Ethics for Quantum Computing and Artificial Intelligence

AI and Quantum computing codes of ethics

Roberto Magnani June 29th 2023

Ethical Considerations in Quantum Computing

quantum computing, quantum communication and quantum sensing

Promise of paradigm-shifting computational capacity with significant ethical consequences.

On a technical level, imposition of fairness and ethical constraints on computation.

quantum ethics are the cross-disciplinary intersection of

quantum information science

technology ethics

moral philosophy

→

Safety: This refers to how well an AI can avoid harming humans. ...
Security: This refers to how well an AI can prevent other systems from attacking it or taking advantage of it in some way. …
Privacy: ...
Fairness:

Need for a roadmap for ethical quantum computing to set out prospective for research programmes.

QC impact on cryptography

protection of data work in different ways:

- **Symmetric algorithms** use the same secret key to encrypt and decrypt data.
  - *Example of utilisation: Clients in the banking industry rely heavily on symmetric cryptography to ensure the confidentiality of data in core banking applications*
- **Asymmetric algorithms**, also known as public key algorithms, use two keys that are mathematically related: a public key and a private key.
  - *Example of utilisation: Automotive connected cars for vehicle-to-everything (V2X) communications and to verify the integrity of the firmware loaded into vehicles*

Current Cryptography

Security Levels for Popular Symmetric and Asymmetric Cryptosystems

The following table indicates the security level of some of the most popular symmetric and asymmetric cryptosystems.

Security Level	Symmetric Cryptosystem Key Size	RSA Key Size	ECDSA Curve Key Size
80	2TDEA (112 bits)	1024 bits	prime192v1 (192 bits)
112	3TDEA (168 bits)	2048 bits	secp224r1 (224 bits)
128	AES-128 (128 bits)	3072 bits	secp256r1 (256 bits)
192	AES-192 (192 bits)	7680 bits	secp384r1 (384 bits)

Ref : https://ieeexplore.ieee.org/abstract/document/8967098/citations#citations

Classical computing
Cost of breaking
$10-100M

Secure
30-40 years ahead

ALERT

160-bit elliptic curves can be broken with a 1000-qubit QC

1024-bit RSA would need roughly 2,000 qubits

An example: blockchain

Post-quantum cryptosystems

Blockchain and other Distributed Ledger Technologies (DLTs) have ability to provide transparency, redundancy and accountability.

- *such characteristics are provided through public-key cryptography and hash functions*

Quantum Computing has opened the possibility of performing attacks

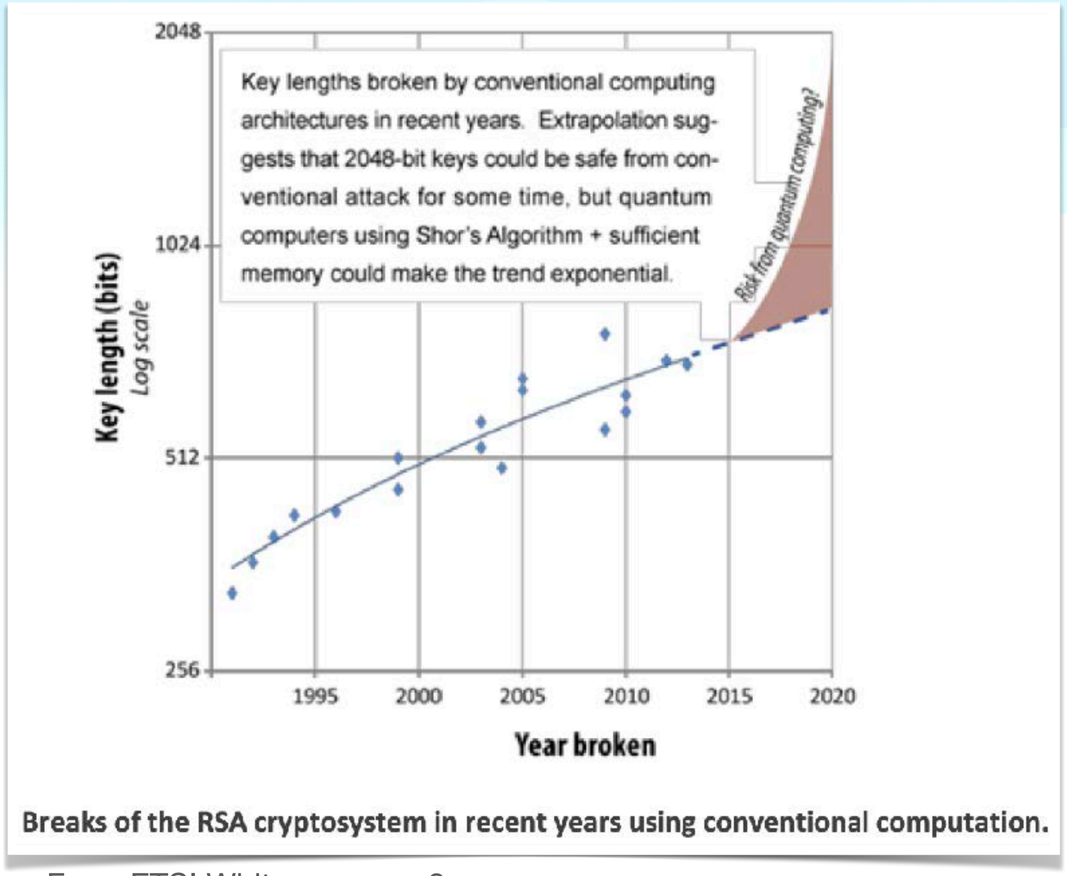
- *Grover's and Shor's algorithms such threaten both public-key cryptography and hash functions*
  - *forcing to redesign blockchains to make use of cryptosystems* ***known as post-quantum cryptosystems***
  - ***Guideline are coming*** *on post-quantum blockchain security for researchers and developers*

A definition of Quantum-Safe cryptography

European Telecommunications Standards Institute (ETSI)

ETSI plays a key role in supporting regulation and legislation with technical standards and specifications

"Quantum-safe cryptography refers to efforts to identify algorithms that are resistant to attacks by both classical and quantum computers, to keep information assets secure even after a large-scale quantum computer has been built."

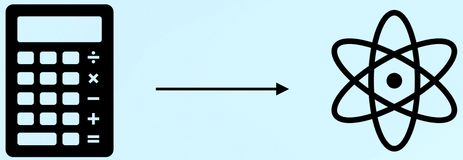


Breaks of the RSA cryptosystem in recent years using conventional computation.

From ETSI White paper nr 8

Quantum cryptography

Physic instead of math
Cambridge Quantum delivered an encryption key anyway there are still limit and challenges



Photons to transmit over fiber optic wires representing binary key

Properties of quantum mechanics

- Particles can exist in more than one place or state at a time
- A quantum property cannot be observed without changing or disturbing it
- Whole particles cannot be copied

NIST First Four Quantum-Resistant Cryptographic Algorithms

U.S. National Institute of Standards and Technology (NIST)

For general encryption, used when we access secure websites,

selected the **CRYSTALS-Kyber** algorithm.

small encryption keys that two parties can exchange easily,

speed of operation.

For digital signatures, used when we need to verify identities during a digital transaction or to sign a document remotely,

CRYSTALS-Dilithium,

FALCON

SPHINCS+.

Roberto Magnani June 29th 2023

Examples of quantum secure algorithms

Lattice-based cryptography	Code-based cryptography	Multivariate-based cryptography
Based on abstract structures of mathematics. It currently looks like the most promising method.	Uses error-correcting-codes that allows read or data being transmitted to be checked for errors and corrected in real time.	Based on solving multi variable equations. These equations are hard to solve using brute force.

Ryan Arel TechTarget “Explore the impact of quantum computing on cryptography”

Cybersecurity measurement

maximum value and effect for finite cybersecurity-related investments

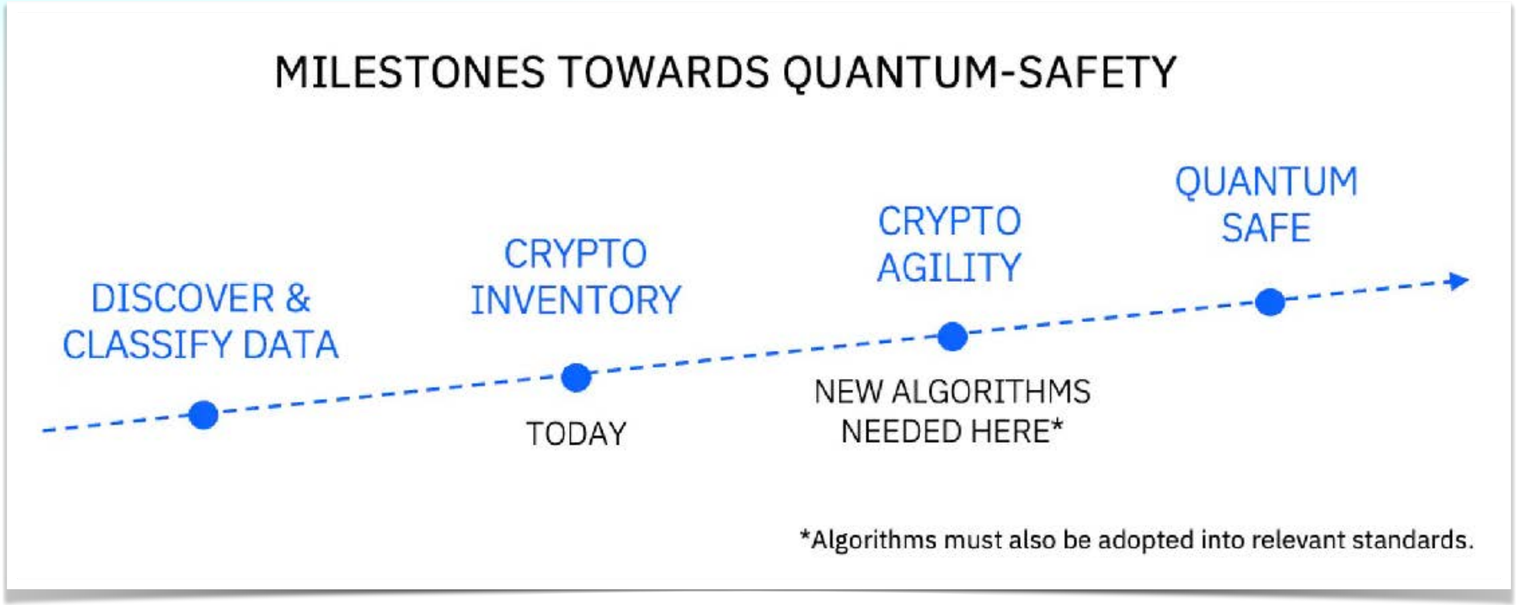
NIST plans to:

- Create a compilation of tools, research, and standards and guidelines that address cybersecurity measurements. The portfolio of resources and activities is continuously expanding.
- Participate actively in voluntary standards initiatives related to cybersecurity measurements.
- Launch a collaboration space for the community to share views and resources relating to cybersecurity measurements.
- Develop a roadmap to address and advance cybersecurity measurement challenges and solutions.

Preparing to adopt quantum-safe standards

key milestones to adopt new quantum-safe standards:

- **Discover and classify data:** define the value of data and understand compliance requirements.
- **Create a crypto inventory:** how your data is encrypted. Crypto inventory includes encryption protocols, symmetric and asymmetric algorithms, key lengths, crypto providers, etc.
- **Embrace crypto agility:** plan a multi-year journey as standards evolve and vendors move to adopt quantum-safe technology.



From IBM introduction to Quantum Safe

Distribution of Computer power

ethical concerns

Access

typical person or smaller company will ever own a quantum computer due to their physical and technical complexity

how to share knowledge gleaned from quantum computers

Health care and life sciences

QC to play a significant role in gene editing by helping researchers understand the effects of subtle genetic changes

Quantum Computing Arms Race

ethical considerations related to the global race for quantum supremacy

Global tensions and the quantum "arms race": $5 billion on quantum technologies in 2022 by China, India, Japan, Germany, Netherlands, Canada, the United States …….

Quantum computing is seen as critical to future defense technologies;

consequence of ratcheting up tensions between nations

potential risks of militarization and the need for international cooperation in establishing ethical guidelines and regulations.

QC and emerging materials

Mindful to avoid environmental complications

QC expected to supercharge research and development of new materials.

perform sophisticated simulations of how small, molecular-level changes alter a material's properties

leading to a major boon in

drug discovery

carbon capture

chemical production …..

Quantum Bias and Fairness

importance of addressing bias and fairness issues in quantum algorithms and applications.

the **fairness** of quantum decision model A is to treat all input states equally,

i.e., there is not a pair of two closed input states

that has a large difference between their corresponding outcomes fairness issues in quantum algorithms and applications.

Need

to prevent potential biases in data used to train quantum systems

for diverse and inclusive development processes to prevent perpetuating biases and inequalities

Bias can impact the performances

Algorithms and data

Algorithms: engaged in economically/Social/Legal important decisions.

Finance, sentencing in criminal courts, resume screening, pricing, hiring, ad-placement, lending decisions and the news media that citizens consume.

Public debate about bias and unfairness in machine-guided decisions, including several high-profile allegations in finance

Policymakers in multiple countries, who have adopted or are considering fairness-related regulations for algorithms

Bias in data
Impacts

Data potential biases to consider:

1. **Sample Bias:** data used not representative of the diverse range of inputs

   if the training data predominantly represents a particular demographic or specific experimental conditions, the system may not generalize well to other groups or situations.

2. **Labeling Bias:** labeling data for training due to human annotators

3. **Historical Bias:** training data may reflect historical biases and inequities,.

Bias prevention

promote diverse and inclusive development processes

1. **Representation:** Include diverse perspectives and voices in the development with diverse teams.
2. **Ethical Guidelines:** ethical guidelines and principles for development process.
3. **Data Collection:** diverse and inclusive dataset that adequately represents the target population.
4. **External Review and Auditing:** help in identifying and rectifying biases.

diverse and inclusive development processes are necessary to prevent the perpetuation of biases and inequities in quantum systems.

Exacerbating existing risks

AI, data harvesting, and privacy: QC able to process large volumes of data incentivise collection even more consumer data, supercharging the data harvesting that already takes place.

Explainability: quantum machine learning, presents the ultimate black box problem. With quantum computers, explainability is more of a physics problem than a programming problem.

Environmental Impact

need for sustainable practices

1. ***Energy Requirements:*** Most of QC operate at extremely low temperatures. Cryogenic refrigerators consume a significant amount of energy and the computational operations are energy-intensive

2. ***Environmental Impact:*** implicationsthrough greenhouse gas emissions and contributions to climate change. The energy required to power quantum computing can rely on non-renewable sources like fossil fuels the manufacturing processes has environmental impacts: extraction and processing of raw materials and waste generation.

3. ***Comparison to Classical Computers:*** Classical computers benefited from decades of optimization and advancements in energy efficiency. Quantum computers have a long way to go in terms of reducing their energy requirements

Mitigate the energy requirements and environmental impact

Strategies to be defined

1. **Energy Efficiency Research:** optimizing the design and architecture of hardware components, reducing the energy required for cooling, and developing more efficient algorithms to minimize computational operations.
2. **Renewable Energy Integration:** enewable energy sources, such as solar, wind, and hydroelectric power
3. **Lifecycle Assessment:** lifecycle assessments to mitigate environmental impactsnot only the energy consumption during operation but also manufacturing, transportation, and disposal of the hardware components.
4. **Recycling and Circular Economy:** recycling and waste management programs emphasizing a circular economy approach
5. **Policy and Standards:** Governments and regulatory bodies role in promoting sustainable practices in the development and operation

Addressing the energy requirements and environmental impact of quantum computers is essential for their long-term viability and adoption.

Ethical framework EU AI ACT

preserve the EU's technological leadership and ensure that European citizens benefit from new technologies

Enable Europe to lead a correct approach to any kind of artificial intelligence

Identify prohibited, high-risk areas that need to be monitored regulate conflicts and legal problems

Protect the rights of EU citizens, where laws are generally stricter and more restrictive than in the US or elsewhere

Difficulties in regulating technological change The risk of obsolescence given the speed of technological innovation

To get flowchart please link to below Burges&Salmon summary

https://media.licdn.com/dms/document/media/D4D1FAQELOTajTD8stw/feedshare-document-pdf-analyzed/0/1686992010045?e=1687996800&v=beta&t=XEx-V_KswNpBEzYTjICB5GEOYIaIJ1f_Ucjr9zGQx-s

EU AI ACT

Not admitted activities

Real-time” remote biometric identification systems in publicly accessible spaces;

“Post” remote biometric identification systems, with the only exception of law enforcement for the prosecution of serious crimes and only after judicial authorization;

Biometric categorisation systems using sensitive characteristics (e.g. gender, race, ethnicity, citizenship status, religion, political orientation);

Predictive policing systems (based on profiling, location or past criminal behaviour);

Emotion recognition systems in law enforcement, border management, workplace, and educational institutions

Indiscriminate scraping of biometric data from social media or CCTV footage to create facial recognition databases (violating human rights and right to privacy).

Rome Call for AI Ethics

From February 2020 to November 2022

The Rome Call for AI Ethics in 2020 is a commitment around ethics, rights, and education, aiming to promote an ethical approach to the design, development, and deployment of AI hosted by the Pontifical Academy for Life, IBM, FAO Microsoft and the Italian Ministry of Innovation to champion

3 areas: Ethics Education and Rights

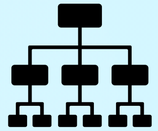
6 Principles: Transparency, Inclusion, Accountability, Impartiality, Reliability, Security and Privacy

Nov 2022 international workshop “Converging on the person. Emerging technologies for the common good”

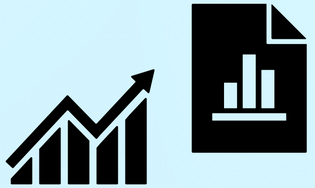
“ …It is good that theology continues to overcome eminently apologetic approaches, to contribute to the definition of a new humanism and to encourage mutual listening and mutual understanding between science, technology and society. The lack of a constructive dialogue between these realities, in fact, impoverishes the mutual trust which is the basis of all human coexistence and of all forms of "social friendship…”. (Pope Francis)

Digital Ethics Officer

Strengthen the transversality of the references and people involved



Sensitise and advise the different organisational entities

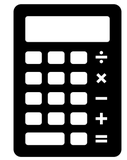


Conceiving and distributing an ethical chart

Be the ethical reference

Develop evaluation and control tools

Organise and lead the operational governance



Eliminate or minimise the ethical risks

Identify exposures and ethical risks

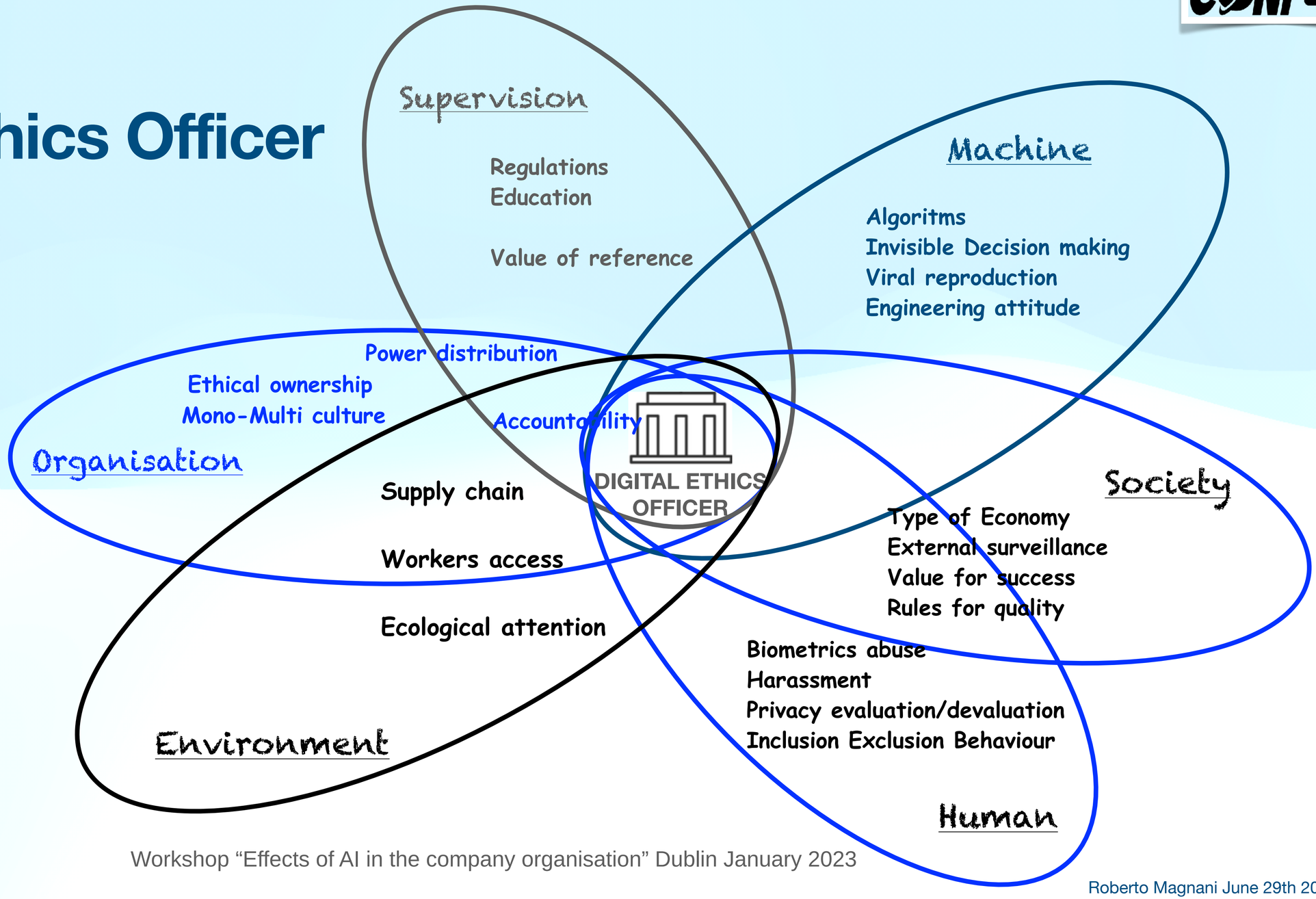
Deep knowledge

Integrate and improve the synergy

Organise internal reflections to evaluate feedbacks

Digital Ethics Officer

Challenges

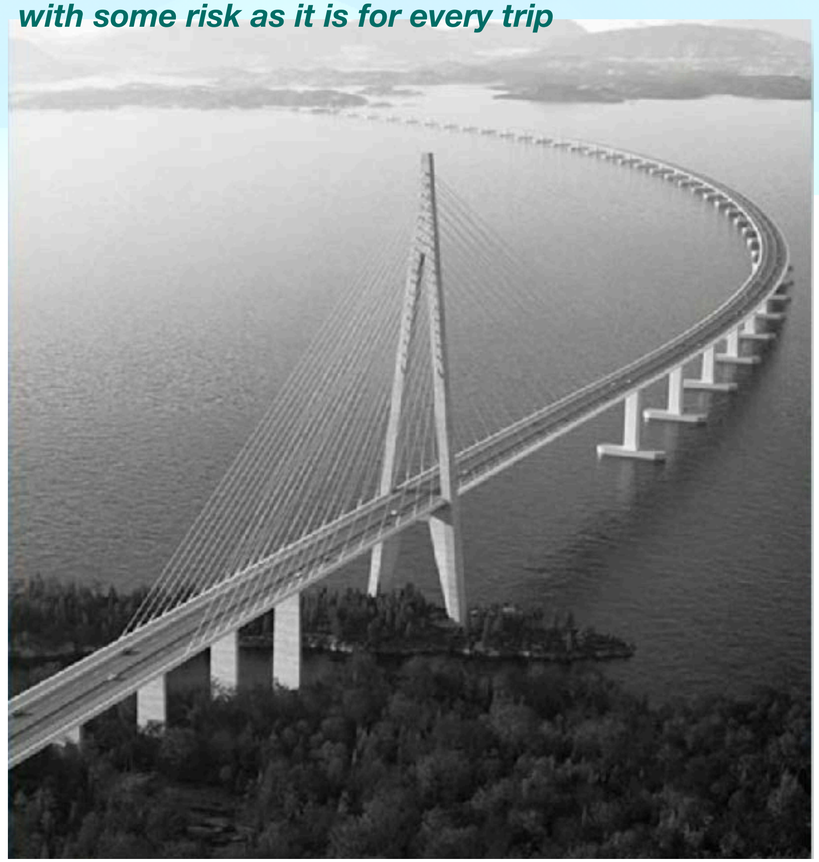


Conclusion

Start Preparing Today for Tomorrow's Quantum Ethics

- There are existing ethical frameworks
- Enterprises should convene internal leaders and experts to determine trigger events to act or increase investment.
- Emphasise the need for proactive ethical practices to maximise the benefits and minimise the risks

We are at the beginning of a journey, exciting, but with some risk as it is for every trip



The author

https://www.linkedin.com/in/robertomagnani/

Roberto Magnani

I help organizations in adopting good, transparent and explainable Artificial Intelligence and eventually exploring Quantum Computing.

MsC in Electronic engineering he developed his career in the IT sector in multinational laboratories in Italy, France, USA, Switzerland, Spain and Ireland. In the last decade he has been responsible for the Public Cloud Web services of a large multinational company in Europe in a technological campus in Dublin and then took on the responsibility of digital projects for Healthcare Life Sciences in EMEA, with the use of artificial intelligence. Since 2022 he has been an independent consultant; advisor of AEIT - Italian Association of Electronics, Electrotechnics, Informatics and Telecommunications, focusing on the ethical and regulatory aspects of artificial intelligence and the introduction of Quantum computing in industry. He is the author of articles and interventions in Italy and abroad on the same topics and recently of an instant book "Artificial intelligence for the professions" published by EBS.

Collaborating with no-profitorganisations

AEIT 1897

Avisor

AEIT is a cultural association and its aim is to promote and encourage:

- the study of electrical, electronic, automation, computer science and telecommunications sciences;
- the development of related technologies and applications in the broadest sense;
- the cultural growth and professional updating of its members in the areas indicated.

INSTITUT EUROPIA

Member

EuropIA acts mainly in Italy and France and promote san ethical and people-focused approach to the design and implementation of artificial intelligence solutions

ORSi Consilium

Co-founder

Free association of expertises that support individuals in skill upgrade in technology and crafts&arta

Thank you