PRIMO PIANO Il Sole 24 Ore 07 MAGGIO 2024

Sicurezza: 5 miliardi per proteggere le reti elettriche e gas

Infrastrutture. In campo piani mirati di Snam e Terna per rafforzare gli asset fisici ma anche per contrastare possibili attacchi informatici

Celestina Dominelli

ROMA

Dai compensatori sincroni disposti lungo la rete elettrica per ridurre al minimo gli sbalzi di tensione ai droni utilizzati per ispezionare i tratti dell'infrastruttura nazionale del gas situati in luoghi impervi o impraticabili, passando per i sistemi di geolocalizzazione che individuano le perdite in tempo reale. Sono tante le misure messe in campo da Snam e Terna per assicurare il consolidamento e la sicurezza delle proprie reti soggette, da un lato, agli impatti derivanti da eventi meteorologici estremi , e, sottoposte, dall'altro, sia alle minacce legate a possibili attacchi informatici sia a riverberi derivanti dal moltiplicarsi dei conflitti.

Ecco perché, nei piani dei due gruppi, il capitolo sulla sicurezza delle infrastrutture ha un peso rilevante e comporta uno sforzo superiore ai 5,2 miliardi di euro. La voce più consistente è rappresentata dagli interventi sugli asset fisici, che spaziano dalle opere di rinnovamento infrastrutturale alle attività di prevenzione e mitigazione dei rischi.

Sul fronte gas, Snam ha previsto un impegno di oltre 2 miliardi di euro, nell'ambito del proprio piano strategico 2023-2027, per iniziative di rafforzamento del sistema di trasporto nazionale, tra cui figurano il rifacimento del metanodotto Ravenna-Chieti, con

fine lavori fissata entro il 2026, e numerosi altre interventi di potenziamento infrastrutturale legati ai metanodotti San Salvo-Bicari, Recanati-Foligno, Foligno-Gallese, Sansepolcro-Terranuova e Alessandria-Torino. In particolare, il rifacimento del Ravenna-Chieti prevede la costruzione di un nuovo gasdotto al posto dell'esistente, la realizzazione di linee secondarie la dismissione di circa 337 chilometri di tubazione. Nel complesso, sono oltre 900 chilometri di rete interessati da questi lavori.

Sul versante elettrico, Terna punta su due leve. La prima è il piano sicurezza da 1,7 miliardi di investimenti, inserito nell'ultimo piano industriale e nel quale è prevista l'implementazione di nuove soluzioni tecnologiche, come i compensatori, per un esercizio sicuro e stabile del sistema, l'adozione di soluzioni digitali per garantire maggiore affidabilità e flessibilità della rete, nonché interventi per incrementare la resilienza. E, proprio a quest'ultimo aspetto, è dedicato il piano ad hoc, allegato al piano Sicurezza, con oltre un miliardo di euro di investimenti, che il gruppo predispone annualmente per poi sottoporlo al via libera del ministero dell'Ambiente e della Sicurezza energetica.

L'altra gamba degli interventi è rappresentata dagli investimenti in sicurezza cibernetica e innovazione tecnologica che, in casa Snam, valgono circa 550 milioni di investimenti. Con il gruppo impegnato, da un lato, nella costruzione di un vero e proprio ecosistema digitale della sicurezza, attraverso l'adozione di un modello di cybersecurity basato su logiche di sistema e di integrazione, e, dall'altro, nel ricorso diffuso a una serie di strumenti (dall'Internet delle cose alla telediagnostica, dai satelliti alle tecnologie di ricerca delle perdite) per assicurare il controllo continuativo, sul campo e da remoto, dello stato di salute della rete di trasporto del gas. A questo si affianca, poi, la nuova Asset Control Room, pienamente operativa da quest'anno e finalizzata al monitoraggio e alla gestione integrata, tempestiva ed efficiente, degli asset e delle attività del gruppo.

Una sorta di "cervellone" che caratterizza anche l'approccio di Terna. Il gruppo - che ha previsto nel complesso circa 2 miliardi di investimenti in digitalizzazione, cyber security e innovazione, non legati però solo alla sicurezza - ha infatti creato un struttura nevralgica-operativa (il Computer Emergency Readiness Team) che assicura il controllo in tempo reale della sicurezza del gruppo e delle sue piattaforme nonché il monitoraggio preventivo e reattivo di tutte le potenziali minacce cyber. Tra i fattori abilitanti, c'è poi l'impegno a una costante collaborazione con enti istituzionali, università e associazioni e stakeholder esterni, per sviluppare ulteriormente questo filone. Senza contare, infine, una specifica convenzione bilaterale proprio con Snam per lo scambio di informazioni nell'ambito della protezione delle reti digitali delle infrastrutture energetiche.