VII CONFERENZA NAZIONALE

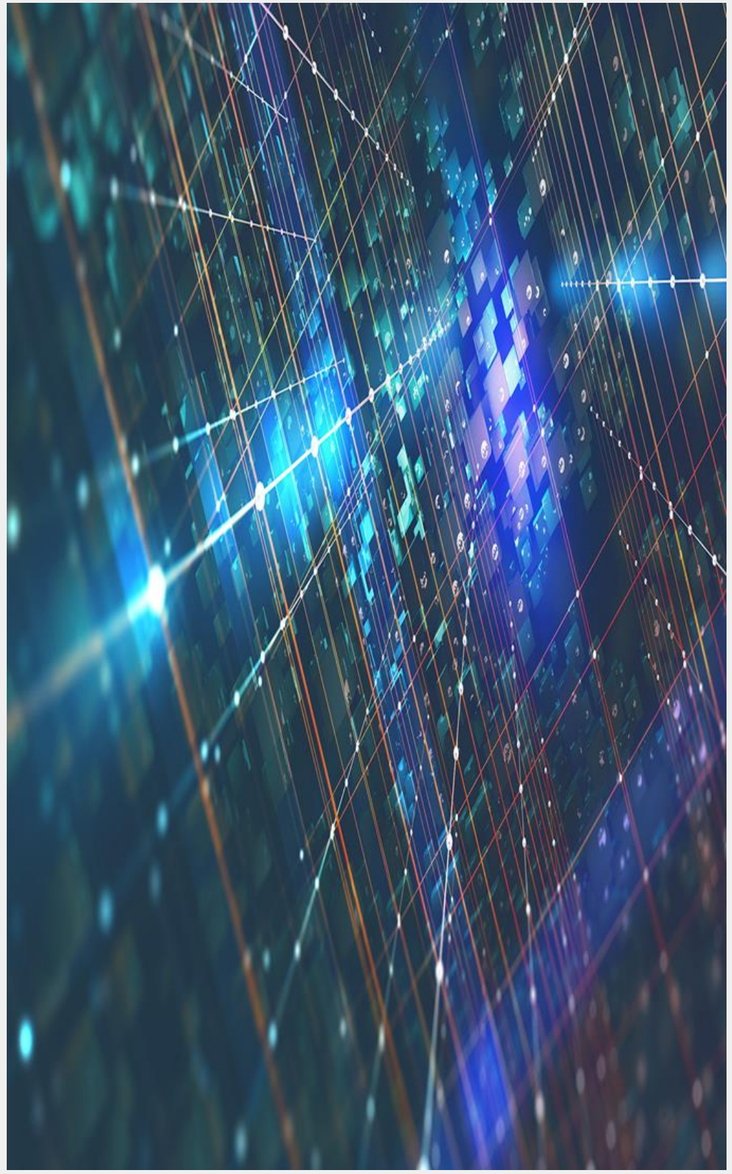
Sicurezza cibernetica e aerospaziale

Conferenza connessa al Master
«Competenze digitali per la Protezione dei Dati, la Cybersecurity e la Privacy»
Università degli Studi di Roma «Tor Vergata»

Dott.ssa Noemi Ferrari– CTO di Quantum Ket

Roma, Palazzo Wedekind, Piazza Colonna 366
7 aprile 2025

Quantum Ket



Tecnologie Quantistiche

Le **Tecnologie Quantistiche** rappresentano una classe di **tecnologie** ad **alto contenuto innovativo** che sfruttano i principi fondamentali della **Meccanica Quantistica** per manipolare in modo attivo gli **stati quantistici** della **materia.**

MQ

La **MQ** è la branca della Fisica, che descrive i fenomeni del **mondo microscopico**, come molecole, atomi e particelle subatomiche. Consente di **manipolare attivamente** gli stati quantistici della **materia**, aprendo nuove prospettive nel campo della scienza e dell'ingegneria avanzata.

Le Tecnologie Quantistiche: Cosa Sono

Le **Tecnologie Quantistiche** vengono suddivise in tre categorie:

Quantum Computing:

nuovo tipo di informatica che sfrutta la Meccanica Quantistica per estendere le capacità dei computer tradizionali e consentire lo sviluppo di **funzionalità innovative**.

Quantum Communication:

campo dell'Informatica Quantistica che si occupa della **trasmissione sicura** di informazioni e di sviluppare **sistemi resistenti** agli attacchi di potenziali **computer quantistici**

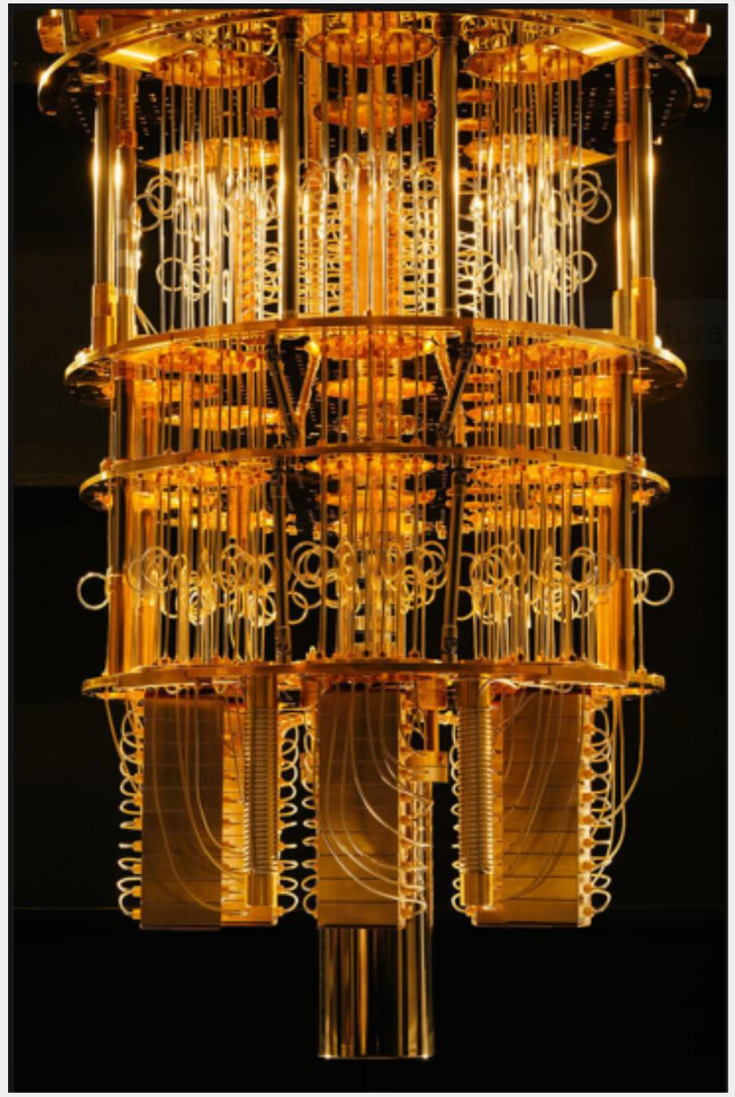
Quantum Sensing and Classical Sensing:

innovativa tipologia di sensori che, utilizzando **sistemi quantistici**, è in grado di effettuare **misurazioni ordini di grandezza più accurate** rispetto ai sensori classici.

Le Tecnologie Quantistiche: Quantum Computing

Quantum Computing: campo **pionieristico** dell'informatica, ha introdotto un **nuovo paradigma** di **calcolo** capace di:

- **potenziare esponenzialmente** le **capacità computazionali**;
- risolvere **problemi complessi** che **non** possono essere **affrontati /risolti** dai sistemi **classici tradizionali**, inclusi l'**HPC** (*High Performance Computing*) e l'**Intelligenza Artificiale**



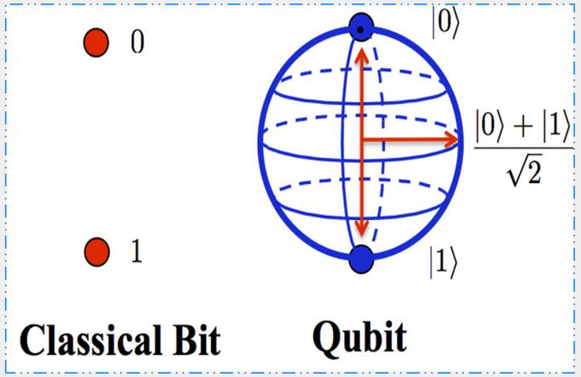
Le Tecnologie Quantistiche: Quantum Computing

I **qubit**, obbedendo alle leggi della **MQ**, sono in grado di **immagazzinare** e **processare molta più informazione** restituendo un **output** in formato digitale **estremamente preciso** con un **approccio probabilistico** anziché deterministico.

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

Pertanto, rispetto ai computer tradizionali, i **computer quantistici abilitano**:

- un **aumento** considerevole della **velocità** di calcolo;
- una maggiore **accuratezza** delle soluzioni;
- la possibilità di **risolvere** alcune **classi di problemi** che, richiedendo grande spazio computazionale e tempo di risoluzione non polinomiale, **non** possono essere **trattati** e **risolti** dalle **macchine classiche** (**ottimizzazioni**, **simulazioni**, **NP complexity problems**).



Sfide tecniche da risolvere:

- Instabilità qubit;
- rumore;
- errore quantistico;
- scalabilità

I **progressi** (in ambito Quantum Error Correction) nell'ultimo anno indicano che un **computer quantistico fault-tolerance** sarà disponibile entro i prossimi **5-7 anni**

Problema sicurezza delle informazioni

Le Tecnologie Quantistiche e Cybersecurity

I recenti progressi tecnologici suggeriscono che un **Computer Quantistico** fault-tolerant e **operativo** sarà disponibile entro i prossimi anni.
L'introduzione imminente di tale dispositivo avrà **implicazioni significative** per la **sicurezza** delle **informazioni**.

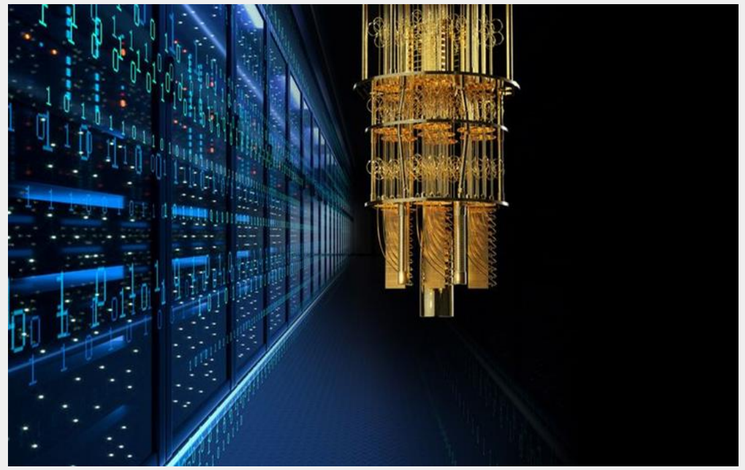
L'**algoritmo di Shor**, sviluppato nel 1994, ha infatti **dimostrato** che le **capacità dirompenti** di un **Computer Quantistico** rendono **vulnerabili** tutti i **sistemi crittografici** la cui sicurezza si basa sulla **potenza computazionale.**

In tali sistemi gli **algoritmi di codifica** utilizzano funzioni **one-way** in cui:

- **encryption** coincide con l'applicazione di una **funzione semplice** da calcolare;
- operazione di **decodifica**, corrisponde a una **funzione estremamente complessa**, la cui esecuzione richiederebbe a una **macchina classica** tempi **estremamente lunghi** (esponenziali).

La "**Minaccia Quantistica**" incombe su **tutti** i **protocolli** con **sicurezza computazionale** come l'**RSA**, i sistemi Discrete Logarithm Problem (**DLP**) e quelli che utilizzano **curve ellittiche**.

Quantum Communication



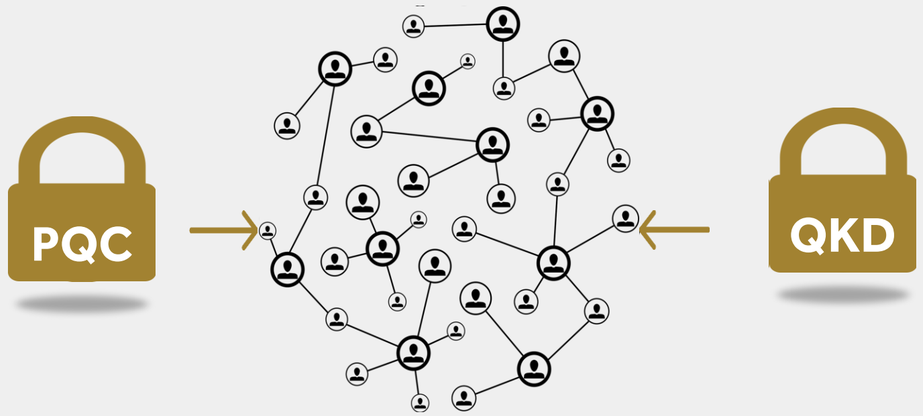
Tecnologie Quantistiche: Quantum Communication

Campo dell'Informatica Quantistica che si occupa della **trasmissione sicura** di **informazioni** e di sviluppare **sistemi resistenti** agli attacchi di potenziali computer quantistici.

Ad oggi, le principali contromisure alla "**Quantum Threat**" sono:

Post-Quantum Cryptography (PQC): area della Crittografia che sviluppa **algoritmi crittografici classici Quantum-Safe** usando problemi computazionali che, finora, sembrano essere resistenti agli attacchi di un computer quantistico.

Limiti: complessità computazionale degli algoritmi PQC, difficoltà passaggio Crittografia attuale a quella PostQuantistica, mancanza Standardizzazione.



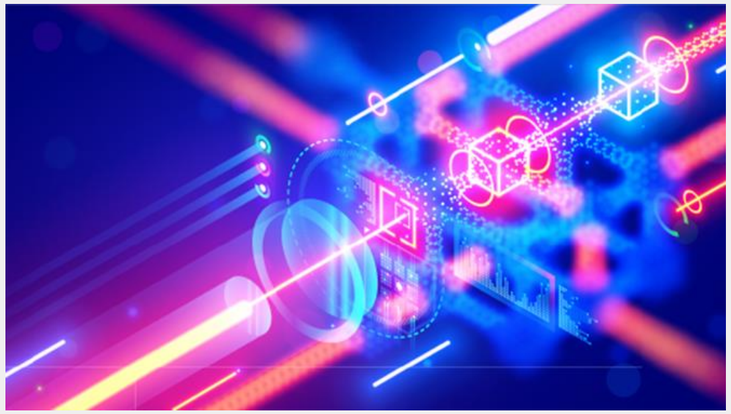
Quantum Key Distribution (QKD): tecnologia che permette a due utenti trusted, "Alice e Bob", di **scambiare** una **chiave crittografica segreta**, la cui **sicurezza** è **unconditional** (garantita dalle leggi di natura). Permette di **stabilire** con **assoluta certezza** la presenza di **eventuali tentativi di intercettazione**.

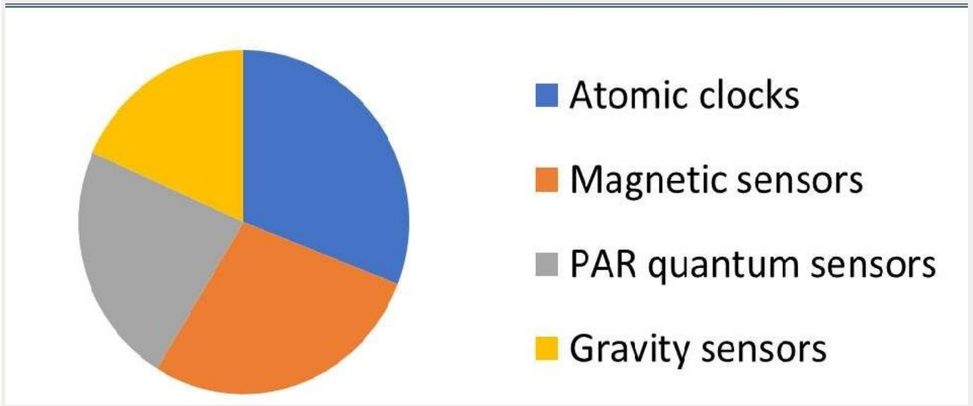
Limiti: Sfide tecniche, distanza raggiungibile, non esistenza di Quantum Repeaters

Tecnologie Quantistiche: Quantum Sensing and Metrology

Area più **sviluppata** delle **Tecnologie Quantistiche** la cui **maturità tecnologica** è prevista nei prossimi **3-5 anni**.

Sfruttando alcuni principi alla base delle **Fisica Quantistica** è possibile realizzare **sensori quantistici** in grado di **misurare** varie grandezze fisiche **con estrema accuratezza**.

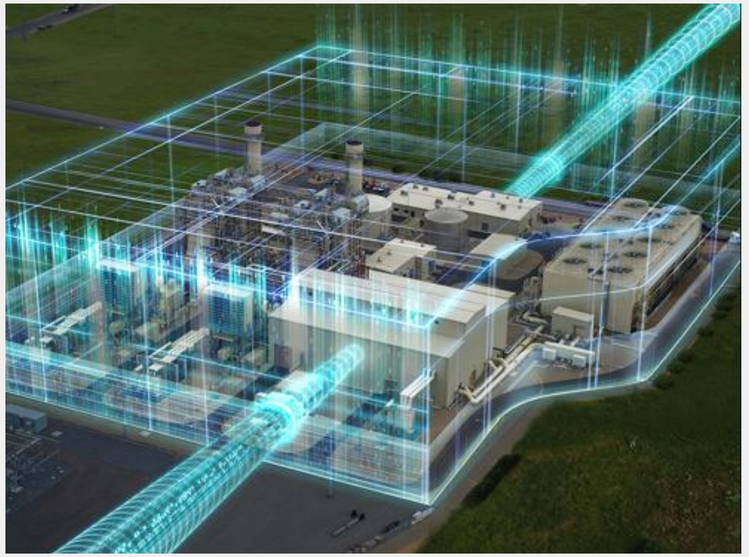




Global quantum sensors market

Significant Advantages:

- misure **più precise**;
- **detection** di segnali **molto deboli**;
- possibilità di **superare** i **limiti** imposti dalla **Fisica Classica**.

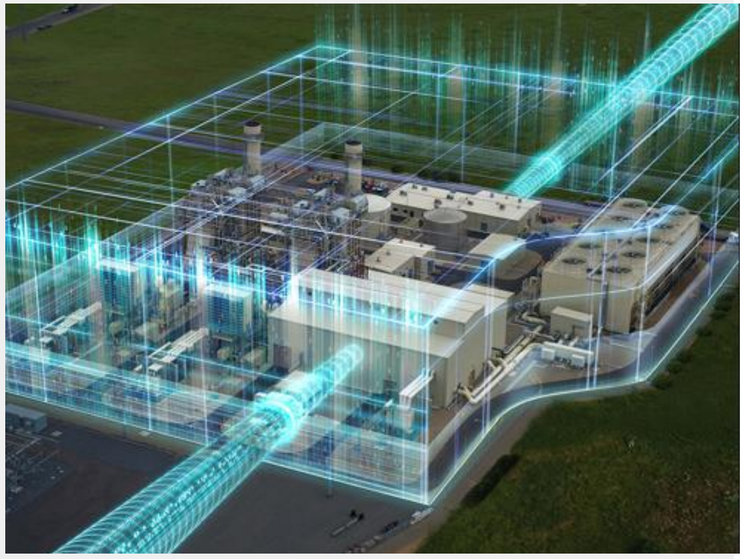


Tecnologie Quantistiche: Quantum Sensing and Metrology

A differenza dei sensori classici, i **sensori quantistici** riescono ad individuare **fluttuazioni puntuali** della grandezza misurata.

Questa **capacità dirompente** offre nuove opportunità in grado di trasformare radicalmente:

- le **scale spaziali**;
- la **persistenza** e la **diversità** delle **caratteristiche** del **monitoraggio** dell'ambiente analizzato, rendendoli **promettenti** per una vasta gamma di **applicazioni** in diversi **segmenti industriali** (**Difesa**, **Spazio**, **Automotive**, **Finance**, **Energia**, settore **Medico**, …);
- permette di raggiungere una **situational awareness** senza precedenti.

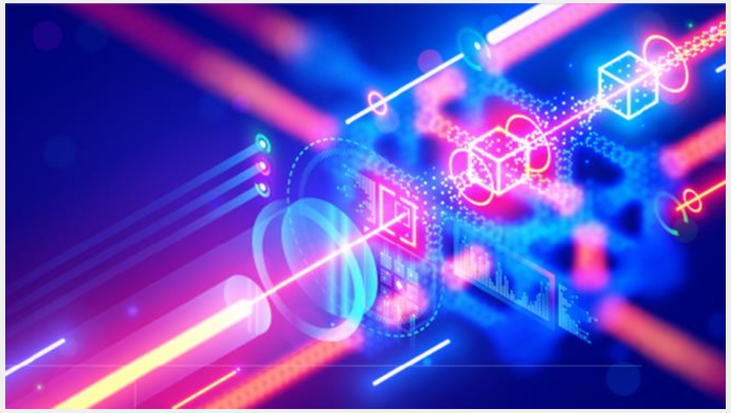


Tuttavia, pur rappresentando **l'area più consolidata** delle Tecnologie Quantistiche, quella con **TRL più alto**, il **Quantum Sensing**:

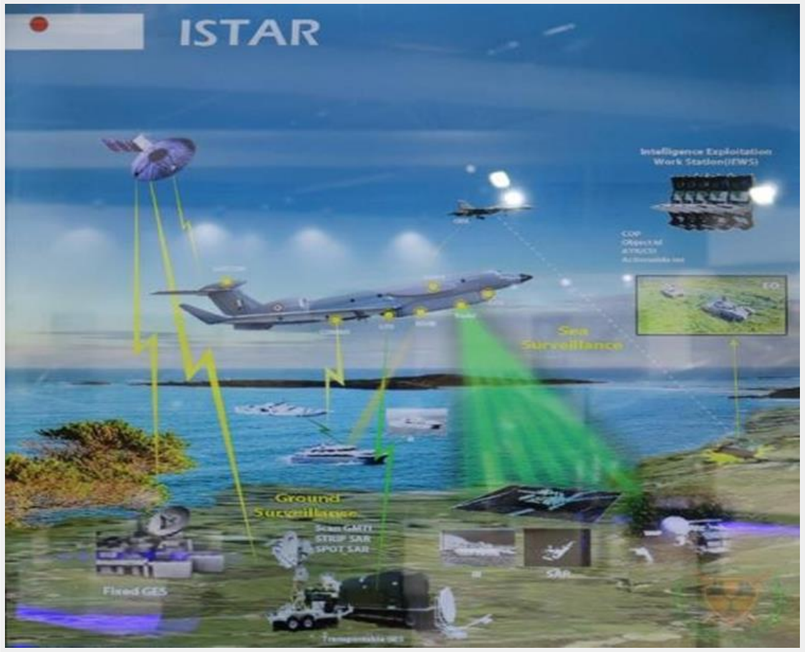
- resta attualmente il **settore meno noto** delle **QT**;
- **sviluppo pratico** è stato **fortemente condizionato** da alcuni **limiti sperimentali** dovuti principalmente alla difficoltà di **interagire** con i singoli sistemi quantistici, **isolandoli** dall'ambiente circostante. ➡ Ciò ha **relegato** tali dispositivi all'interno dei **laboratori**

Quantum Sensing e Mondo Reale

2023: i **progressi tecnici** raggiunti hanno permesso di **sperimentare** i **sensori quantistici** nel **mondo reale**: **posizionamento** dei sensori quantistici su **veicoli** di **terra/mare/aria** , su **droni**, su **satelliti** a bassa orbita (**LEO**).

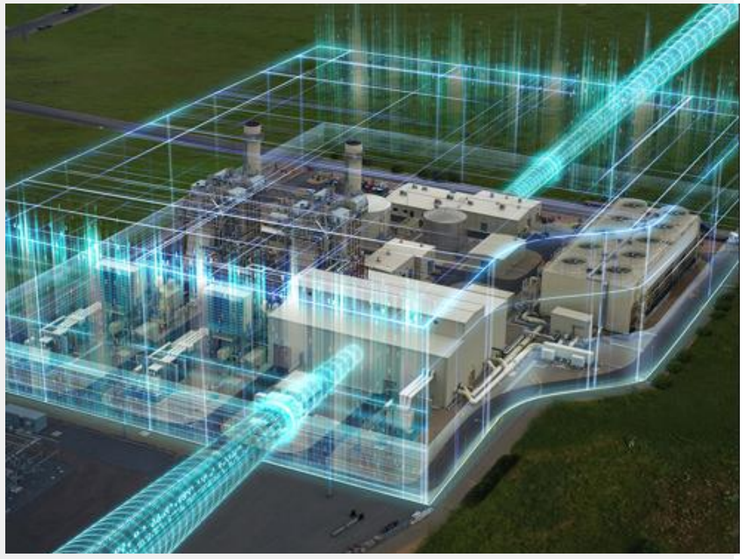


I **risultati empirici** hanno dimostrato la **netta superiorità** di quest'ultimi sulla controparte classica, ottenendo **misure ordini** di **grandezza più precise**.



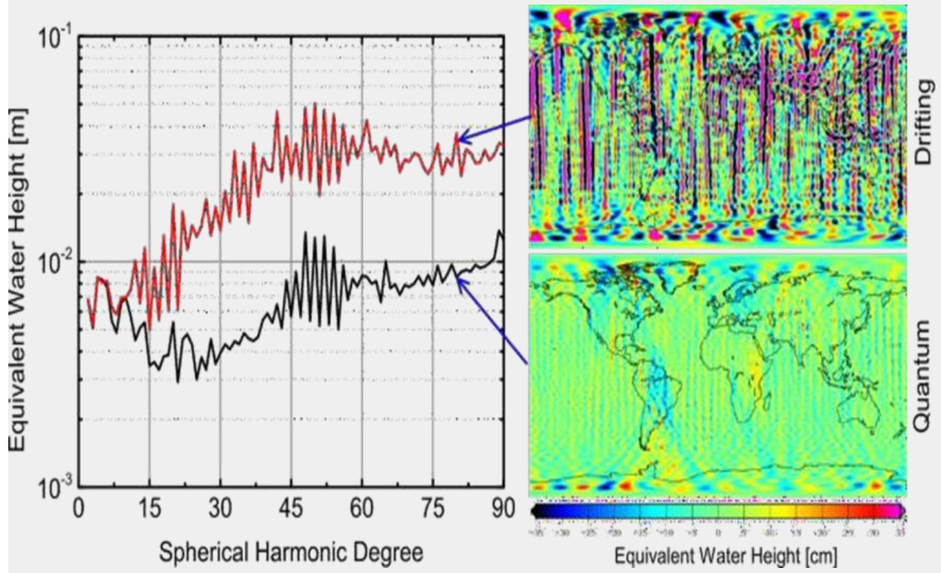
Difesa: recenti pubblicazioni hanno **dimostrato** come l'utilizzo dei **sensori quantistici** sia in grado di **rivoluzionare** la **sorveglianza** e il **monitoraggio**:

- superficie terrestre;
- sottosuolo;
- dominio underwater.



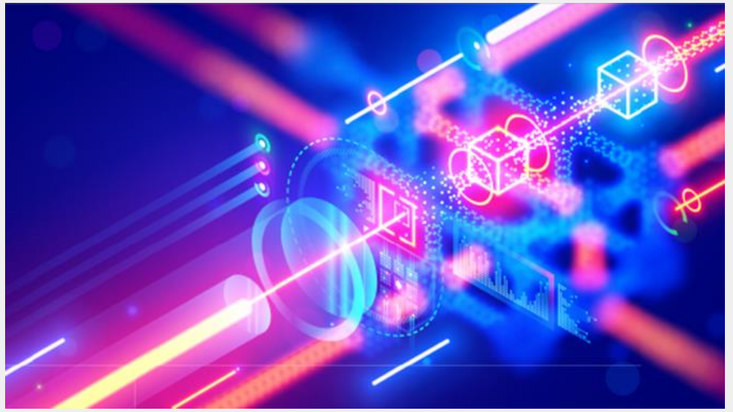
Quantum Sensing e Mondo Reale

Confronto delle **variazioni sperimentali** del **campo gravitazionale terrestre** misurate nelle **medesime condizioni** con un **Gravimetro Quantistico** (basso) e con un **Gravimetro Classico** (alto).



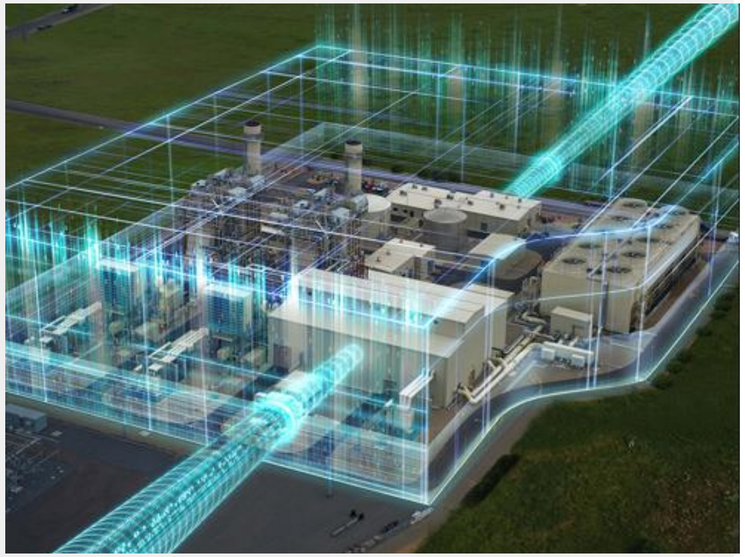
Sinistra: confronto fra il rumore del sensore quantistico (nero) e di quello classico (rosso).

Destra: confronto delle variazioni sperimentali del campo gravitazionale terrestre misurate da satellite con un Gravimetro Quantistico (basso) e con un Gravimetro Classico (alto)



Risultati:

- il **sensore quantistico** è in grado di **rilevare fluttuazioni gravitazionali locali** estremamente più **piccole**
- il **rumore** nel caso **quantistico** (curva nera grafico a sinistra) è **fortemente soppresso** rispetto al caso classico (curva rossa).



Quantum Lidar: Risultati Sperimentali

Esperimento condotto nella città di Shanghai che ha dimostrato come il **Quantum Lidar** sia in grado di Long range 3D imaging.

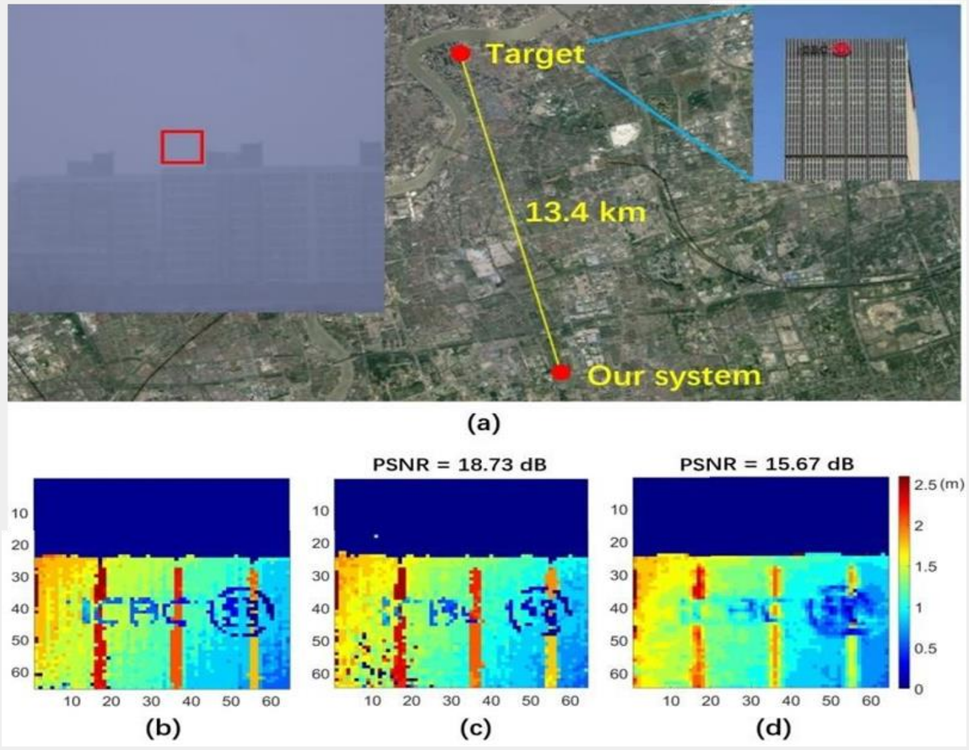


Immagine satellitare dell'esperimento con una visibilità minima di 4km.

- **Sinistra:** fotografia scattata durante l'esperimento in cui il rettangolo rosso indica la posizione del Quantum Lidar;
- **Destra:** foto dell'edificio bersaglio scattata nelle vicinanze

Immagine delle **lettere individuate** sullo **schermo** di un **computer** all'**interno** di una **stanza dell'edificio** situato a **oltre 13 km**.

Risultato:

- È stata dimostrata la capacità di **Quantum Lidar** di eseguire **imaging 3D ad alta risoluzione** nella **nebbia** a una **distanza superiore a 13 km** con una **visibilità minima di 4 km**

Quantum Ket

Thank You

Contact us to learn more

Quantum Ket
Rome, Italy
www.qket.it
info@qket.it