Contromisure per il dominio spaziale

- **Cybersecurity "On-Board" e IA predittiva:** Installazione di micro-firewall e sistemi di rilevamento delle intrusioni (IDS) direttamente a bordo dei satelliti. Algoritmi di Intelligenza Artificiale leggeri analizzano il traffico di dati in orbita e bloccano autonomamente comandi anomali senza attendere l'input da terra.
- **Distribuzione Quantistica delle Chiavi (QKD) via satellite:** utilizzo della tecnologia Quantum Key Distribution per scambiare chiavi di cifratura tra terra e spazio tramite fotoni. Se un hacker tenta di intercettare il segnale laser, le leggi della fisica quantistica alterano lo stato dei fotoni, svelando immediatamente l'intrusione e annullando la chiave.
- **Architetture a costellazione resiliente (Megacostellazioni LEO)**: passaggio da singoli satelliti enormi e costosi a reti di migliaia di piccoli satelliti (come fatto da Starlink). Se un attacco cyber o un'azione di disturbo (jamming) ne disabilita dieci, la rete si riconfigura automaticamente deviano il traffico sugli altri nodi, annullando l'impatto del sabotaggio.
- **Gemelli Digitali (Digital Twins) per il patching sicuro:** creazione di repliche virtuali esatte del satellite a terra. Prima di inviare un aggiornamento software o una patch di sicurezza nello spazio (operazione ad altissimo rischio), questa viene testata e "attaccata" nel gemello digitale per escludere malfunzionamenti.

Contromisure per il dominio underwater

- **Sistemi acustici e droni di pattugliamento (UUV/USV)**: impiego di droni sottomarini autonomi (UUV) e di superficie (USV) dotati di sonar ad alta risoluzione. Pattugliano costantemente le rotte dei cavi e dei gasdotti per rilevare ancore trascinate, sommergibili ostili o subacquei.
- **Fibra ottica intelligente (Distributed Acoustic Sensing - DAS):** trasformazione dei cavi dati in veri e propri sensori acustici. La tecnologia DAS invia impulsi laser lungo la fibra; se una nave getta l'ancora o un sottomarino si avvicina, la vibrazione altera il ritorno del laser. Il sistema localizza l'intrusione con precisione millimetrica in tempo reale.
- **Crittografia Post-Quantum (PQC) a terra**: per neutralizzare lo spionaggio sottomarino (tapping), i dati vengono protetti alla radice nelle Landing Stations con algoritmi crittografici resistenti ai futuri computer quantistici. Se anche i dati venissero intercettati sul fondale, resterebbero indecifrabili.
- **Sistemi OT "Air-Gapped" e Zero Trust:** isolamento totale delle reti logiche che controllano le valvole dei gasdotti o la potenza dei cavi dalle reti internet aziendali, combinato con un'autenticazione continua e rigida per ogni singolo comando operato da terra.