EST 2014

HERMES BAY

ENHANCED AWARENESS

La protezione delle IC nazionali

In un mondo in cui i confini sono sempre più labili

CYBER ACT FORUM 2026

HERMESBAY.COM

La protezione delle IC nazionali

In un mondo in cui i confini sono sempre più labili



La crescente digitalizzazione delle reti energetiche e dei sistemi di trasporto nazionali ha ridefinito il concetto stesso di «confine di Stato».

Considerando l'attuale frammentazione degli equilibri globali, assistiamo a un passaggio da una gestione puramente tecnica e commerciale delle infrastrutture critiche a una loro totale militarizzazione geopolitica.

in questo scenario, come possono le democrazie occidentali bilanciare la necessità di una protezione totale con il mantenimento di mercati aperti e interconnessi?

Quali sono i limiti strutturali dell'attuale governance internazionale nel prevenire e sanzionare i sabotaggi in zone grigie come le acque internazionali?

Il contesto: i dati sugli attacchi



Negli ultimi anni, in merito agli attacchi contro le infrastrutture critiche, sono stati osservati:

- **Sabotaggio più frequente:** aumento delle operazioni contro infrastrutture in Europa, spesso condotte con modalità poco sofisticate.
- **Più deniability:** cavi danneggiati, incendi, sabotaggi e altri eventi possono essere presentati come incidenti o reati comuni.
- **Nuovi vettori:** droni, GNSS, cavi sottomarini e infrastrutture critiche entrano stabilmente nel perimetro della minaccia.
- **Convergenza fisico-cyber:** ricognizione, reclutamento locale, intrusione informatica e azione fisica possono appartenere alla stessa campagna.
- **Ritmo politico:** alcune campagne cyber e hacktiviste aumentano in corrispondenza di eventi e decisioni politiche.

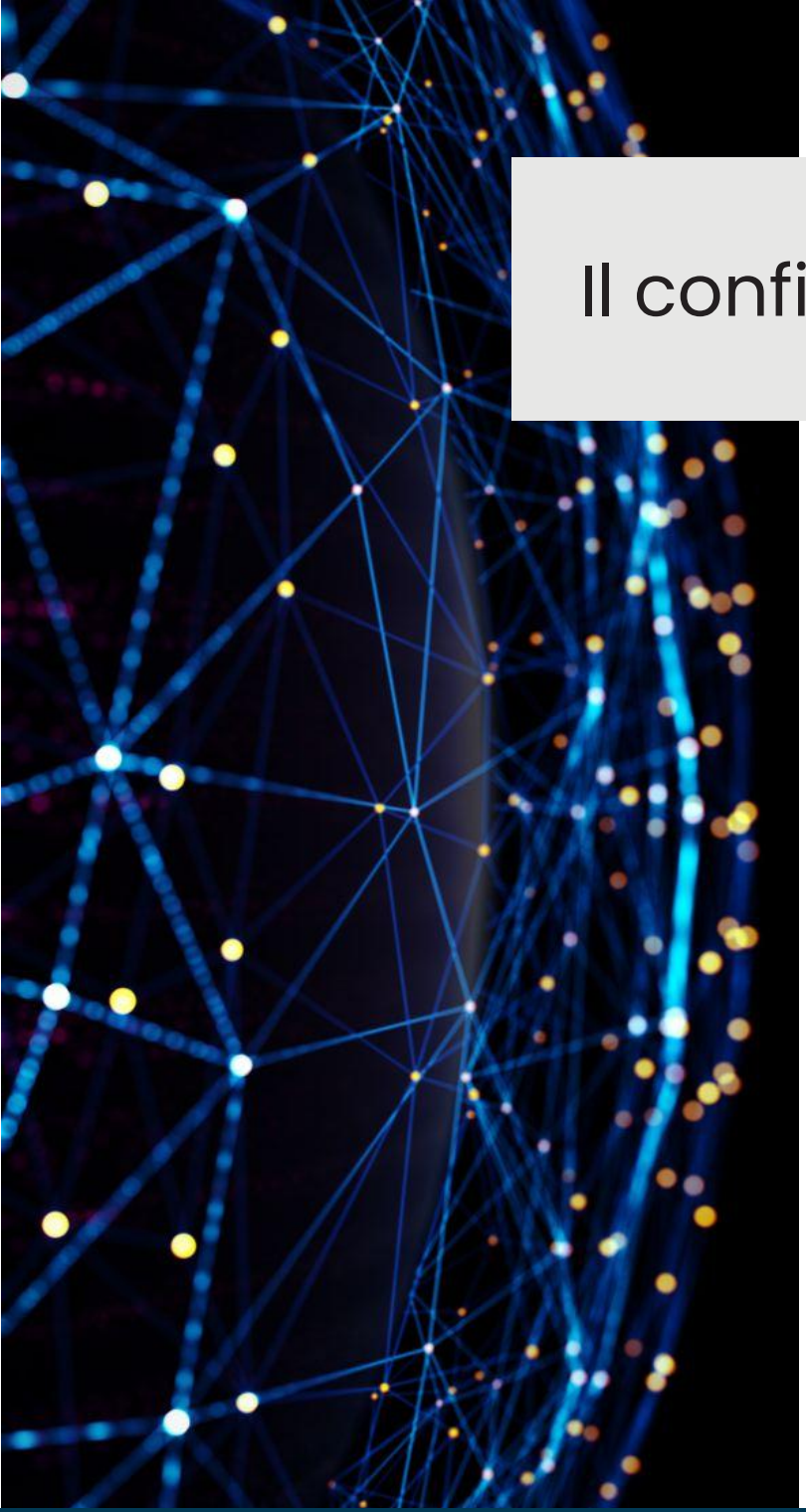
I nuovi confini di stato

La digitalizzazione delle reti energetiche e dei sistemi di trasporto ha ridefinito il concetto stesso di **confine di Stato**: ciò che uno Stato deve proteggere non coincide più con ciò che sta dentro i suoi confini fisici.



In un contesto di equilibri globali frammentati, le infrastrutture critiche passano da una gestione tecnica e commerciale a una **dimensione geopolitica**, in alcuni casi militare.

- Come possono le democrazie occidentali conciliare una adeguata protezione con mercati aperti e interconnessi?
- Quali sono i limiti strutturali della governance internazionale nel prevenire e sanzionare i sabotaggi in zone grigie come le acque internazionali?



Il confine ridefinito dalla digitalizzazione

Quattro "confini" che si sono spostati:

- **Confine fisico:** interconnettori elettrici, gasdotti e cavi attraversano mari e frontiere.
- **Confine digitale:** cloud, reti di controllo industriale (ICS/OT), telecomunicazioni.
- **Confine della filiera:** hardware, firmware e software prodotti e aggiornati altrove.
- **Confine giuridico:** l'infrastruttura è in uno spazio, l'operatore in un altro, il proprietario in un terzo.

Le infrastrutture come asset strategico

Oggi le infrastrutture sono bersagli, leve di pressione e strumenti di deterrenza. Gli attori ostili agiscono sotto la soglia del conflitto armato, dove l'azione è ambigua e la responsabilità difficile da dimostrare.

Si passa da una logica di gestione tecnico-commerciale a una di deterrenza e protezione.

	Prima	Oggi
Logica dominante	efficienza, costi, concorrenza	sicurezza nazionale, resilienza, deterrenza
Rischio principale	guasto, incidente, evento naturale	sabotaggio, pre-posizionamento, coercizione
Attore	operatore e regolatore	operatore, Stato, alleanze, forze armate
Il conflitto	dichiarato, con una soglia chiara	sotto soglia, ambiguo, negabile

Strumenti a livello europeo

Legge	Oggetto	Conseguenze per le IC
Direttiva CER 2022/2557	La legge europea sulla resilienza dei soggetti critici in 11 settori; include il sabotaggio tra le minacce.	Ogni Stato individua i propri soggetti critici, che devono valutare i rischi, adottare misure di resilienza e notificare gli incidenti. È vincolante.
Direttiva NIS2 2022/2555	La legge europea sulla cybersicurezza di un'ampia gamma di settori.	Obblighi di sicurezza e notifica, responsabilità diretta degli organi di amministrazione, sanzioni fino a 10 milioni di euro o al 2% del fatturato. È vincolante.
Piano d'azione sui cavi (2025) e Cable Security Toolbox (2026)	Il programma europeo per proteggere i cavi sottomarini: prevenire, rilevare, rispondere e ripristinare, dissuadere.	Misure per ridondanza, monitoraggio e riparazione, 13 progetti prioritari e 347 milioni di euro di finanziamenti. Le misure non sono vincolanti.

Strumenti a livello nazionale

Legge	Oggetto	Conseguenze per le IC
D.lgs. 138/2024 (recepimento NIS2)	La legge italiana sulla cybersicurezza dei settori essenziali e importanti. Designa l'ACN, l'Agenzia per la cybersicurezza nazionale, come **autorità competente**: il soggetto che controlla il rispetto degli obblighi e può sanzionare.	L'azienda deve registrarsi presso l'ACN, adottare misure di sicurezza e notificare gli incidenti significativi. Il **CSIRT Italia**, il centro operativo dell'ACN, riceve le notifiche, invia le allerte sulle vulnerabilità e supporta la risposta.
D.lgs. 134/2024 (recepimento CER)	La legge italiana sulla resilienza fisica e operativa dei soggetti critici, dall'energia ai trasporti, dall'acqua alla sanità.	Lo Stato adotta una strategia nazionale, valuta i rischi e individua i soggetti critici. Ciascuno deve valutare i propri rischi, adottare un piano di resilienza e notificare gli incidenti.
Legge 26 gennaio 2026, n. 9	La prima legge organica italiana sulla sicurezza delle attività subacquee. Istituisce l'ASAS, l'Agenzia per la sicurezza delle attività subacquee.	L'ASAS coordina il monitoraggio delle infrastrutture sottomarine di interesse nazionale (cavi, condotte), prepara i piani d'emergenza per ripararle e riceve le comunicazioni sulle attività subacquee.

A che punto siamo?

VEDERE → La capacità di rilevazione è cresciuta: nel primo semestre 2026 CSIRT Italia ha gestito **2.171 eventi** e ricevuto **1.160 notifiche NIS2 da 890 soggetti**.
Fonte: Comunicato stampa ACN 24 luglio 2026 (link)

IMPEDIRE → La sorveglianza può aumentare la probabilità di individuare un'azione ostile, ma non può coprire continuamente migliaia di chilometri di cavi e fondali.

RIPRISTINARE → Le infrastrutture possono quindi essere resilienti abbastanza da continuare a funzionare anche dopo un attacco, ma il ripristino fisico di un cavo sottomarino richiede mesi.

ATTRIBUIRE → Anche quando il danno è evidente, dimostrare chi lo ha causato e con quale responsabilità può richiedere anni.

L’equilibrio tra protezione e mercato aperto

Una dipendenza esterna diventa pericolosa quando riguarda un componente critico, difficile da sostituire e capace di compromettere un intero servizio: occorre capire quali dipendenze possiamo permetterci.

1

Quanto è critica la funzione?
Un componente che può compromettere una rete mobile, un sistema industriale o un'infrastruttura essenziale non può essere valutato come un normale acquisto. Più alto è l'impatto sistemico, più forte deve essere il controllo sul fornitore e sulla tecnologia.

2

Quanto è sostituibile il fornitore?
La stessa dipendenza cambia significato se esistono alternative immediate oppure se sostituirla richiede anni, investimenti enormi o una completa riprogettazione. **Il rischio cresce quando non possiamo cambiare fornitore nel momento in cui diventa necessario.**

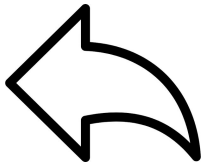
3

Quanto costa ridurre quella dipendenza?
Escludere un fornitore può aumentare prezzi, ridurre concorrenza e rallentare l'innovazione. Ma mantenere una dipendenza critica ha un costo potenziale molto maggiore se quella dipendenza diventa una leva di pressione.

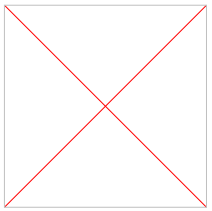
Conclusioni



Non esiste protezione assoluta
Non è realistico eliminare ogni dipendenza tecnologica, sorvegliare ogni tratto di fondale o impedire ogni sabotaggio. La sicurezza deve quindi concentrarsi sulle vulnerabilità che possono produrre **effetti sistemici**.



Proteggere significa anche poter reagire
Ridondanza, diversificazione dei fornitori, capacità di riparazione, monitoraggio e cooperazione investigativa riducono il valore strategico di un singolo attacco. L'obiettivo non è evitare ogni incidente, ma **impedire che l'incidente comprometta il sistema**.



La zona grigia resta il punto più difficile
Quando il danno avviene in acque internazionali, l'attribuzione è incerta e la responsabilità coinvolge più ordinamenti, la risposta diventa lenta e la deterrenza si indebolisce. È qui che i limiti tecnici degli strumenti incontrano i limiti della governance internazionale.

CYBER ACT FORUM 2026

EST 2014

HERMES BAY

ENHANCED AWARENESS

Grazie per l'attenzione

Dott. Ing. Luisa Franchina
CEO

Via Nazionale, 214 - 00184 Roma
l.franchina@hermesbay.com
06 59 24 441

HERMESBAY.COM