Generic issues only
Train	Confidentiality, Integrity, Availability
Test	Availability
Deployment	Confidentiality, Integrity, Availability
Upgrades	Integrity, Availability

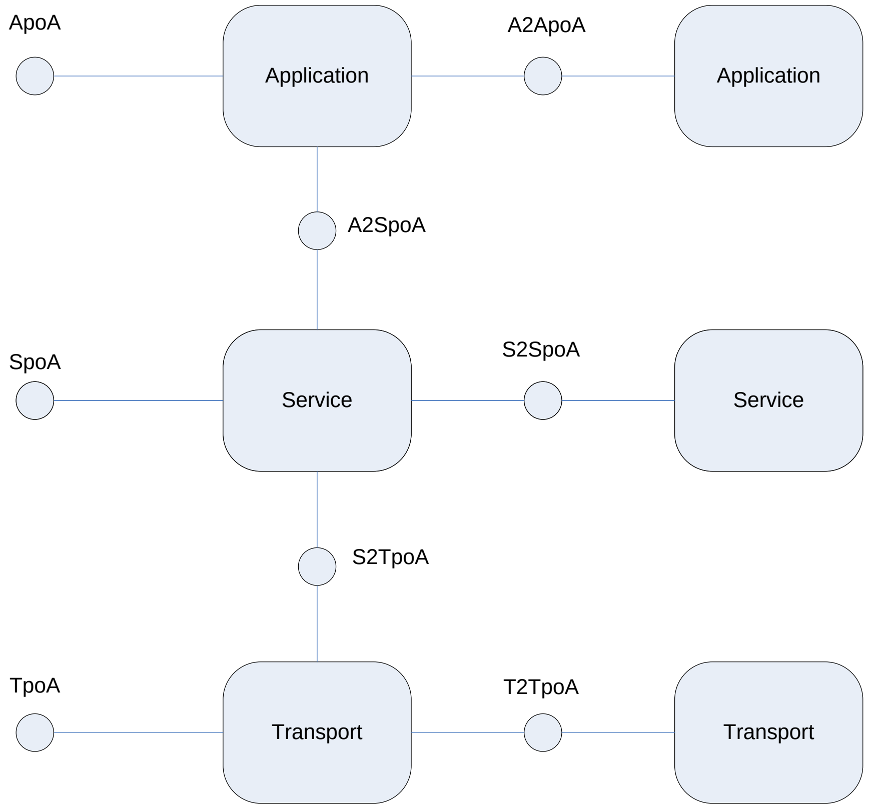


Design challenges

- Bias
  - Not always bad but has to be considered
  - Bias in favour of balance of all users of the network
- Ethics
  - Do ethics have a role in 6G networks? Yes - open question?
- Explicability and transparency
  - **explicability**: property of an action to be able to be accounted for or understood
  - **transparency**: property of an action to be open to inspection with no hidden properties

Points of attachment to networks

- Slight change from the OSI-7, IETF-5 models towards a simplified 3 plane model
  - OTT services lie in the application plane
  - Using service building blocks in the Service plane
  - Using transport/network building blocks in the Transport plane
- Each plane offers training data



AI and cryptography

- Cryptography is not Security
    - “A cryptosystem should be secure even if everything about the system, except the key, is public knowledge”, Kerchoff
    - Technical security measures give hard and fast assurances for explicit environments
        - E.g. the contents of an encrypted file cannot, ever, be seen by somebody without the key to decrypt it.
    - cryptography provides us with a complicated set of locks
        - we don’t need to bother installing a lock on door if we have an open window next to it - the attacker will ignore the locked door and enter the house through the open window
- Accelerating cryptanalysis
    - Key space is huge and a lot of cryptanalysis is statistical and AI is brilliant at statistics

AI in 6G - some thoughts

- Context driven reactivity
  - We already design network capacity to cater for events
  - EXAMPLE: The Emirates stadium in London has poor coverage most of the time but on match/event days cell capacity is increased both at the stadium and all routes to it
  - In 6G with beam forming and micro-cell architecture at the core of the design context is shorter in duration and not forecastable on calendar time
- Attack surface mapping
  - The attack surface is mutable and contextual so being able to continuously model it can allow efficient deployment of protection measures

Time to open the floor to questions

- Any topic?
  - Standards
  - AI
  - Security
  - Privacy
  - Safety
  - Forecasting

Thanks for listening

Scott CADZOW, scott at cadzow dot com, somewhere in England