



S&A
SISTEMI & AUTOMAZIONE

Forum Cyber 4.0

Università LUISS – 4 giugno 2026

Dott.ssa Maria Felicita Mucci – S&A

Sovranità Digitale e Competizione fra Potenze

Il Dominio Cyber come Nuova Westfalia

www.sealink.it

Un Cambio di Paradigma

Da Wesfalia alla sovranità digitale post territoriale: il dominio cibernetico come principale “Game Changer” nelle Relazioni Internazionali.

ITALIA - RANSOMWARE

SynLab Italia

Aprile 2024



380

laboratori clinici paralizzati

73 giorni

il malware era già dentro

1,5 TB

dati medici rubati • €12M danni

BlackBasta entra silenzioso. Per 73 giorni nessuno se ne accorge. Poi 380 laboratori si fermano.

EUROPA - EMERGENZA NAZIONALE

Romania – Rete Ospedaliera

Febbraio 2024



18

Ospedali colpiti simultaneamente

~ 100

Strutture offline per precauzione

Emergenza

Cyber dichiarata dallo Stato

Backmydata/ALPHV cifra cartelle cliniche. I pazienti vengono reindirizzati.

USA – RECORD MONDIALE

Change Healthcare

Febbraio 2024



190M

Americani con dati sanitari esposti

\$ 22M

Riscatto pagato da UnitedHealth

6 mesi

di caos nella fatturazione sanitaria

ALPHV/BlackCat entra in Change Healthcare. 190 milioni di cartelle. Il sistema sanitario nazionale va in tilt.

Nuove Dottrine di Scontro

Il **Cyber Power** genera il **Security Dilemma algoritmico**: la postura difensiva di uno Stato viene percepita come minaccia, innescando una corsa agli armamenti digitali (John Herz).



Deterrenza Tradizionale

Risposta punitiva ex-post. Deterrenza reattiva. Si preserva lo status quo attendendo l'attacco.

VS



«Persistent Engagement» (USA)

Presenza costante e proattiva nelle reti avversarie. Vantaggi informativi continui e difesa preventiva.

Contesto VUCA (Volatility, Uncertainty, Complexity, Ambiguity):
Cross-Domain Escalation come rischio concreto per la sicurezza globale

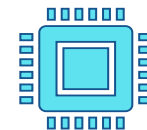
Geopolitica dei Dati & AI

Il potere digitale poggia su **asset fisici critici**. L'AI accelera i conflitti verso una «**Hyperwar**» **algoritmica** (John R. Allen)



Cavi Sottomarini

Nervi vitali della trasmissione globale.
Contesi tra USA, Cina ed Europa.
Sfida geostrategica per il dominio
dei flussi informative globali.



Chip e Semiconduttori

Hardware avanzati e rincorsa al Quantum Computing.
Dipendenza dalle supply chain
come vulnerabilità strategica primaria.



Data Center

Pilastri della “**Geopolitica dei Dati**”.
Depositivi del “**Petrolio del XXI secolo**”.

Le **infrastrutture critiche digitali e fisiche** sono il fondamento del potere nazionale.

Autonomia Strategica & Valori

UE come Centro e Potenza normativa globale. In un rischio di “**Balkanizzazione Digitale**” (Cina, Russia, Iran), la “**Cyber Hygiene**” è un dovere civico e un pilastro della sicurezza nazionale.



Sovranità Normativa

Caso Schrems II: Standard indipendenti con i valori europei, rifiutando giurisdizioni non equivalenti.



Cyber Diplomacy

Ordine internazionale basato su norme condivise arginando la militarizzazione indiscriminate e tutelando le società aperte.



Responsabilità Collettiva

Dalla governance internazionale alla Cyber Hygiene quotidiana. Mutualità inevitabile (M.L. King) per evitare derive distopiche.



«Il costo della Democrazia è la vigilanza» (Karl Popper)

SOVRANITÀ, NORME E VALORI: il fondamento del Cyber Power europeo.

