L'IA è fondamentale per migliorare la resilienza delle infrastrutture critiche

Intervista con Franco Federici, Consigliere Militare del Presidente del Consiglio dei Ministri

Franco Federici, è il Consigliere Militare del Presidente del Consiglio dei ministri e, in tale incarico, è responsabile selle segreteria infrastrutture critiche. Generale di Corpo d'Armata (alpino) dell'Esercito, ha frequentato il 166° Corso presso l'Accademia Militare di Modena e, nel corso della sua carriera, ha partecipato a diverse Operazioni, come la "Joint Guard" in Bosnia Erzegovina e NATO ISAF in Afghanistan. Ha comandato la Brigata "Taurinense" e, in tale veste, ha comandato il settore ovest della missione Unifil in Libano. È anche stato capo del Reparto Operazioni dello Stato Maggiore dell'Esercito e Capo Reparto Operazioni e Supporto Operativo del Comando operativo di vertice interforze. Nel 2020 ha assunto il Comando NATO della KOSOVO Force.

A lui abbiamo chiesto quali sono le principali minacce che l'Italia deve affrontare nella protezione delle infrastrutture critiche?

La protezione e la resilienza delle infrastrutture critiche non sono tematiche recenti: il dibattito ha avuto origine alla fine degli anni '90, con l'aumento dell'integrazione tra diversi settori e l'evoluzione delle tecnologie digitali, che da strumenti di supporto sono diventate elementi centrali nella gestione di queste infrastrutture, aumentando, al contempo, i rischi legati alla cybersicurezza, alle interdipendenze tra settori e agli effetti a cascata. Le principali minacce che l'Italia si trova ad affrontare si possono riassumere in tre macro-categorie:

1. Interdipendenze e vulnerabilità sistemiche. L'interconnessione crescente tra le infrastrutture ha introdotto fenomeni di dipendenza reciproca che possono amplificare l'impatto di un incidente. Un guasto o un attacco in un settore – ad esempio, l'energia o le telecomunicazioni – può propagarsi rapidamente, compromettendo l'operatività di altri servizi essenziali. Un esempio concreto si è verificato il 28 novembre 2023, quando un danno alla rete del gas in Svizzera ha interrotto cavi in fibra ottica, bloccando in Italia i pagamenti elettronici e causando un impatto economico stimato intorno al miliardo di euro.
2. Cambiamento climatico e eventi estremi. L'aumento della frequenza e dell'intensità di fenomeni meteorologici avversi – ondate di calore, alluvioni, tempeste – mette sotto pressione le reti energetiche, idriche e di trasporto, aumentando il rischio di blackout, interruzioni dei servizi e danni strutturali.
3. Minacce dolose e cyber-attacchi - Le infrastrutture critiche sono bersaglio di attacchi dolosi, inclusi atti terroristici, sabotaggi e cyber-attacchi. La crescente esposizione dell'Italia sulla scena internazionale nei prossimi mesi accresce ulteriormente il rischio. Il governo ha già adottato misure per la protezione del cyber-spazio con l'implementazione del Perimetro di sicurezza cibernetica nazionale e l'istituzione dell'Agenzia per la Cybersicurezza Nazionale (ACN).

> "Aumentano i rischi legati alla cybersicurezza"

A queste si aggiungono le minacce ibride, come ad esempio campagne di disinformazione e azioni di sabotaggio che rimangono al di sotto della soglia di un attacco armato.

In che modo la tecnologia può essere utilizzata per migliorare la resilienza delle infrastrutture critiche italiane?

La tecnologia gioca un ruolo essenziale nel rafforzare la sicurezza e la resilienza delle infrastrutture critiche nazionali, permettendo un miglioramento significativo delle capacità di monitoraggio, rilevamento delle minacce (detection) ed early warning. L'adozione di sistemi Internet of Things avanzati, combinati con l'impiego di droni e impianti di videosorveglianza intelligenti, consente un controllo più capillare e tempestivo degli asset strategici. L'IoT infatti consente il monitoraggio in tempo reale delle condizioni delle infrastrutture, consentendo una rapida identificazione e risposta alle anomalie.
Inoltre, per gestire l'enorme quantità di dati generata da questi sistemi, è fondamentale l'impiego dell'Intelligenza Artificiale, che permette di filtrare le informazioni rilevanti, identificare anomalie e segnalare in tempo reale situazioni potenzialmente critiche, riducendo i tempi di risposta. Inoltre, l'IA può essere utilizzata per automatizzare l'analisi dei dati e migliorare il processo decisionale.
Una volta identificata una minaccia, la tecnologia deve supportare non solo la fase di contrasto, ma soprattutto quella di gestione dell'evento avverso, garantendo un coordinamento efficace tra i diversi attori coinvolti. Questo aspetto è cruciale per affrontare le problematiche legate alle interdipendenze tra settori e mitigare i possibili effetti a cascata.
In questo contesto, risultano particolarmente rilevanti le iniziative promosse da ENEA, che da oltre un decennio conduce studi sulle interdipendenze infrastrutturali. Un esempio significativo è CipCast, una piattaforma avanzata per la valutazione del rischio e la gestione ottimizzata degli scenari interdipendenti, che rappresenta uno strumento di grande interesse per il rafforzamento della resilienza delle infrastrutture critiche in Italia.

È possibile citare qualche esempio di come l'IA è stata implementata con successo nella protezione delle infrastrutture critiche?

Le infrastrutture critiche, come la rete elettrica e quella ferroviaria, si estendono per migliaia di chilometri sul territorio nazionale. Per garantirne il funzionamento e la sicurezza, gli operatori stanno progressivamente implementando reti di sensori in grado di raccogliere una grande quantità di dati relativi allo stato delle infrastrutture.
Questi dati, che affluiscono in tempo reale nelle sale di controllo, vengono già oggi analizzati con tecniche di Intelligenza Artificiale, che consentono di aggregare, filtrare e prioritizzare le informazioni in base alla loro rilevanza operativa. L'IA, inoltre, può integrare questi dati con quelli provenienti da altre fonti – come sensori ambientali o sistemi di monitoraggio esterni – per individuare potenziali situazioni di pericolo, sia accidentali che dolose, fornendo agli operatori un supporto decisionale più efficace.
Per fare un altro esempio, la distribuzione di energia in Italia sta utilizzando l'IA per migliorare la resilienza della rete. In particolare, si sta sviluppando un sistema basato su dati satellitari per prevedere e mitigare i rischi di alluvione. Sempre nel settore della distribuzione di energia si sta utilizzando l'IA per stimare la probabilità di malfunzionamenti e anticipare le esigenze di manutenzione.
Un esempio concreto di applicazione avanzata dell'IA riguarda la protezione dei cavi sottomarini, un'infrastruttura sempre più strategica nel contesto geopolitico globale, ma al tempo stesso altamente vulnerabile a causa della sua estensione e della molteplicità di soggetti coinvolti. In questo ambito, la Marina Militare, attraverso il Programma Nazionale di Ricerca Militare (PNRM), sta sviluppando il progetto IMPROVE, che sfrutta tecniche di Intelligenza Artificiale per analizzare dati provenienti da AIS (Automatic Identification System), radar e satelliti, creando un quadro operativo unificato in grado di individuare imbarcazioni che seguono rotte anomale o potenzialmente minacciose.
Parallelamente, a livello europeo, l'Ufficio del Consigliere militare sta seguendo da vicino il progetto VIGIMARE, che rappresenta un ulteriore sviluppo delle tecnologie IA applicate al monitoraggio marittimo. Questo progetto, operativo sia nel Baltico che nel Mediterraneo, mira a potenziare la capacità di sorveglianza e prevenzione, sfruttando modelli avanzati di analisi comportamentale delle imbarcazioni per identificare e contrastare attività sospette prima che possano rappresentare una minaccia concreta.

La IA oltre che risorsa per aumentare la resilienza delle infrastrutture critiche, può introdurre nuove minacce alla capacità di questi sistemi di erogare con continuità i loro servizi essenziali?

L'Intelligenza Artificiale rappresenta uno strumento potente, destinato a migliorare significativamente non solo la resilienza delle infrastrutture critiche, ma anche molteplici aspetti della vita quotidiana. Tuttavia, come ogni tecnologia avanzata, introduce anche nuove vulnerabilità che devono essere identificate, monitorate e gestite per garantire la continuità operativa dei servizi essenziali.

"L'IA è uno strumento potente, ma introduce anche nuove vulnerabilità"

Uno dei rischi più rilevanti, oggi al centro del dibattito pubblico, riguarda la dipendenza tecnologica dell'Europa da altri attori globali. Il timore di una perdita di sovranità tecnologica a favore di competitor internazionali è una questione strategica che l'Unione Europea sta cercando di affrontare. In questa direzione va il piano da 200 miliardi di euro annunciato dal presidente Von der Leyen al recente vertice sull'IA a Parigi, un'iniziativa volta a rafforzare la competitività e l'indipendenza europea in questo settore chiave.
Dal punto di vista tecnico, l'IA – come qualsiasi software complesso – è soggetta a bug e vulnerabilità che potrebbero essere sfruttati da attori ostili per indurre comportamenti anomali nei sistemi, con potenziali impatti sulla sicurezza e sulla continuità dei servizi. Il rischio di manipolazione dei modelli di IA attraverso attacchi mirati, come l'adversarial AI, è una minaccia concreta che richiede strategie di mitigazione efficaci.
Infine, l'implementazione diffusa dell'IA porterà a un'integrazione sempre più stretta tra sistemi e infrastrutture, con effetti sia positivi che problematici. Da un lato, ciò consentirà una gestione più efficiente e reattiva; dall'altro, potrebbe aumentare la complessità sistemica, rendendo le infrastrutture più vulnerabili a effetti a cascata, in cui un malfunzionamento o un attacco in un punto della rete potrebbe propagarsi rapidamente, compromettendo interi settori strategici.
Occorre inoltre essere consapevoli che oggi l'IA ha alcuni limiti che possono renderla uno strumento non sempre idoneo per sostenere la resilienza delle infrastrutture critiche: consuma troppa energia; non è pronta per studiare sistemi complessi e le dinamiche complessive di correlazione non sono sempre comprese bene; non esiste un meccanismo per capire le correlazioni causa effetto generate dall'IA. Vi è infine il limite degli aggiornamenti il quale risiede nel fatto che, pur migliorando continuamente grazie ai nuovi dati e alle ottimizzazioni degli algoritmi, ogni aggiornamento può introdurre nuove vulnerabilità o comportamenti imprevisti.
Affrontare queste sfide richiede un approccio bilanciato, che sappia sfruttare le potenzialità dell'IA senza trascurarne i rischi, attraverso investimenti mirati, regolamentazioni efficaci e una solida strategia di cybersecurity.

Come vede il futuro della collaborazione tra settore pubblico e privato nella protezione delle infrastrutture critiche?

È fondamentale instaurare una collaborazione efficace tra il settore pubblico e quello privato. Le aziende che gestiscono infrastrutture critiche giocano un ruolo cruciale nella protezione e nella resilienza delle proprie infrastrutture. Il governo, dal canto suo, deve fornire il quadro normativo e il supporto necessario per facilitare questa collaborazione. Un quadro normativo chiaro e la creazione di partnership pubblico-privato sono strumenti importanti per definire ruoli, responsabilità e meccanismi di collaborazione. In quest'ottica, l decreto legislativo del 4 settembre 2024, n. 134, sottolinea l'importanza della collaborazione tra settore pubblico e privato nella protezione delle infrastrutture critiche. Nel decreto, la collaborazione pubblico privata è stata realizzata attraverso varie disposizioni che mirano a favorire il dialogo, la cooperazione e lo scambio di informazioni tra soggetti pubblici e privati.

"È fondamentale una collaborazione efficace tra il settore pubblico e quello privato"

È stata istituita la Conferenza per la Resilienza dei Soggetti Critici composta da un rappresentante per ciascuna delle Autorità settoriali competenti, un rappresentante del Ministero dell'interno, uno del Ministero della difesa e uno del Dipartimento della Protezione civile, e per le questioni di cybersicurezza, un rappresentante

dell'Agenzia per la cybersicurezza nazionale. Alla conferenza potranno partecipare i soggetti critici appartenenti ai settori di volta in volta oggetto della discussione, nonché soggetti pubblici e privati invitati dal Punto di Contatto Unico in base all'oggetto della conferenza.
La condivisione delle informazioni sulle minacce, le vulnerabilità e gli incidenti sono fondamentali per la resilienza delle infrastrutture critiche. Il settore pubblico può fornire dati di intelligence, mentre il settore privato può contribuire con la conoscenza dei propri sistemi e delle proprie esperienze.

Inoltre, programmi di formazione congiunti ed esercitazioni pratiche permettono di preparare gli operatori e testare la risposta agli incidenti, migliorando il coordinamento tra pubblico e privato. Anche l'esercizio di effettuare stress test sulle infrastrutture critiche può essere visto in quest'ottica. Infine, a ricerca e l'innovazione tecnologica rappresentano un terreno fertile per tale collaborazione: sviluppare nuove tecnologie condivise può consentire di migliorare la protezione delle infrastrutture critiche.