

SOVRANITA' DIGITALE E PERCORSI DI ADOZIONE

SOVRANITA' DIGITALE E CYBERSECURITY

2 DICEMBRE 2025

ELENA VACIAGO, RESEARCH MANAGER, TIG – THE INNOVATION GROUP

UN EVENTO DI



SOVRANITA' DIGITALE e cybersecurity

09.30 - 09.40

INTRODUZIONE E PRESENTAZIONE RICERCA TIG

Elena Vaciago, *Research Manager, TIG - The Innovation Group*

09.40 - 11.15

SESSIONE PLENARIA: SCENARI DI RISCHIO E TECNOLOGIE STRATEGICHE

Chaired by Giancarlo Calzetta, *Research & Content Manager, TIG - The Innovation Group*

I RISCHI DELLO SCENARIO GEOPOLITICO INTERNAZIONALE E IL RUOLO DELLA SOVRANITA' DIGITALE

Mark William Lowe, *Advisor on geopolitical and corporate risk management*

COSA DICONO LE NORMATIVE EUROPEE E PERCHÉ

Valerio Vertua, *Partner, 42 Law Firm*

ROUNDTABLE LE VOCI SUL CAMPO: CYBERSECURITY COME ABILITATORE DELLA SOVRANITÀ

Guido Arnone, *Direttore della Direzione Innovazione Tecnologica e Digitale, Comune di Milano*

Nicla Ivana Diomede, *Dirigente Responsabile "Governance e Gestione cybersecurity", ATS Città Metropolitana di Milano*

Maurizio Desiderio, *Country Manager Italia, ClearSkies*

Federico Lucia, *Direttore Didattico & Board Member, ANRA*

Riccardo Paglia, *Cybersecurity Executive e Go-to-Market Strategist, Maticmind*

Davide Telasi, *Sales Manager, Equixly*

UN EVENTO DI



SOVRANITA' DIGITALE e cybersecurity

11.15 - 11.35

COFFEE BREAK & ENGAGEMENT IN THE NETWORKING AREA

11:35 - 13:00

SESSIONE PLENARIA: SCENARI DI RISCHIO E TECNOLOGIE STRATEGICHE

Chaired by Giancarlo Calzetta, *Research & Content Manager, TIG - The Innovation Group*

COME IL SISTEMA ITALIA PUÒ SUPPORTARE LA SOVRANITÀ DIGITALE

Paolo Spagnoletti, *Presidente Cyber4.0, Full Professor of Organization Studies Luiss University*

RUOLO E RISCHI DEI MODELLI AI OPEN WEIGHTS NELLA SOVRANITA' DIGITALE

Enrico Frumento, *Cybersecurity Research Lead, Cefriel*

ROUNDTABLE SOVRANITÀ DIGITALE E MODELLI DI ADOZIONE

Vincenzo Calabrò, *ISO, Ministero dell'Interno*

Fabio Ciolino, *Head of Product, Aruba Cloud*

Massimo Cottafavi, *Director Cyber Security & Resilience, Snam*

Giuseppe Cozzolino, *Country Manager, SUSE Italia*

Rino Micheloni, *Chief Executive Officer, Avaneidi*

Alessia Valentini, *Advisory Board Member, Osservatorio sulla Sicurezza Nazionale - OSSN Unipegaso*

UN EVENTO DI



SOVRANITA' DIGITALE e cybersecurity

14.00 – 15.20

TAVOLI DI LAVORO PARALLELI RISERVATI

Tavolo 1: SOVRANITÀ DIGITALE & RESILIENZA OPERATIVA

Hardware & Software made in EU per la resilienza operativa;

Data Governance & Sovranità dei Dati.

moderato da **Giancarlo Calzetta**, Research & Content Manager, TIG – The Innovation Group

Tavolo 2: RIDURRE I RISCHI INTEGRARE LA CYBERSECURITY

Tendenze e minacce emergenti; Contenimento & Mitigazione;

Trusted Infrastructure: controllo tecnologico delle infrastrutture digitali e dei servizi in cloud.

moderato da **Elena Vaciago**, Research Manager, TIG – The Innovation Group

Tavolo 3: THREAT INTELLIGENCE

Case study di Threat Intelligence in azione;

Threat intelligence predittiva con AI; Infosharing a livello nazionale.

moderato da **Enrico Frumento**, Cybersecurity Research Lead, Cefriel

SOVRANITA' DIGITALE, UNA DEFINIZIONE

PARLIAMO DI «AUTONOMIA» O «INDIPENDENZA» TECNOLOGICA?

Aspetto	Autonomia	Indipendenza
Origine	deriva dal greco <i>autós</i> (“sé stesso”) e <i>nómos</i> (“legge”), quindi letteralmente significa “darsi la propria legge”	deriva dal latino <i>in-</i> (“non”) e <i>dependere</i> (“dipendere”), cioè “non dipendere da”
Significato	Capacità di autodeterminarsi entro un contesto	Condizione di non dipendenza da altri
Focus	Interno (autogoverno)	Esterno (assenza di vincoli)
Implica	Responsabilità, consapevolezza	Libertà, emancipazione

- **Autonomia** = capacità interna → autogoverno, competenza, responsabilità e libertà di scelta consapevole all’interno di un contesto.
- **Indipendenza** = condizione esterna → assenza di subordinazione o di controllo da parte di altri.

COSA SIGNIFICA QUINDI «SOVRANITA' TECNOLOGICA»? UNA DEFINIZIONE

*«La Sovranità Digitale è la capacità di uno Stato, di un'organizzazione pubblica o privata, di un insieme di soggetti, di esercitare un **controllo autonomo, consapevole e sicuro sulle tecnologie digitali critiche** (infrastrutture, dati, software, piattaforme e competenze) al fine di garantire che le scelte strategiche e l'uso del digitale siano **coerenti con i propri valori, interessi e regole**».*

La Sovranità Digitale è un tassello fondamentale dell'autonomia strategica degli Stati».

I PRINCIPI GENERALI DELLA SOVRANITA' DIGITALE

- ❖ **Autonomia tecnologica.** Capacità di sviluppare, produrre e gestire **tecnologie critiche (cloud, semiconduttori, AI, cybersecurity, telecomunicazioni, ecc.)** senza dipendere totalmente da fornitori extraeuropei. Include la possibilità di sostituire componenti o servizi senza blocchi nella continuità operativa.
- ❖ **Controllo sui dati.** I dati generati da cittadini, imprese e pubbliche amministrazioni devono essere conservati, elaborati e trasferiti in conformità con le regole nazionali o europee (es. GDPR). Ciò implica anche la possibilità di limitare il trasferimento transfrontaliero dei dati verso paesi che non garantiscono tutele equivalenti.
- ❖ **Sicurezza e resilienza.** Garantire che infrastrutture digitali, reti e servizi essenziali siano protetti da minacce cibernetiche e possano continuare a funzionare anche in scenari di crisi o conflitto. Include anche la capacità di reagire autonomamente a incidenti o interruzioni.
- ❖ **Governance e trasparenza.** Le decisioni su tecnologie, standard e infrastrutture devono essere governate da regole trasparenti e democratiche, coerenti con i valori dello Stato o dell'Unione europea (diritti digitali, privacy, non discriminazione, ecc.).
- ❖ **Competenza e innovazione.** La sovranità digitale non è solo "controllo", ma anche capacità di innovare e di sviluppare competenze locali in settori chiave (AI, Quantum, cybersecurity, Cloud, Edge computing...). Promuovere un ecosistema tecnologico indipendente, con investimenti in ricerca, formazione e startup.
- ❖ **Interoperabilità e cooperazione.** La sovranità digitale non significa isolamento, ma partecipazione consapevole a un sistema globale basato su standard aperti, interoperabilità e cooperazione tra partner che condividono valori comuni (es. all'interno dell'UE).

INFRASTRUTTURE TECNOLOGICHE A SUPPORTO DELLA SOVRANITÀ DIGITALE

CLOUD E EDGE SOVRANI



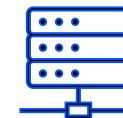
- **Obiettivo:** garantire che dati sensibili e servizi critici siano ospitati e trattati secondo normative locali o europee.
- **Elementi chiave:** Cloud nazionale/europeo (GAIA-X, Polo Strategico Nazionale), Edge computing sovrano, EU Cloud Rulebook.
- **Benefici:** autonomia tecnologica, protezione dei dati, riduzione delle dipendenze da hyperscaler globali.

CYBERSECURITY



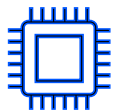
- **Obiettivo:** proteggere asset digitali, reti e dati da minacce esterne, garantendo continuità e controllo.
- **Elementi chiave:** SOC sovrani, Centri nazionali, piattaforme di Threat Intelligence europee, crittografia e identità digitale (es. EU Digital Identity Wallet) sviluppati e controllati localmente.
- **Esempi:** rete europea dei Cybersecurity Competence Centres, direttiva NIS2.

GESTIONE DEI DATI



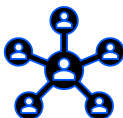
- **Obiettivo:** assicurare il controllo, la localizzazione e il valore economico dei dati generati da cittadini e imprese.
- **Elementi chiave:** European Data Spaces, Data Act, Repository nazionali sicuri per dati pubblici e privati strategici.
- **Benefici:** garantire interoperabilità, protezione della privacy e uso etico dei dati senza bloccare l'innovazione.

HARDWARE E SEMICONDUTTORI



- **Obiettivo:** ridurre la dipendenza da fornitori esteri (soprattutto asiatici e americani) nei componenti strategici.
- **Elementi chiave:** European Chips Act, sviluppo di chip europei, filiere sicure e tracciabili, ricerca su processori open source (es. RISC-V europei).
- **Sfida:** colmare il gap industriale e tecnologico rispetto a Stati Uniti e Asia.

CONNETTIVITÀ E RETI SICURE



- **Obiettivo:** assicurare un accesso equo, resiliente e controllato alle reti digitali.
- **Elementi chiave:** reti 5G/6G sicure, dorsali europee, cavi sottomarini, programma satellitare IRIS.
- **Benefici:** sovranità nelle comunicazioni, riduzione delle dipendenze infrastrutturali.
- **Sfida:** bilanciare sicurezza nazionale, apertura del mercato e rapidità di adozione.

AI E SUPERCOMPUTING



- **Obiettivo:** disporre di capacità computazionali autonome e algoritmi addestrati su dati sovrani.
- **Elementi chiave:** supercomputer europei (EuroHPC), AI Act, centri di calcolo nazionali.
- **Benefici:** innovazione controllata, sicurezza e conformità etica.
- **Sfida:** competere con i colossi globali (USA e Cina) e garantire un uso responsabile dell'AI.

QUANTO IMPATTANO OGGI I TREND TECNOLOGICI E L'ATTUALE SITUAZIONE GEOPOLITICA IN TEMA CYBERSECURITY?

TREND TECNOLOGICI CHE COMPORTANO UN RIPENSAMENTO DELLA CYBERSECURITY

		INDUSTRIA	FINANZA	PA	UTILITIES
Intelligenza artificiale	85%	82%	89%	90%	88%
Migrazione al cloud	51%	54%	63%	70%	44%
Evoluzione dell'Identity Management	49%	46%	44%	65%	56%
Connettività degli oggetti, OT e IoT	46%	75%	26%	40%	63%
Quantum computing	35%	21%	63%	35%	6%
DevOps	32%	14%	30%	35%	19%

D. Le aziende sono costantemente coinvolte in processi di trasformazione digitale. Quali dei seguenti trend tecnologici comportano un ripensamento della cybersecurity?
Base: tutti i rispondenti (158)

SITUAZIONE GEOPOLITICA, QUANTO IMPATTA SULLA CYBERSECURITY?

TREND GEOPOLITICI CHE INFLUENZANO SCELTE E INVESTIMENTI IN CYBERSECURITY

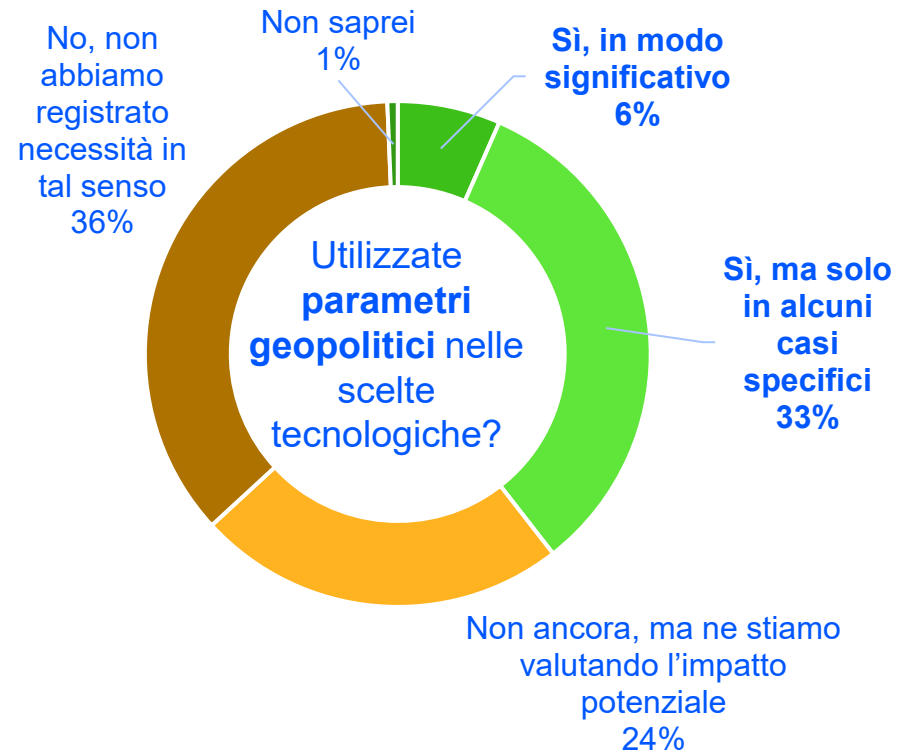
		INDUSTRIA	FINANZA	PA	UTILITIES
Politiche di cybersicurezza nazionale o UE (es. NIS2, EUCS)	61%	68%	42%	65%	71%
Rischi legati alla sovranità e localizzazione dei dati	53%	43%	58%	65%	50%
Tensioni o instabilità in aree chiave della supply chain	34%	39%	31%	35%	43%
Volontà di ridurre la dipendenza da tecnologie extra-UE	26%	25%	31%	35%	21%
Timori legati a backdoor o ingerenze statali nei software	20%	21%	35%	30%	21%
Restrizioni/ sanzioni internazionali verso vendor/ Paesi	20%	39%	27%	20%	7%

D. Quali aspetti geopolitici influenzano maggiormente le valutazioni su tecnologie e fornitori nella Sua organizzazione?

Base: tutti i rispondenti (152)

PRESENZA ATTUALE DI VALUTAZIONI GEOPOLITICHE NELLE SCELTE TECNOLOGICHE

VALUTAZIONI GEOPOLITICHE	
INDUSTRIA	46%
FINANZA	35%
PA	30%
UTILITIES	29%

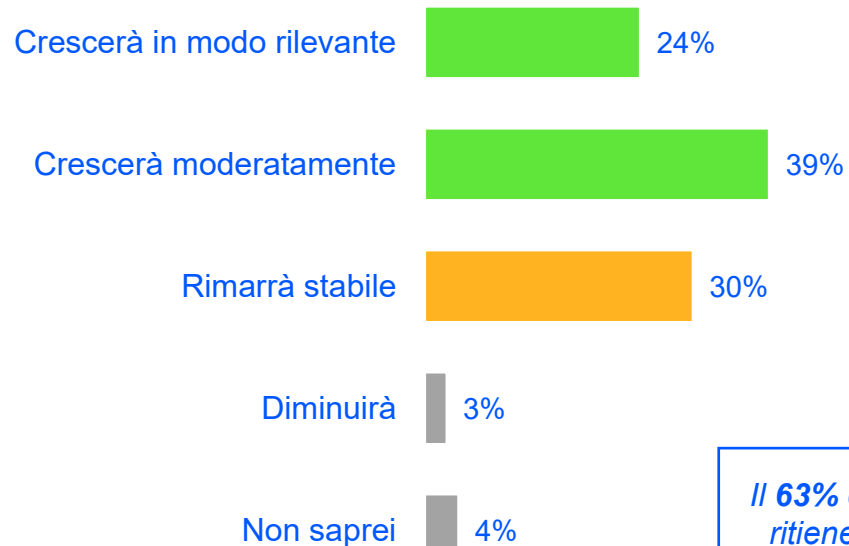


VALUTAZIONI GEOPOLITICHE	
TUTTE	39%
LARGE	38%
MEDIUM	36%
SMALL	50%

D. La Sua organizzazione ha recentemente rivalutato o modificato le scelte tecnologiche (vendor, servizi, cloud, etc.) a causa di dinamiche geopolitiche?
Base: tutti i rispondenti (152) – Small (50-200 addetti) 22; medium (200-1000 addetti) 36; Large (>1000) 94

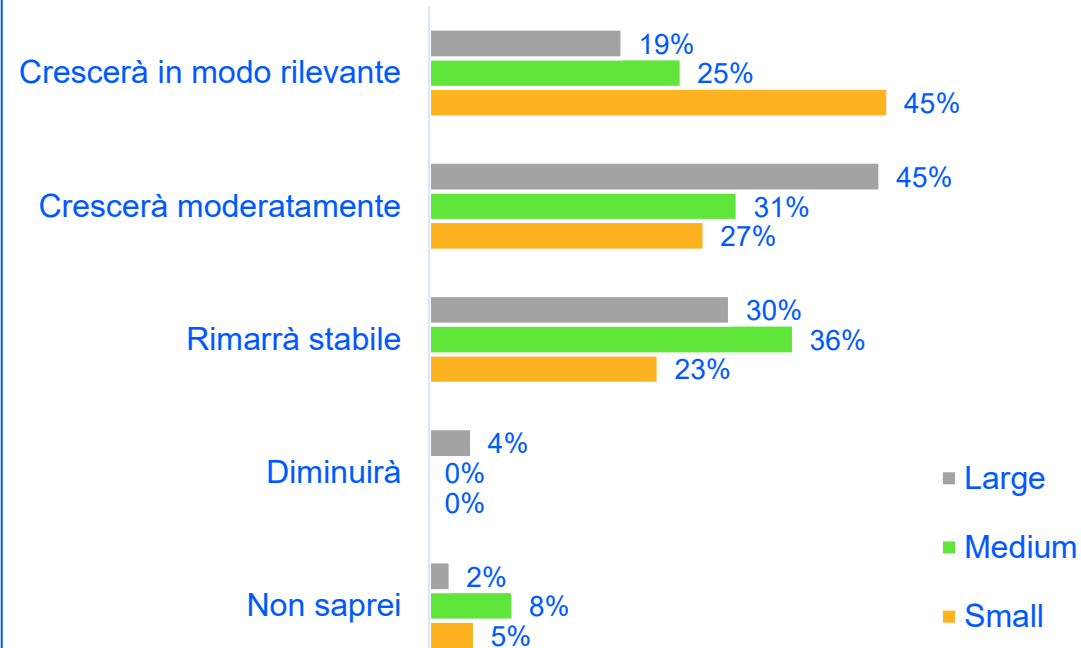
TENDENZA A EFFETTUARE VALUTAZIONI GEOPOLITICHE NELLE SCELTE TECNOLOGICHE

L'INFLUENZA DELLE TENSIONI GEOPOLITICHE SULLE SCELTE TECNOLOGICHE CRESCERÀ O DIMINUIRÀ?



Il 63% del campione ritiene che il peso geopolitico andrà ad aumentare in futuro

L'INFLUENZA DELLE TENSIONI GEOPOLITICHE SULLE SCELTE TECNOLOGICHE CRESCERÀ O DIMINUIRÀ?



D. Ritiene che nei prossimi 12-24 mesi l'influenza delle tensioni geopolitiche sulle scelte tecnologiche crescerà o diminuirà?
Base: tutti i rispondenti (152)

Siamo The Innovation Group.

Progettiamo, raccontiamo e governiamo il cambiamento.



www.tig.it
info@tig.it
+39 02.49988.1

TIG Events s.r.l.
Via Ettore Romagnoli, 6
20146, Milano
