

immagine: generata con intelligenza artificiale e rielaborata da Antonio Morlupi

GIUSEPPE CALABRÒ

PROF. UNIVERSITÀ DEGLI STUDI DELLA TUSCIA

ENERGIA E CALCOLO AVANZATO

Progettare le infrastrutture digitali per la sicurezza nazionale

AI, HPC e quantum computing impongono una nuova idea di infrastruttura critica. Serve un'architettura strategica che integri energia, calcolo e cyber. L'Italia deve potenziare le proprie infrastrutture di calcolo avanzato per garantire competitività, sicurezza e sovranità tecnologica

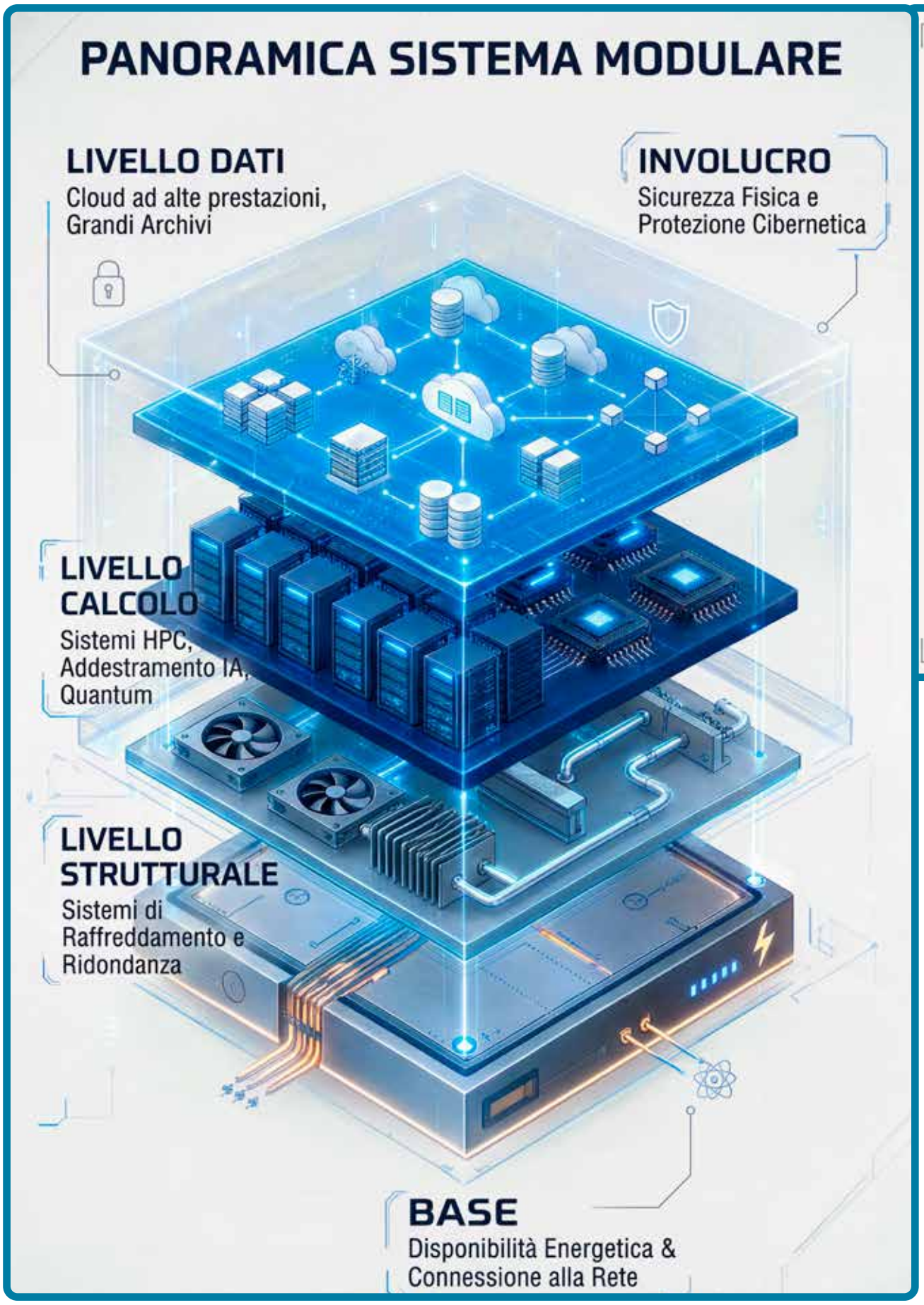


La diffusione dell'intelligenza artificiale, del calcolo ad alte prestazioni (High Performance Computing, HPC) e delle future applicazioni di quantum computing sta trasformando profondamente il concetto di infrastruttura critica. La crescente domanda di energia associata alle nuove tecnologie digitali rende sempre più evidente la necessità di progettare infrastrutture nelle quali produzione energetica, capacità di calcolo, gestione dei dati e cybersicurezza costituiscano elementi di un'unica architettura strategica. L'Italia dispone oggi di importanti competenze scientifiche e industriali in questi settori, ma il nuovo scenario internazionale suggerisce una riflessione sulla necessità di sviluppare infrastrutture nazionali di calcolo avanzato capaci di sostenere la competitività, la sicurezza e la sovranità tecnologica del Paese.

Negli ultimi anni il rapporto tra energia e capacità computazionale è cambiato profondamente. Se fino a poco tempo fa il principale fattore competitivo era rappresentato dalla disponibilità di sistemi di calcolo sempre più potenti, oggi emerge con chiarezza un nuovo elemento: la disponibilità di energia.

L'intelligenza artificiale generativa, i modelli fondazionali, il calcolo ad alte prestazioni, i servizi cloud e, in prospettiva, il quantum computing stanno determinando una crescita senza precedenti della domanda energetica delle infrastrutture digitali. La conseguenza è un cambiamento di paradigma: il limite allo sviluppo non è più rappresentato esclusivamente dalla capacità di progettare nuovi processori, ma dalla possibilità di alimentare infrastrutture sempre più energivore garantendo continuità di esercizio, resilienza e sicurezza.

Questa trasformazione non riguarda soltanto la competitività economica. La disponibilità di infrastrutture nazionali di calcolo avanzato rappresenta oggi una capacità abilitante per numerose funzioni strategiche dello Stato: dalla ricerca scientifica alla sanità,


PANORAMICA SISTEMA MODULARE
LIVELLO DATI
Cloud ad alte prestazioni, Grandi Archivi
INVOLUCRO
Sicurezza Fisica e Protezione Cibernetica
LIVELLO CALCOLO
Sistemi HPC, Addestramento IA, Quantum
LIVELLO STRUTTURALE
Sistemi di Raffreddamento e Ridondanza
BASE
Disponibilità Energetica & Connessione alla Rete



dalla protezione civile alla cybersicurezza, fino ai sistemi di comando e controllo e alle capacità decisionali della Difesa. La resilienza delle infrastrutture digitali diventa quindi un elemento essenziale della sicurezza nazionale.

L'Italia dispone oggi di competenze di assoluto rilievo nel settore del supercalcolo e della ricerca scientifica avanzata. Università, enti di ricerca e industria hanno contribuito negli ultimi anni allo sviluppo di infrastrutture che collocano il Paese tra i protagonisti europei del calcolo ad alte prestazioni. Tuttavia, il rapido sviluppo dell'intelligenza artificiale e delle nuove applicazioni digitali rende evidente che le infrastrutture esistenti, per quanto avanzate, dovranno essere progressivamente affiancate da una nuova generazione di piattaforme nazionali, concepite per rispondere a esigenze molto più ampie rispetto al solo supercalcolo.

Le future infrastrutture nazionali di calcolo non potranno infatti essere considerate semplicemente come supercomputer di dimensioni maggiori. Esse dovranno integrare capacità di addestramento e inferenza dei modelli di intelligenza artificiale, sistemi HPC, cloud ad alte prestazioni, grandi archivi di dati, piattaforme di cybersicurezza, servizi digitali strategici e, progressivamente, tecnologie quantistiche. Si tratta di un ecosistema complesso nel quale differenti componenti dovranno condividere reti di comunicazione, sistemi di raffreddamento, continuità operativa, capacità di archiviazione e disponibilità energetica.

La vera sfida non consiste quindi soltanto nell'acquisizione di hardware sempre più performante, ma nella progettazione dell'intera infrastruttura che ne rende possibile il funzionamento. Disponibilità di energia, connessione alla rete elettrica, sistemi di raffreddamento, sicurezza fisica, protezione cibernetica, ridondanza e continuità operativa diventano elementi inseparabili di un'unica architettura nazionale.

Questa evoluzione richiede anche un cambiamento culturale nel modo di progettare le infrastrutture strategiche. Per molti anni la sicurezza è stata affrontata prevalentemente come un'attività successiva alla realizzazione



delle opere, intervenendo per mitigare vulnerabilità emerse nel tempo. Le infrastrutture digitali critiche del futuro richiedono invece un approccio opposto: la sicurezza deve diventare un requisito progettuale originario, non una correzione successiva. In altre parole, occorre passare da una logica di Security by Reaction a una di Security by Design, nella quale resilienza energetica, protezione cibernetica, sicurezza fisica, continuità operativa e affidabilità siano concepite come caratteristiche intrinseche dell'infrastruttura e non come elementi aggiunti in una fase successiva.

Per molti anni la sovranità tecnologica è stata associata principalmente alla capacità di

Pianificare congiuntamente produzione energetica, capacità computazionale e sviluppo industriale, riconoscendo come tali elementi costituiscano ormai componenti di un'unica infrastruttura nazionale

sviluppare algoritmi, software e microprocessori. Oggi questa definizione appare incompleta. La crescente domanda di energia da parte delle infrastrutture digitali suggerisce che la sovranità tecnologica dipenderà sempre più dalla capacità di progettare ecosistemi nazionali nei quali produzione energetica, reti elettriche, capacità di calcolo, gestione dei dati e cybersicurezza siano sviluppati in maniera coordinata. In questa prospettiva, l'infrastruttura diventa essa stessa un elemento di sovranità.

A livello internazionale questa trasformazione è già evidente. I principali investimenti nelle infrastrutture digitali sono sempre più accompagnati da strategie dedicate all'approvvigionamento energetico, nella consapevolezza che la capacità di calcolo dipende ormai dalla disponibilità di energia continua e programmabile. Il vero collo di bottiglia rischia quindi di non essere più il processore, ma l'infrastruttura energetica necessaria a sostenerne il funzionamento.

In questo scenario assume particolare rilevanza il dibattito sulle possibili soluzioni energetiche. Le fonti rinnovabili rappresentano una componente imprescindibile della transizione energetica, ma la loro natura non programmabile rende necessario valutare sistemi complementari in grado di garantire continuità di produzione, stabilità della rete e resilienza delle infrastrutture critiche. Tra le tecnologie oggi oggetto di crescente interesse figurano gli Small Modular Reactors (SMR) e gli Advanced Modular Reactors (AMR), progettati per offrire elevati standard di sicurezza, modularità costruttiva e una maggiore flessibilità di integrazione con grandi infrastrutture industriali e digitali. Il loro eventuale impiego dovrà naturalmente essere valutato nell'ambito di un mix energetico equilibrato, capace di coniugare sostenibilità ambientale, sicurezza degli approvvigionamenti e competitività industriale. In questa direzione si collocano anche alcune iniziative internazionali che stanno sperimentando un approccio integrato tra energia e infrastrutture digitali. Un esempio significativo è rappresentato dal Trent Supercluster nel Regno Unito, un programma di rigenerazione industriale che punta a trasformare un'area storicamente legata alla produzione energetica in un polo dedicato alle tecnologie pulite, alla fusione, all'idrogeno, all'innovazione nucleare e alle infrastrutture digitali ad alta intensità di calcolo. Più che il singolo progetto, è l'approccio ad assumere rilievo strategico: pianificare congiuntamente produzione energetica, capacità computazionale e sviluppo industriale, riconoscendo come tali elementi costituiscano ormai componenti di un'unica infrastruttura nazionale.

La questione, tuttavia, non riguarda esclusivamente la scelta della fonte energetica. Il punto centrale consiste nella capacità di pianificare infrastrutture nazionali nelle quali energia, calcolo avanzato, gestione dei dati, cybersicurezza e comunicazioni siano progettati come elementi di un'unica strategia. La disponibilità di una moderna infrastruttura nazionale di calcolo avanzato rappresenta molto più di un investimento tecnologico: costituisce una componente essenziale della competitività industriale, della capacità scientifica e della sicurezza nazionale.

Per il settore della Difesa questa evoluzione assume un valore ancora più rilevante. Le future capacità operative dipenderanno sempre più dall'intelligenza artificiale, dalle simulazioni numeriche, dall'analisi di grandi moli di dati, dai sistemi autonomi, dalla cybersicurezza e da processi decisionali supportati dal calcolo avanzato. Disporre di infrastrutture nazionali resilienti significa quindi rafforzare non soltanto la capacità tecnologica del Paese, ma anche la sua autonomia strategica nei settori più sensibili. L'Italia possiede le competenze scientifiche, industriali e tecnologiche per partecipare da protagonista a questa trasformazione. La sfida consiste ora nel tradurre tale patrimonio in una visione di lungo periodo, capace di integrare politiche energetiche, infrastrutture digitali, sicurezza e strategie industriali fin dalla fase di progettazione. Se nel secolo scorso autostrade, porti e reti elettriche hanno rappresentato le infrastrutture abilitative dello sviluppo economico, nel XXI secolo saranno le infrastrutture nazionali di calcolo avanzato, sostenute da sistemi energetici resilienti e progettate secondo i principi della Security by Design, a costituire uno dei principali pilastri della competitività, della sicurezza e della sovranità tecnologica dell'Italia.