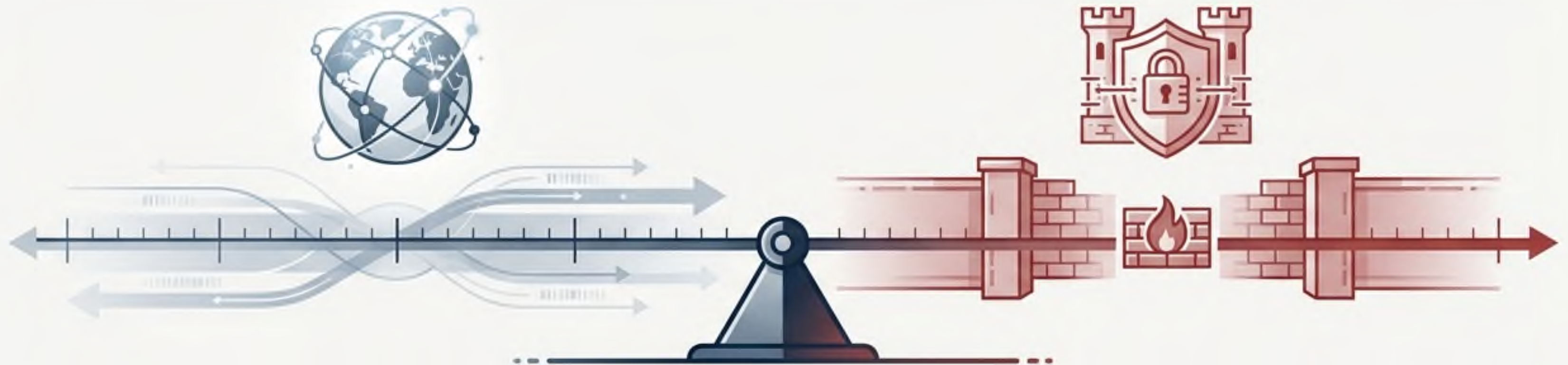


Il Nuovo Ordine Mondiale del Cyberspazio

Una guida strategica alla Sovranità
Digitale, basata sull'analisi di
Roberto Baldoni.



La fine dell'innocenza tecnologica: dalla globalizzazione alla post-globalizzazione



L'Era del Libero Mercato (1990s-2014)

Dominio della "Californian Ideology". Le filiere globali massimizzano l'efficienza a scapito della sicurezza (es. cessione divisione PC di IBM a Lenovo nel 2005).

L'Era della Sicurezza (2014-Oggi)

Il punto di svolta geopolitico. Le superpotenze adottano il de-risking. Le vulnerabilità sistemiche spingono i governi a proteggere le tecnologie critiche.

L'Anatomia della Sovranità Digitale



Pilastro 1: Controllo dei Dati Nazionali

Autorità sui dati generati da cittadini, imprese e infrastrutture critiche.



Pilastro 2: Tecnologie e Filiere Sicure

Uso di sistemi computazionali affidabili per evitare la dipendenza da potenze ostili.



Pilastro 3: Consapevolezza Diffusa

Educazione al rischio per cittadini, lavoratori e consigli di amministrazione.



Pilastro 4: Collaborazione Internazionale

Costruzione di alleanze per minacce che non possono essere affrontate in autarchia.

L'obiettivo dinamico e il divario di vulnerabilità



Minaccia i: Il dominio degli attacchi informatici



Attori Statuali (APT)

Focus su spionaggio, furto di proprietà intellettuale e sabotaggio militare (es. attacco HermeticWiper in Ucraina, Stuxnet).



Cybercriminali

Focus su estorsione finanziaria. Il modello Ransomware-as-a-Service paralizza infrastrutture (es. oleodotto Colonial Pipeline, ferrovie italiane via The Hive).



Hacktivisti

Focus su azioni dimostrative e politiche. Attacchi DDoS su vasta scala (es. caso Dyn tramite botnet Mirai).

Minaccia 2: La fragilità delle filiere tecnologiche



Disponibilità (Blocco)

Interruzioni geopolitiche 0 incidenti critici (es. aggiornamento CrowdStrike che ha bloccato 8 milioni di PC).

Integrità (Manomissione)

Inserimento di codici malevoli o esplosivi in prodotti apparentemente sicuri (es. caso SolarWinds, cercapersone in Libano).

| Confidenzialità (Spionaggio)

Estrazione silenziosa di dati sensibili tramite servizi Cloud 0 reti 5G gestite da fornitori non affidabili.

Minaccia 3: L'orizzonte e l'uso ostile dell'Intelligenza Artificiale

Rischi a Breve Termine (ANI)

Allucinazioni (es. 'Napoleone scopre l'America'), Deepfakes, contenuti tossici e sudditanza (sycophancy) verso gli utenti.

Rischi a Lungo Termine (AGI/ASI) AY

Macchine con prestazioni sovrumane. Perdita di controllo umano sulle strategie autonome.

/ // 7

L'Uso Ostile

Sviluppo di IA senza meccanismi di sicurezza (guardrails) per scopi militari o di destabilizzazione (es. il sistema israeliano The Gospel).

Minaccia 4: L'apocalisse crittografica e il 'Q-Day'



il Q-Day

Il momento in cui un computer quantistico riuscirà a violare l'algoritmo RSA-2048, esponendo in chiaro i segreti militari, finanziari e commerciali del mondo.

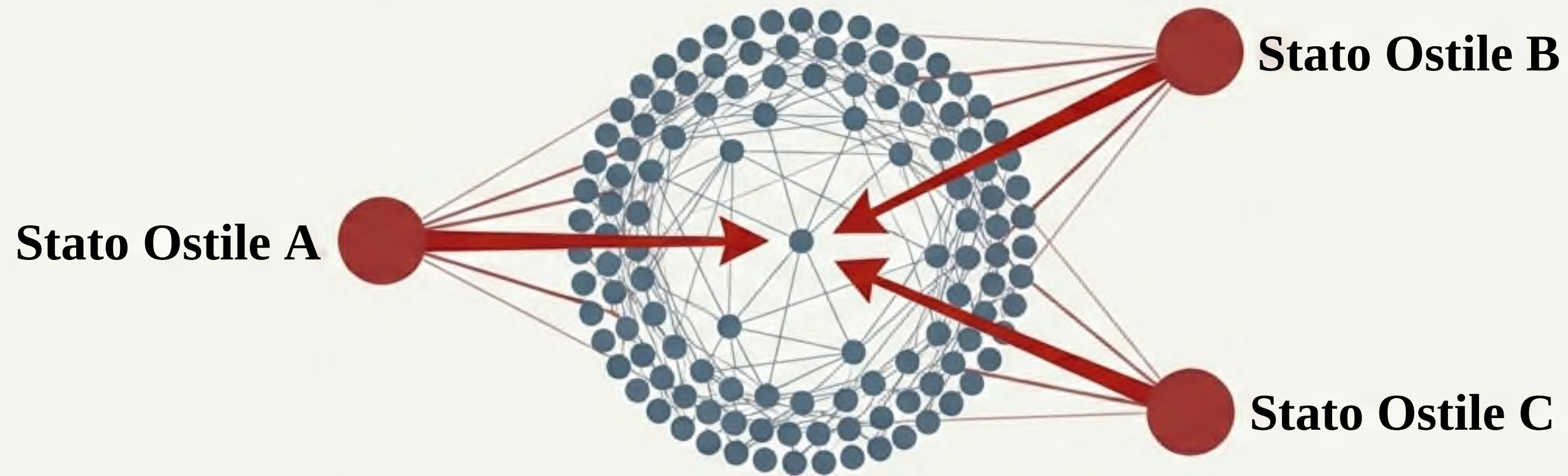
10.000 Qubit = 104 Giorni

La corsa contro il tempo: Ricercatori stimano che un computer con 10.000 qubit potrebbe decifrare l'RSA in soli 104 giorni.

Target 2035

La contromisura: Transizione urgente verso protocolli quantum-safe. Gli Stati Uniti impongono l'adeguamento delle risorse federali entro il 2035.

Minaccia 5: Guerra ibrida e l'arma della disinformazione



La Bolla Informativa (Echo Chamber)

Algoritmi progettati per massimizzare il profitto creano polarizzazione sociale, confermando continuamente i pregiudizi degli utenti.

Manipolazione Statuale

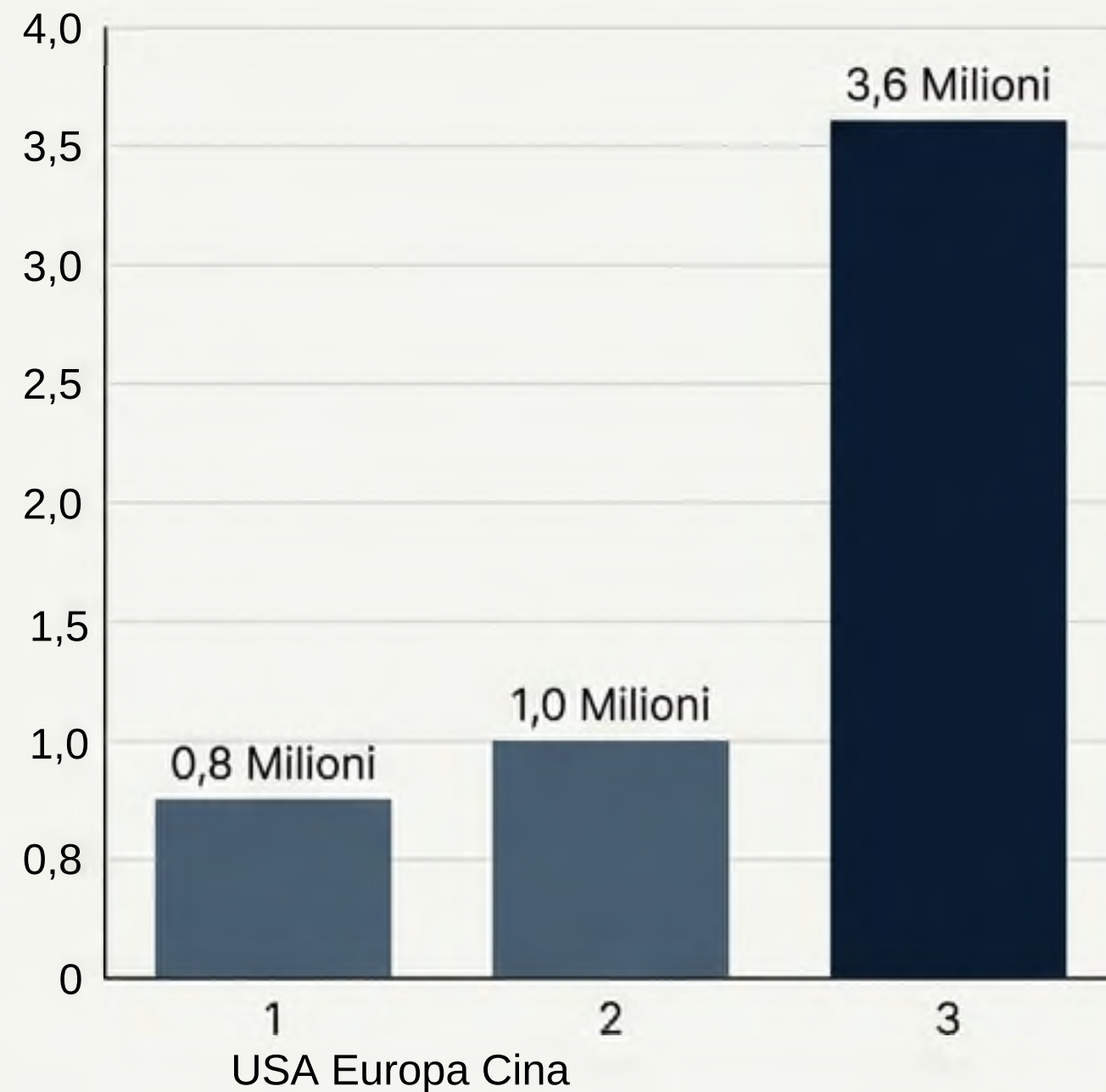
Attori ostili sfruttano le piattaforme per campagne di micro-targeting (es. interferenza russa IRA e Cambridge Analytica su 50 milioni di profili).

La Minaccia Ibrida

Combinazione simultanea di cyber-attacchi, disinformazione e coercizione economica per paralizzare il processo decisionale delle democrazie.

Il tallone d'Achille: il deficit globale di talenti

Laureati STEM Annuali (2020)



85
Milioni

Un Vuoto Critico: Si stima una carenza globale di 85 milioni di lavoratori qualificati entro il 2030 (dati Korn Ferry).



Rischio Sicurezza: La disperata ricerca di personale costringe le aziende ad abbassare i controlli di sicurezza, aprendo le porte a infiltrazioni ostili nelle infrastrutture critiche.

Il tabellone geopolitico: tre modelli a confronto

		
Stati Uniti d'America	Cina	Unione Europea
Tecno-Democrazia	Autarchia Tecnologica	Superpotenza Normativa
Focus su reindustrializzazione aggressiva e alleanza simbiotica con le Big Tech.	Controllo statale assoluto, Internet Sovrano e allineamento ideologico dell'innovazione.	Focus primario su protezione dei diritti e standardizzazione globale, ma debolezza industriale interna.

USA: Reindustrializzazione e Tecno-Democrazia

- **Investimenti Massicci**

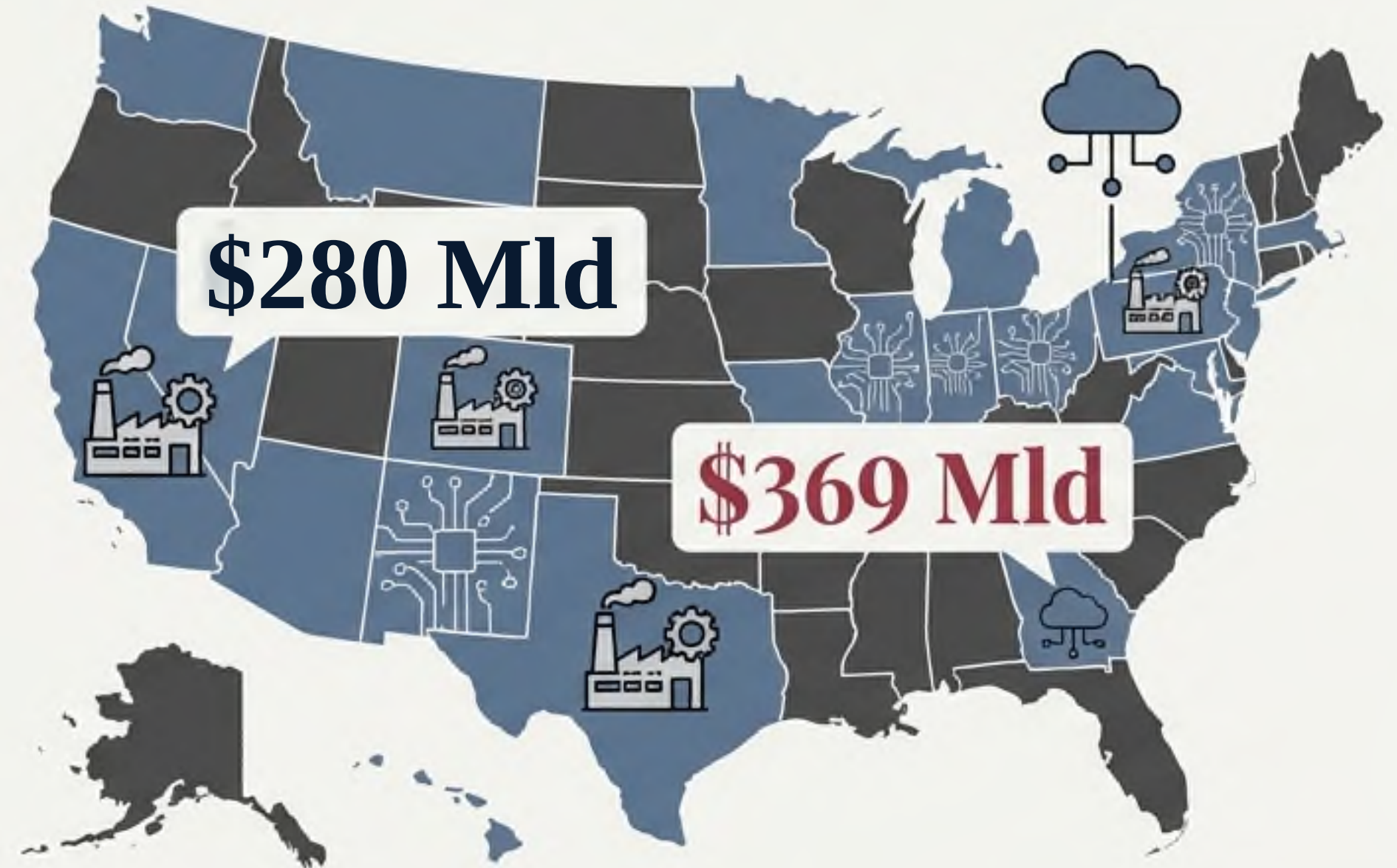
Il CHIPS and Science Act (\$280 miliardi) e l'Inflation Reduction Act (IRA, \$369 miliardi) mirano a riportare le filiere critiche su suolo americano.

- **Sinergia con la Silicon Valley**

Il governo federale si affida alle Big Tech per infrastrutture cloud sicure, intelligenza artificiale militare e supporto nei teatri di guerra (es. Ucraina).

- **De -Risking Aggressivo**

Bandi diretti a tecnologie straniere (es. divieto di TikTok sui dispositivi governativi e restrizioni all'esportazione di microchip avanzati).



Cina: Autarchia tecnologica e “Internet Sovrano”



- **L’Internet Sovrano**

Una rete blindata e frammentata (Great Firewall) per controllare il dissenso interno e prevenire iniezioni di valori occidentali.

- **Sottomissione delle Big Tech**

Il Partito ha ridimensionato giganti come Alibaba (ristrutturazione forzata) per impedire la nascita di poteri finanziari indipendenti.

- **Allineamento dell'IA**

Linee guida severe impongono che l'Intelligenza Artificiale generativa rispetti i "valori fondamentali del socialismo", creando un ecosistema incompatibile con l'Occidente.

Unione Europea: La Superpotenza Normativa

O Standard Globali

L'UE guida il mondo nei diritti digitali. Il GDPR è uno standard globale; il Digital Services Act (DSA) combatte la disinformazione; l'AI Act pioneristico regola l'Intelligenza Artificiale.

O La Vulnerabilità Strutturale

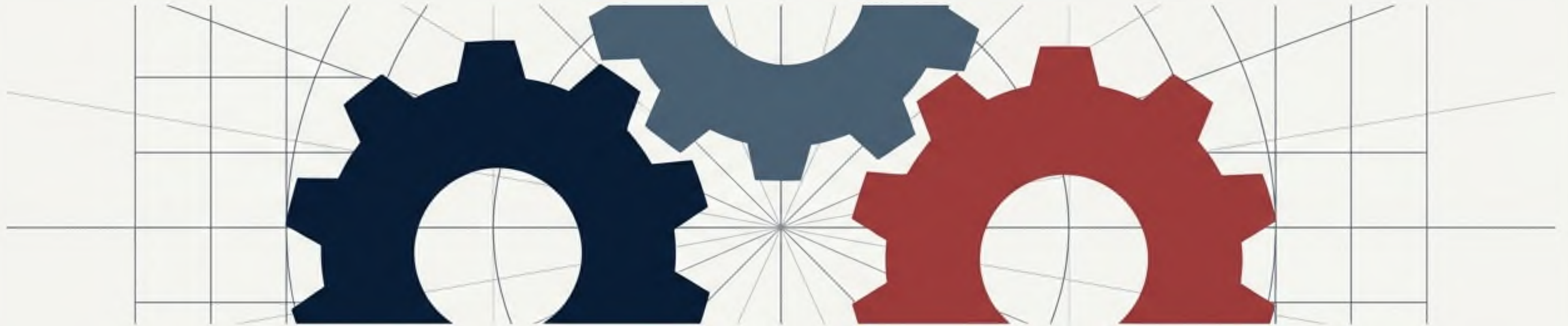
Il dilemma 'Mercato vs. Sicurezza'. La frammentazione in 27 mercati impedisce la creazione di campioni industriali (Big Tech) europei.

O Dipendenza Estera

Nonostante iniziative come l'EUCS per il Cloud e il Chips Act, l'Europa rimane pericolosamente dipendente da tecnologie americane e asiatiche.



La via da seguire: dall'autarchia all'interdipendenza strategica



Sinergia Pubblico-Privato

La sovranità digitale moderna richiede un'alleanza ferrea tra governi e aziende tecnologiche.

Interdipendenza, non Isolamento

Nessuna nazione democratica può sopravvivere in totale autarchia. La risposta è il friend-shoring e il controllo dei nodi critici delle filiere.

Difesa Collettiva

La sicurezza del futuro si baserà su alleanze internazionali fluide, innovazione continua e cittadini formati. Il cyberspazio globale si difende insieme.