# Il pilastro nascosto della sovranità digitale:

## Perché l'Europa deve dare importanza ai router Internet

IEF SAFENet SOVEREIGNTY ALLIANCE FOR EUROPEAN NETWORK TECHNOLOGY iconomy

# INDICE

# Premessa

DA RAGAZZO, quando facevo il chierichetto in chiesa, mi fu dato un consiglio indimenticabile riguardo al mio ruolo di piccolo aiutante del sacerdote all'altare: nessuno nota un chierichetto a meno che, o finché, non commetta un errore. Mentre ci apprestavamo a redigere questo articolo, quell'idea continuava a tornarmi in mente, perché i router, il tema di questo articolo, sono simili agli aiutanti invisibili della nostra vita quotidiana su Internet. Sono ovunque, ma sotto molti aspetti nascosti e trascurati. Di solito ci si accorge della loro presenza solo quando abbiamo problemi con la nostra connessione a Internet.

Normalmente questo non sarebbe un problema, ma le recenti realtà politiche hanno portato la geopolitica in ogni livello del mondo tecnologico. L'Europa e gli Stati Uniti, ad esempio, hanno compiuto grandi sforzi per discutere o addirittura rimuovere l'hardware cinese dalle reti 5G considerate critiche. C'è ancora chi si chiede se la minaccia sia proporzionata alle misure adottate, ma l'opinione pubblica e chi fa le leggi mostrano una disponibilità crescente a tutelare gli interessi europei. Eppure, fino a oggi, questa attenzione non è arrivata in modo coerente fino al dispositivo finale dell'utente. Questo articolo mira a cambiare la situazione.

La Innovate Europe Foundation sostiene da tempo una maggiore sovranità attraverso lo sviluppo di un ecosistema tecnologico e digitale europeo. Come molti, ci siamo spesso concentrati sulle piattaforme e sui servizi digitali costruiti su di esse, finché non abbiamo iniziato a rivolgere maggiormente la nostra attenzione agli strati infrastrutturali sottostanti. Il nostro articolo sul cloud computing del 2018 aveva già evidenziato il rischio di dipendenze critiche nell'infrastruttura cloud.

Ora che le ambizioni europee per una maggiore sovranità tecnologica si sono diffuse, suggeriamo umilmente che esiste ancora un altro livello tecnologico che è stato troppo spesso ignorato: i router e i ripetitori che costituiscono l'infrastruttura di base nella maggior parte delle abitazioni e delle aziende. Finora, pochi sono consapevoli a) dell'origine prevalentemente non europea di queste apparecchiature e b) del livello di rischio che ciò potenzialmente comporta. Fortunatamente, si sta formando una nuova coalizione europea, SAFENet, per contribuire a sensibilizzare su questa vulnerabilità.

Pertanto, insieme ai nostri amici di SAFENet e iconomy, l'IE.F ha realizzato quello che speriamo sarà un articolo di approfondimento capace di aprire gli occhi su una delle ultime aree ancora poco esaminate dei nostri stack tecnologici comuni. Ci auguriamo che questo articolo dia un contributo prezioso al dibattito pubblico su questo argomento e, in particolare, non vediamo l'ora di vedere la nuova coalizione SAFENet affermarsi come una voce unitaria per questa componente fondamentale dell'ecosistema hardware europeo.

**Clark Parsons**
Amministratore delegato della Innovate Europe Foundation

# Riepilogo Esecutivo

LE INFRASTRUTTURE DIGITALI CRITICHE sono diventate il fronte su cui si combattono i conflitti geopolitici ed economici più determinanti del nostro tempo. I governi degli Stati Uniti, della Cina e di tutto il mondo hanno concluso che l'hardware e il software alla base dei sistemi critici non possono più essere trattati come beni commerciali comuni. Queste catene di approvvigionamento tecnologico sono ora considerate strumenti di competizione geopolitica e di sicurezza nazionale, determinando controlli sulle importazioni, restrizioni di mercato e designazioni di sicurezza un tempo ritenute misure impensabili. L'aumento degli attacchi informatici a sostegno statale contro le infrastrutture critiche ha rafforzato questo cambiamento, trasformando la sicurezza dei sistemi digitali in una questione di difesa nazionale e sovranità.

Eppure l'Unione Europea non è riuscita ad adattarsi a questa nuova realtà strategica. I suoi mercati rimangono aperti alle importazioni di hardware e software che creano dipendenze strategiche e vulnerabilità in materia di sicurezza nelle infrastrutture critiche, minando al contempo le stesse catene di approvvigionamento digitali dell'Europa. Ciò che è più preoccupante è che alcuni degli strati più fondamentali dell'infrastruttura digitale europea rimangono in gran parte al di fuori dell'ambito di una politica significativa in materia di sovranità e sicurezza della catena di approvvigionamento.

Nel corso dell'ultimo decennio, l'Unione Europea ha costruito uno dei quadri normativi più ambiziosi al mondo in materia di regolamentazione digitale e sicurezza informatica. Il Regolamento Generale sulla Protezione dei Dati, il Data Act, la Direttiva sulle apparecchiature radio, l'AI Act, la Direttiva NIS2, il Cyber Resilience Act e il 5G Cybersecurity Toolbox affrontano ciascuno aspetti distinti di come i prodotti, i servizi e le infrastrutture digitali siano regolati nel mercato unico. Nel loro insieme, questi strumenti riflettono **un consenso politico conquistato a fatica, secondo cui i sistemi digitali critici richiedono una governance attiva.**

All'interno di questa architettura, tuttavia, la dimensione della catena di approvvigionamento relativa a un livello critico dell'infrastruttura continua a essere affrontata in modo insufficiente. I **router e i dispositivi gateway per uso domestico** installati in centinaia di milioni di abitazioni europee, piccole e medie imprese, amministrazioni pubbliche, istituti scolastici e strutture sanitarie, ovvero l'hardware fisico attraverso il quale scorre circa **il 93% del traffico Internet europeo**, operano in gran parte al di fuori del più ampio quadro di sovranità e sicurezza della catena di approvvigionamento dell'UE. Mentre l'Europa adottava normative in materia di sovranità del cloud e delle catene di approvvigionamento dei semiconduttori, il primo e l'ultimo hop hardware, in senso letterale, dell'attività digitale europea sono diventati un punto cieco critico della catena di approvvigionamento. Installati in centinaia di milioni di abitazioni e aziende europee e forniti direttamente dagli ISP senza che i consumatori possano scegliere il produttore, questi dispositivi si trovano, senza essere sottoposti ad alcun controllo, al centro dell'infrastruttura digitale europea. Considerati affidabili per default e invisibili nella pratica, rappresentano un potenziale cavallo di Troia che nessun quadro coordinato di sicurezza della catena di approvvigionamento affronta attualmente.

Il presente articolo sostiene che i dispositivi di rete dei clienti, che comprendono router, gateway domestici, dispositivi Wi-Fi mesh e ripetitori, rappresentino la **lacuna più evidente nell'architettura della sovranità digitale dell'UE** e che colmarla sia una delle misure politiche a più basso attrito e maggiore leva di cui dispongono la Commissione e gli Stati membri nell'attuale ciclo legislativo.

La questione in esame si fonda su quattro pilastri: la portata e la centralità dei router, che gestiscono la stragrande maggioranza del traffico Internet europeo; un mercato concentrato in cui i produttori cinesi detengono il 37% delle apparecchiature di rete domestiche nell'Unione Europea; i rischi documentati per la sicurezza informatica derivanti da botnet, backdoor nel firmware e dagli obblighi imposti dalla Legge nazionale cinese sull'intelligence; e una crescente incoerenza normativa, data la disponibilità dell'Europa ad agire contro fornitori ad alto rischio in altri settori hardware critici.

Per colmare questa lacuna, l'Unione Europea non è priva di capacità normativa né di strumenti analitici. Esiste già un'architettura robusta incentrata sulla sicurezza delle infrastrutture digitali. Gli strumenti attuali e futuri affrontano i requisiti di base in materia di sicurezza informatica, i rischi legati alla catena di approvvigionamento, le preferenze in materia di appalti e la resilienza delle infrastrutture critiche in una vasta gamma di settori e tecnologie. Come illustrato in dettaglio nel presente artico-

lo, tale architettura non ha finora affrontato in modo adeguato i rischi strategici e quelli legati alla catena di approvvigionamento associati alle apparecchiature di rete domestiche e delle PMI. L'Europa ha dimostrato, in modo particolarmente evidente attraverso il "5G Cybersecurity Toolbox", di sapere come affrontare questo problema. La domanda è perché non lo abbia ancora fatto.

La necessità di un intervento normativo è ulteriormente rafforzata dal sentimento dell'opinione pubblica. I dati provenienti da recenti sondaggi condotti negli Stati membri dell'UE mostrano un netto cambiamento nell'opinione pubblica contro l'influenza dei fornitori di tecnologia stranieri sulle infrastrutture digitali europee. Gli stessi cittadini che esprimono tale scetticismo ignorano in gran parte che il router installato nelle loro abitazioni dal proprio fornitore di servizi Internet (ISP) potrebbe essere prodotto proprio dalle aziende di cui diffidano. Una volta colmato tale divario, attraverso le misure di trasparenza raccomandate di seguito, la logica politica a sostegno di ulteriori azioni diventerà molto difficile da ignorare. L'opinione pubblica è già un passo avanti rispetto al quadro normativo.

Le questioni individuate nel presente articolo indicano quattro ambiti in cui le istituzioni europee e i governi degli Stati membri possono intervenire, ciascuno dei quali riflette una leva diversa, un attore diverso e un esito positivo diverso per l'Unione europea.

- La **trasparenza** è il punto di partenza meno costoso e quello più immediatamente realizzabile attraverso strumenti già in vigore. Rendere obbligatoria la divulgazione dell'origine dell'hardware, della giurisdizione del firmware e della responsabilità del canale di aggiornamento per tutti i dispositivi di rete immessi sul mercato dell'UE, compresi quelli forniti dagli ISP e quelli white label, crea la base informativa senza la quale la riforma degli appalti e la governance della catena di approvvigionamento non possono funzionare. Gli ISP dovrebbero essere tenuti a comunicare chiaramente la provenienza agli abbonati, e un'iniziativa coordinata di sensibilizzazione pubblica attraverso l'ENISA dovrebbe colmare il divario tra ciò di cui i cittadini dichiarano di diffidare e ciò che, inconsapevolmente, hanno installato nelle loro case.

- La **riforma degli appalti** è la leva più diretta sul lato della domanda attualmente disponibile. L'applicazione dei requisiti "Buy Trusted" alle autorità pubbliche, agli operatori di infrastrutture critiche e agli enti finanziati con fondi pubblici, supportata da una base di certificazione attenta alla catena di approvvigionamento per i router forniti dagli ISP nell'ambito del Quadro europeo di certificazione per la sicurezza informatica, rimodellerebbe gli incentivi di mercato senza attendere un nuovo strumento legislativo orizzontale. Incentivi strutturati alla sostituzione, sul modello di quelli utilizzati per l'eliminazione graduale dei prodotti Huawei nel 5G, dovrebbero sostenere i settori prioritari nella transizione verso l'abbandono dell'hardware ad alto rischio.

- La **governance della catena di approvvigionamento** rappresenta l'opzione strutturalmente più significativa, e le condizioni istituzionali per agire esistono già. In primo luogo, il prossimo trilogo sul Cybersecurity Act (CSA2) rappresenta un'opportunità concreta per includere i dispositivi di rete domestici nel dibattito sui rischi della catena di approvvigionamento. Parallelamente, il gruppo di cooperazione NIS ha il mandato conferito dalla NIS2 per dare priorità a una valutazione coordinata dei rischi della catena di approvvigionamento dei router, e il "5G Cybersecurity Toolbox" fornisce già il modello operativo per ciò che tale valutazione dovrebbe produrre: una metodologia comune di valutazione dei rischi e un meccanismo di designazione dei fornitori ad alto rischio applicabile in tutti gli Stati membri.

- La **capacità industriale** è la condizione a lungo termine. Gli investimenti attraverso i quadri InvestEU e IPCEI, combinati con l'armonizzazione della libertà di scelta dei router in tutto il mercato unico, rafforzerebbero la capacità produttiva europea ed espanderebbero i segmenti di mercato in cui i produttori europei sono già competitivi.

# 1

# L'AGENDA ANCORA INCOMPIUTA DELLA SOVRANITÀ



L'EUROPA HA COMPIUTO PROGRESSI SIGNIFICATIVI in materia di sovranità digitale nell'ultimo decennio. L'AI Act, il Data Act, il Digital Markets Act, la direttiva NIS2, il Cyber Resilience Act, la proposta di Industrial Accelerator Act e il pacchetto sulla sovranità tecnologica, nonché il 5G Cybersecurity Toolbox, affrontano ciascuno aspetti distinti di come i sistemi digitali sono governati nel mercato unico. Il concetto di EuroStack, ovvero l'insieme stratificato di capacità digitali europee che va dalla connettività alla base fino alle applicazioni al vertice, ha strutturato le più recenti analisi strategiche sull'argomento.

Nel loro insieme, questi strumenti rivelano che la sovranità digitale non è un concetto unico, ma un concetto a più livelli che opera attraverso quattro dimensioni distinte ma che si rafforzano a vicenda. **La sovranità della catena di approvvigionamento** si interroga su chi produca l'hardware e su quali Stati possano legalmente imporre la cooperazione dei produttori. **La sovranità del know-how e della proprietà intellettuale** si interroga sul fatto che le imprese europee mantengano le capacità progettuali e software che determinano l'indipendenza competitiva a lungo termine. **La sovranità della sicurezza** si interroga sul fatto che l'Europa possa difendere i propri sistemi da attacchi informatici, vulnerabilità e sfruttamento criminale provenienti dall'esterno. **La sovranità delle infrastrutture** si interroga se i sistemi già installati in Europa possano essere utilizzati contro di essa dall'interno, come strumento di spionaggio, sabotaggio o coercizione da parte di Stati stranieri. Ciascuna dimensione rafforza le altre, e una debolezza in una di esse si ripercuote sulle restanti. Un programma credibile in materia di sovranità deve quindi affrontare tutte e quattro le dimensioni e farlo a ogni livello dello stack digitale.

La maggior parte del dibattito sulla sovranità digitale, tuttavia, si è concentrata sulla dipendenza dell'Europa dal software degli hyperscaler statunitensi ai livelli superiori dello stack tecnologico digitale. I servizi cloud, i sistemi di intelligenza artificiale e le piattaforme online hanno attirato grande attenzione da parte di Bruxelles e delle capitali degli Stati membri. L'infrastruttura hardware al livello di base, in particolare le apparecchiature di rete destinate ai consumatori e alle PMI attraverso le quali transita effettivamente l'attività digitale europea, è stata trascurata nel dibattito pubblico.

Gli studi strategici più influenti sull'UE, come il rapporto Draghi sul futuro della competitività europea, la relazione del Parlamento europeo sulla sovranità tecnologica europea e le infrastrutture digitali,[1] e la "Bussola per la competitività" della Commissione europea[2] , individuano ciascuno preoccupazioni crescenti in merito alla dipendenza tecnologica, alla concorrenza industriale asimmetrica e all'erosione della sovranità digitale europea.

Più recentemente, le prove emergenti di un "secondo shock cinese"[3] hanno rafforzato tali preoccupazioni e dimostrato che il loro impatto sui settori industriali e tecnologici europei sta diventando sempre più grave. Una recente analisi del Centre for European Reform ha stimato che la sola Germania potrebbe aver già perso più di 400.000 posti di lavoro legati al crollo delle esportazioni verso la Cina, avvertendo al contempo che la sovraccapacità industriale cinese e la crescita delle esportazioni stanno perturbando sempre più i settori strategici in tutta Europa[4] . Nonostante la crescente enfasi sulla sovranità digitale e sulla resilienza industriale, è stata prestata scarsa attenzione normativa al livello di accesso alla rete e alla catena di approvvigionamento dei dispositivi di rete dei clienti.

**Un ecosistema europeo sovrano di cloud e dati continua a essere esposto a rischi qualora i gateway hardware che vi si collegano risultino vulnerabili ad attacchi alla catena di approvvigionamento, all'intercettazione di dati o a interruzioni del servizio realizzate attraverso software controllato da soggetti terzi non appartenenti all'UE.**

1 Il futuro della competitività europea, Commissione europea, disponibile all'indirizzo: https://commission.europa.eu/topics/competitiveness/draghi-report_en; Relazione sulla sovranità tecnologica e delle infrastrutture digitali, Parlamento europeo, disponibile all'indirizzo: https://www.europarl.europa.eu/doceo/document/A-10-2025-0107_EN.html

2 Bussola per la competitività, Commissione europea, disponibile all'indirizzo: https://commission.europa.eu/topics/competitiveness/competitiveness-compass_it

3 Deutschland ist das Epizentrum des zweiten China-Schocks, di Handelsblatt, disponibile su: https://www.handelsblatt.com/politik/deutschland/china-deutschland-ist-das-epizentrumdes-zweiten-china-schocks-01/100226122.html

4 China shock 2.0: il costo dell'autocompiacimento della Germania, Centre for European Reform, disponibile all'indirizzo: https://www.cer.eu/sites/default/files/pb_BS_ST_china_shock_2.0_18.5.26.pdf

Le conseguenze di questa svista sono significative. I router domestici e delle PMI costituiscono un'infrastruttura di massa e di lunga durata, installata in oltre 100 milioni di famiglie europee e in decine di milioni di piccole e medie imprese. Rappresentano inoltre il livello più esposto della catena di approvvigionamento delle telecomunicazioni, al quale attualmente non si applica alcun quadro coordinato a livello UE. Il core 5G, sebbene ancora imperfettamente protetto in termini di implementazione, è stato sottoposto almeno dal 2019 a un approccio comune di classificazione dei rischi e a una responsabilità politica a livello UE e nazionale.

Il livello dei dispositivi di rete occupa una posizione insolita nel panorama normativo. Si tratta contemporaneamente di un prodotto di consumo e di un elemento di infrastruttura digitale critica, venduto attraverso canali al dettaglio e di fornitori di servizi Internet (ISP) frammentati, in cui le considerazioni di costo commerciale hanno storicamente avuto la precedenza sulla sicurezza della catena di approvvigionamento. A differenza delle apparecchiature di rete professionali, questi dispositivi sono nelle mani degli utenti finali, i quali hanno un legittimo interesse a scegliere i propri dispositivi, e qualsiasi risposta normativa dovrebbe ampliare tale libertà anziché limitarla. Allo stesso tempo, la portata della diffusione e l'assenza di un quadro coordinato a livello UE comportano che milioni di dispositivi prodotti da entità soggette alla giurisdizione di Stati stranieri siano installati nelle abitazioni e nelle aziende europee senza alcun meccanismo per valutare o mitigare il rischio che rappresentano.

Il presente articolo analizza le complessità e le attuali vulnerabilità del livello dei dispositivi di rete, esaminando perché i router sono importanti in quanto infrastrutture critiche per la sicurezza, come è strutturato il mercato attuale, quale sia il quadro delle minacce e quale slancio normativo già esista che possa essere esteso per colmare questa lacuna. Si avvale del precedente legislativo del "5G Toolbox" e di un modello di azione riscontrabile in numerosi altri settori per sostenere che i router rappresentano il prossimo passo logico e necessario nell'agenda della sovranità europea.

Le condizioni politiche per agire sono insolitamente favorevoli. La decisione della Commissione del maggio 2026 di sospendere i finanziamenti dell'UE a progetti che utilizzano inverter solari provenienti da giurisdizioni ad alto rischio[5] , citando il rischio esplicito di una manipolazione coordinata del firmware da remoto che causi blackout su scala di rete, stabilisce sia il precedente giuridico-politico sia la volontà istituzionale di estendere una logica equivalente alle infrastrutture di rete. La proposta di legge sulla sicurezza informatica Cybersecurity Act 2[6] e la legge sull'acceleratore industriale puntano nella stessa direzione a livello legislativo: la prima introducendo un quadro orizzontale di sicurezza della catena di approvvigionamento delle TIC che crea un'argomentazione diretta per includere le apparecchiature di rete nell'ambito di applicazione, la seconda affrontando gli svantaggi economici che i produttori europei devono affrontare rispetto ai concorrenti sostenuti da sussidi statali. Entrambi i dossier politici rappresentano un'opportunità concreta per garantire che le apparecchiature di rete domestiche siano esplicitamente riconosciute come settore prioritario. Le condizioni per intervenire sui router non saranno mai più favorevoli di quanto lo siano ora.

Questo slancio trova il suo esempio più chiaro nel "Tech Sovereignty Package"[7] , che riunisce cloud, IA, semiconduttori e data center sotto un unico quadro di sovranità. Si tratta di un'iniziativa di grande rilievo, che il presente articolo accoglie con favore. Ma è anche, ancora una volta, un quadro che tralascia le apparecchiature di rete domestiche. I semiconduttori sovrani richiedono vie di trasporto protette. Le infrastrutture cloud sovrane dipendono da punti di accesso resilienti. L'IA sovrana può espandersi solo su un'infrastruttura affidabile. Il livello di rete che collega il tutto rimane trascurato, ed è proprio questa lacuna che il presente articolo intende colmare.

SAFENet (Sovereignty Alliance for European Network Technology), un'alleanza strategica tra le principali aziende europee nel settore delle tecnologie di rete, invita le istituzioni dell'UE e i governi degli Stati membri a considerare i router domestici e delle PMI come infrastrutture critiche, ad applicare la stessa logica della catena di approvvigionamento basata sul rischio già collaudata nel 5G e ad agire prima che la finestra di dipendenza si chiuda.

**5** La Commissione blocca i finanziamenti UE per la tecnologia solare di Huawei, secondo quanto riportato da Politico, disponibile all'indirizzo: https://www.politico.eu/article/commission-blocks-eu-funding-for-huawei-solar-tech

**6** Proposta di regolamento relativa alla legge sulla sicurezza informatica dell'UE, disponibile all'indirizzo: https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-eu-cybersecurity-act

**7** Rafforzare la sovranità tecnologica dell'Europa, Commissione europea, disponibile all'indirizzo: https://digital-strategy.ec.europa.eu/en/policies/eu-tech-sovereignty

# 2
# PERCHÉ I ROUTER SONO IMPORTANTI COME GATEWAY NASCOSTO



## 2.1 L'architettura del traffico Internet europeo

Il dibattito sulle infrastrutture digitali in Europa è dominato da risorse visibili e di alto profilo. Tra queste figurano i data center, i cavi sottomarini, le stazioni base 5G e i satelliti. Il router, un piccolo dispositivo di rete collocato in un corridoio, in un seminterrato o dietro un televisore, non attira quasi nessuna attenzione paragonabile. Eppure il router è, in termini pratici, uno dei singoli componenti hardware più determinanti dell'intero ecosistema digitale europeo. L'immagine nella pagina seguente aiuta a illustrarne il motivo.

L'infrastruttura digitale europea funziona come una struttura a livelli: dalle applicazioni e dalle piattaforme al vertice, passando per i servizi cloud e l'infrastruttura operativa a metà strada, fino al livello fisico alla base. Ogni livello superiore dipende da quello sottostante. E proprio alla base di questa struttura, prima che qualsiasi dato raggiunga un servizio cloud, una piattaforma o un'applicazione, passa attraverso un router. Ogni bonifico bancario, ogni cartella clinica, ogni messaggio privato, ogni accesso ai servizi pubblici, ogni videochiamata dal proprio ufficio a casa, ogni dispositivo domotico, in sostanza tutto ciò che un nucleo familiare o un'azienda invia o riceve su Internet, passa attraverso questo singolo dispositivo. Oltre ai dati, tutte le comunicazioni locali all'interno della rete Wi-Fi o LAN sono gestite dal router, come la stampa di una lettera dal PC alla stampante, l'invio di foto dallo smartphone alla TV, il controllo dei termostati tramite una app, e molti altri esempi.

È il gateway obbligatorio attraverso il quale deve passare tutto il traffico, in entrambe le direzioni, per ogni utente e ogni dispositivo. Un data center compromesso ha ripercussioni sugli utenti di quel data center. Un router compromesso ha ripercussioni su ogni dispositivo, ogni servizio e ogni comunicazione di chiunque vi sia connesso, in modo silenzioso, persistente e senza che l'utente se ne accorga mai.

**Immagine 1: I tre livelli e le tre fondamenta dell'ecosistema digitale**[8]

**Livello 1** **Infrastruttura di intermediazione**

**App specifiche per settore**
Promuovere un design centrato sull'essere umano da parte di start-up locali in settori specifici, ad esempio gestione dell'energia, mobilità e salute

**E-commerce**
Garantire la protezione dei diritti dei consumatori e organizzare standard aperti per le reti di transazioni o API per l'e-commerce

**Ricerca & social**
Investire in un'infrastruttura comune per il sociale e la ricerca, con sostegno al pluralismo algoritmico

**Competenze & mobilità**
Investire nelle competenze digitali, un pool di talenti e migliorare la mobilità per le figure professionali altamente specializzate

**Livello 2** **Infrastruttura software/logica**

**Piattaforme**
Garantire la contendibilità del mercato delle piattaforme digitali come sistemi operativi per dispositivi mobili, desktop e server, cloud, API e browser

**Spazi dati protetti**
Archiviare in modo sicuro i dati personali sensibili e garantire un accesso basato sul consenso

**Pagamenti digitali**
Sviluppare infrastrutture di pagamento pubbliche per promuovere un mercato unico digitale inclusivo

**Identità digitale**
Sviluppare soluzioni di identità digitale con protezione della privacy per l'autenticazione biometrica

**Cloud, IA & dati**
Includere soluzioni cloud sovrane, supportare la capacità computazionale e il deployment dell'IA

**Livello 3** **Infrastruttura hardware/fisica**

**Dispositivi & hardware**
Interfacce fisiche sicure per l'economia digitale, inclusi IoT, hardware e dispositivi connessi

**Reti & cavi**
Favorire un mercato delle telecomunicazioni competitivo e investire nelle reti e nei cavi di nuova generazione (standard 6G e cavi sottomarini)

**Data center**
Aumentare la capacità dei data center e dei servizi cloud e investire nell'edge computing

**Chip & quantistica**
Resilienza nelle catene di approvvigionamento digitali, inclusi i semiconduttori, e ricerca e sviluppo critica nel settore quantistico

**CRM, energia & acqua**
Garantire un accesso sostenibile e diversificato alle materie prime critiche (CRM), all'approvvigionamento di energia rinnovabile e all'acqua

8 Il «modello europeo» – Un progetto per riprendere il controllo del nostro futuro digitale, pagina 17, disponibile all'indirizzo https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5251254&download=yes Basato su "The Technology Stack" di Gautam Kamath, ECDPM, 2025



Sulla base dei dati raccolti dalla Bundesnetzagentur, dal rapporto "State of Wi-Fi" di ASSIA e dall'analisi della GSMA,[9] i router e i dispositivi gateway domestici gestiscono circa il 93% di tutto il traffico dati Internet europeo. Le reti mobili, oggetto di un'intensa attenzione normativa e di significativi investimenti pubblici, rappresentano il restante 7%.

**I router trasportano il 93% del traffico Internet europeo. L'attenzione normativa loro dedicata non è affatto proporzionata al loro ruolo nell'economia digitale.**

## 2.2 Cosa fanno realmente i router

Un router per uso domestico di ultima generazione, o un gateway domestico, fa molto di più che instradare pacchetti e informazioni sensibili. È il centro nevralgico dell'attività digitale di nuclei familiari e PMI: gestisce le reti Wi-Fi, coordina i dispositivi Smart Home, gestisce la telefonia VoIP, applica il controllo genitori e il filtraggio di rete e, in un numero crescente di casi, elabora il traffico associato al lavoro da remoto, alla telemedicina e ai servizi pubblici digitali. In termini funzionali, si tratta di un piccolo server esposto costantemente alla rete Internet pubblica e connesso continuamente alla vita digitale più sensibile di un utente.

Il punto critico è che il router lavora ininterrottamente, con accesso costante a tutti i dati che transitano sulla rete. Un'applicazione browser può essere sottoposta a verifica, aggiornata o sostituita in pochi minuti. Al contrario, il software del router viene in genere aggiornato raramente, spesso per nulla, e il dispositivo stesso può rimanere in servizio per un periodo compreso tra i cinque e i dieci anni. A differenza di uno smartphone, che la maggior parte degli utenti sostituisce ogni due o tre anni, l'acquisto di un router è raramente una scelta ponderata. Viene fornito con un contratto con il provider di servizi Internet e rimane in uso fino a quando non si guasta.

9 Calcolo basato sulle seguenti fonti: Bundesnetzagentur; ASSIA: "State of Wi-Fi Reporting", 8 giugno 2021, disponibile all'indirizzo: https://dynamicspectrumalliance.org/wp-content/uploads/2021/06/ASSIA-DSA-Summit-Presentation-v7.8.pdf; GSMA: "The Importance of 6 GHz to Mobile Evolution», settembre 2024, disponibile all'indirizzo: https://www.gsma.com/connectivity-forgood/spectrum/wp-content/uploads/2024/09/GSMA_Mobile-Evolution-in-6-GHz.pdf

Ai fini del presente articolo, è importante considerare i router non come un singolo dispositivo, ma come tre livelli distinti, ciascuno con la propria origine, il proprio proprietario e la propria esposizione a giurisdizioni straniere.

1. **L'hardware fisico** è il dispositivo stesso, assemblato in uno stabilimento di produzione in un determinato Paese.
2. **Il firmware e il sistema operativo** sono il software integrato in quell'hardware, in genere sviluppato dal produttore del marchio o da un produttore a monte responsabile del progetto originale, ed è qui che si concentra la maggior parte dei rischi per la sicurezza.
3. **Il canale di gestione** è il canale remoto attraverso il quale il produttore invia le modifiche al dispositivo dopo l'installazione e che rappresenta un controllo effettivo e continuo sul dispositivo per tutta la sua vita di servizio.

La compromissione di un singolo livello è sufficiente a compromettere l'intero sistema. Ciò implica che non è possibile ottenere sovranità su un router limitandosi a intervenire solo su uno di questi livelli. Un dispositivo assemblato in Europa ma che esegue un firmware sviluppato sotto una giurisdizione estera e che riceve aggiornamenti tramite server controllati all'estero rimane fondamentalmente esposto. Tenendo presente questa architettura, possiamo ora esaminare le tre categorie di rischio che qualsiasi risposta normativa seria dovrà affrontare.

### 2.3 Tre rischi fondamentali

L'architettura a tre livelli descritta sopra (hardware, firmware e canale di aggiornamento) crea tre diverse categorie di rischio, che qualsiasi risposta normativa seria dovrà affrontare.

- **Intercettazione dei dati (livello firmware)**. Il traffico che passa attraverso un router compromesso può essere ispezionato, copiato e reindirizzato. Ciò si applica direttamente al traffico non crittografato e, tramite attacchi più sofisticati a livello di firmware, può potenzialmente interessare anche le comunicazioni crittografate.[10] Poiché il router si trova a monte di ogni dispositivo sulla rete, una singola compromissione offre a un aggressore la visibilità sull'intera attività digitale di una famiglia o di un'azienda.

- **Strumentalizzazione per attacchi informatici (livello hardware e firmware)**. I router compromessi costituiscono l'elemento fondamentale dei botnet, vaste reti di dispositivi dirottati utilizzate per lanciare attacchi Distributed Denial of Service (DDoS), distribuire malware e compiere furti di credenziali su larga scala. Dato che una singola vulnerabilità del firmware può interessare contemporaneamente tutti i dispositivi dello stesso produttore, la concentrazione del mercato amplifica direttamente questo rischio.

- **Kill switch e interruzione delle infrastrutture (livello del canale di aggiornamento)**. È a livello del canale di aggiornamento che questo rischio diventa più acuto. Un produttore soggetto alla giurisdizione di uno Stato straniero mantiene, attraverso il canale di aggiornamento, un controllo effettivo e continuo su ogni dispositivo che abbia mai commercializzato. Un soggetto statale con autorità legale su quell'ISP e/o produttore può, in linea di principio, ordinargli di distribuire un aggiornamento del firmware o di attivare una funzione preinstallata già integrata che disabiliti, interrompa o trasformi in arma milioni di router contemporaneamente.

Proprio perché questi rischi sono strutturali piuttosto che accidentali, la questione di chi produca e fornisca i router europei non è una questione di mercato. È una questione di sicurezza. Comprendere lo stato attuale del mercato europeo dei dispositivi di rete è quindi il punto di partenza necessario per qualsiasi risposta politica seria.

10 ENISA Threat Landscape 2024, Agenzia dell'Unione europea per la sicurezza informatica, ottobre 2024, disponibile all'indirizzo https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024.
ENISA Threat Landscape 2023, Agenzia dell'Unione europea per la sicurezza informatica, ottobre 2023, disponibile all'indirizzo https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023.

# 3
# CHI DOMINA LE RETI EUROPEE



## 3.1 Struttura del mercato dei router

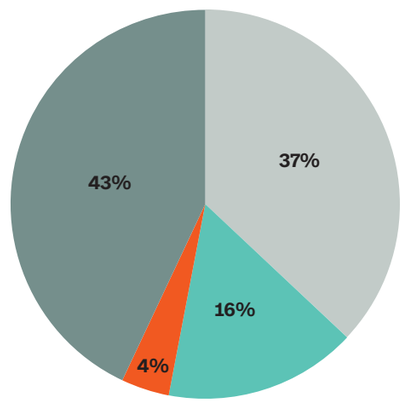
Per comprendere il rischio rappresentato dai router per uso domestico e per PMI è necessario avere un quadro chiaro dell'attuale mercato europeo. I dati raccolti dal sondaggio YouGov Consumer Survey 2025 e integrati dai dati del panel GfK Point-of-Sale[11] forniscono la panoramica più completa attualmente disponibile.

I risultati evidenziano un mercato in cui i produttori con sede nella Repubblica Popolare Cinese detengono una quota sostanziale, affiancati da fornitori europei e taiwanesi. I produttori dell'UE e altri produttori rappresentano circa il 43% del totale dei router e dei ripetitori presenti nelle famiglie europee, con aziende che spaziano da quelle che operano su larga scala nel canale degli ISP, come Sagemcom e Vantiva, a marchi che competono direttamente nei segmenti al dettaglio e specializzati, tra cui FRITZ!, Devolo, Lancom, Icotera, MikroTik e Teltonika. I produttori cinesi, tra cui ZTE, Huawei, TP-Link, Xiaomi e Tenda, rappresentano circa il 37% dei dispositivi, corrispondente a una base installata su circa 95 milioni di famiglie europee. I fornitori taiwanesi, tra cui Sercomm, Arcadyan, ASUS, D-Link e Zyxel, detengono un ulteriore 16%, mentre la presenza degli Stati Uniti è contenuta al 4% ed è concentrata sul canale retail. Nel complesso, i fornitori extra-UE coprono oltre metà di tutte le installazioni di router e ripetitori in Europa.

Dietro a queste cifre relative alle quote di mercato si nasconde una dinamica di distribuzione che la maggior parte dei consumatori europei non vede mai. Il modo in cui un router arriva in una casa determina, in gran parte, di chi sarà quel router.

**11** Raccolta basata sul sondaggio YouGov sui consumatori 2025 (DE, AT, CH, NL, IT, UK); database interno FRITZ! relativo ai dispositivi CPE degli ISP; dati del panel GfK sui punti vendita 2025; dati del panel Context sui punti vendita per ES, FR, BE, DK, NO, SE, FI (07/2023–06/2024). Ipotesi fissa applicata agli altri Stati membri dell'Unione europea. I dati sono indicativi.

**Router e ripetitori nell'UE per regione di produzione**




Fonte: Sondaggio YouGov 2025 in DE, AT, CH, NL, IT e UK – Per i router degli ISP, la ripartizione per Paese di produzione è stata determinata utilizzando un database interno sui dispositivi CPE degli ISP.
Altri paesi (FR, PL, ES, GR, CZ, SE, NO, DK, FI) – Per i router degli ISP, la ripartizione per Paese di produzione è stata determinata utilizzando un database interno sui dispositivi CPE degli ISP.
Dati GFK sulle quote di mercato dei ripetitori

| Origine dei produttori | Produttori principali |
|---|---|
| **Europei** | Sagemcom e Vantiva su larga scala nel canale ISP; FRITZ!, Devolo, Lancom, Icotera, MikroTik, Teltonika e altri produttori nazionali nei segmenti retail e specializzati |
| **Repubblica Popolare Cinese** | ZTE, Xiaomi, Huawei, TP-Link, Tenda, Reyee con white-label per gli ISP e come brand consumer nel settore retail |
| **Taiwan** | Sercomm, Arcadyan, Compal, ASUS, D-Link, Zyxel, spesso con white-label per gli ISP e alcuni anche come brand consumer |
| **Stati Uniti** | Principalmente Netgear, eero (Amazon), concentrati nel segmento retail. Anche Cisco, Linksys, Ubiquiti, Belkin, Google e Starlink sono fornitori. |



## 3.2 Come i router raggiungono i consumatori europei

Le apparecchiature di rete per ambienti domestici e PMI raggiungono gli utenti europei attraverso due canali di distribuzione distinti e la differenza tra questi determina sia il profilo di sicurezza della base installata sia le leve politiche disponibili per affrontarlo.

Il primo canale è quello della fornitura del **provider di servizi Internet (ISP)**. Nella maggior parte dei mercati europei, la maggioranza dei nuclei familiari riceve il proprio router principale come parte dell'abbonamento a banda larga. Il dispositivo viene selezionato dall'ISP tramite approvvigionamento commerciale, installato al momento dell'attivazione e in genere rimane in uso per tutta la durata del contratto, spesso per anni. Il consumatore non ha alcun ruolo nella scelta dell'apparecchiatura e, in molti casi, non è a conoscenza di chi abbia prodotto il dispositivo installato nella propria abitazione.

Il secondo canale è **l'acquisto al dettaglio** (retail). I consumatori e le piccole imprese acquistano router, sistemi mesh e ripetitori direttamente dai rivenditori di elettronica, dai marketplace online e dai venditori specializzati. Sebbene le informazioni sulla provenienza della catena di approvvigionamento e sulla giurisdizione del produttore non siano sistematicamente disponibili nemmeno in questo canale, il consumatore è almeno parte integrante del processo decisionale, tende a impegnarsi in modo più attivo e mantiene un rapporto diretto con il dispositivo e il suo produttore.

**Questi due canali producono esiti di mercato sistematicamente diversi.** Laddove la scelta del consumatore è più presente, in particolare nei mercati che hanno adottato una legislazione specifica sulla libertà di scelta dei router, i consumatori manifestano una maggiore soddisfazione per le proprie apparecchiature di rete e scelgono in misura sproporzionata produttori con sede in Europa.

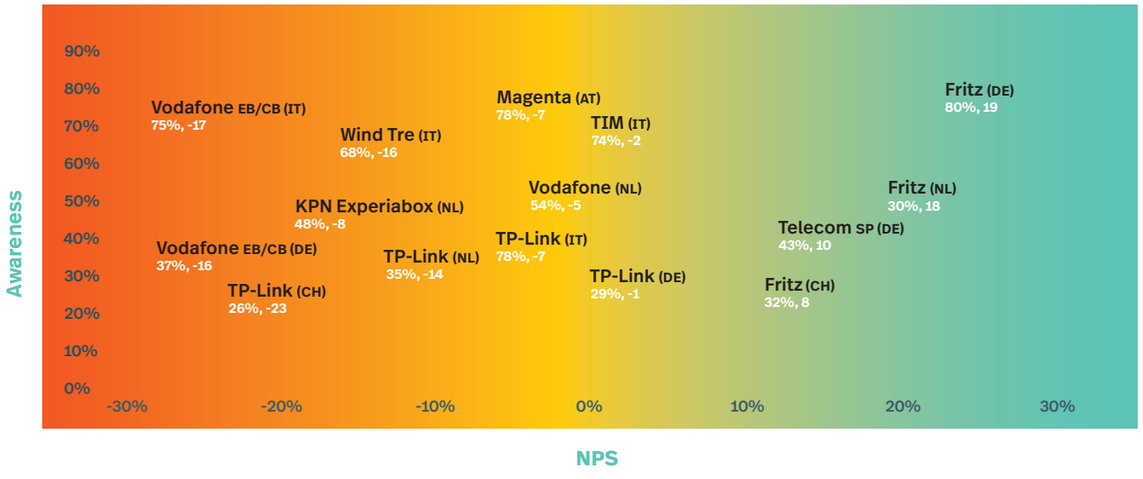
Il diritto europeo riconosce già il principio secondo cui i consumatori dovrebbero poter scegliere le proprie apparecchiature terminali. L'articolo 3, paragrafo 1, del regolamento sui diritti degli utenti ai servizi di comu-

nicazione elettronica[12] sancisce il diritto degli utenti finali di utilizzare apparecchiature terminali di propria scelta quando si connettono a una rete di comunicazioni elettroniche. Gli Stati membri hanno attuato questo principio con gradi di incisività diversi. La legge tedesca del 2016 sulla libera scelta delle apparecchiature terminali di telecomunicazione, nota come "Freie Routerwahl"[13] , ha stabilito l'attuazione nazionale più rigorosa, imponendo agli ISP di consentire ai clienti di utilizzare il proprio router e di fornire le credenziali di accesso necessarie a tal fine. L'Italia ha adottato disposizioni analoghe nel 2018[14] , e norme simili si applicano con ambito di applicazione variabile in altri Stati membri. Altri mercati europei, tra cui il Regno Unito, non hanno attuato tutele equivalenti.

Esaminando i dati relativi ai brand insieme alla struttura del mercato, emerge un quadro chiaro. Come illustra il grafico nella pagina seguente, i brand scelti dai consumatori nei mercati in cui vige un'effettiva libertà di scelta del router registrano costantemente Net Promoter Score positivi, mentre i dispositivi forniti dagli ISP e quelli prodotti in Cina si collocano in territorio NPS negativo, indipendentemente dal loro livello di notorietà. I brand che i consumatori scelgono attivamente quando hanno la possibilità di scegliere non solo godono di maggiore fiducia, ma hanno anche prevalentemente sede in Europa. Laddove la decisione di acquisto spetta al consumatore, la soddisfazione e la preferenza per i produttori europei vanno di pari passo.

I dati evidenziano un aspetto che i soli dati sulla struttura di mercato non riescono a cogliere, ovvero un settore europeo resiliente e apprezzato dai consumatori, in grado di competere efficacemente **laddove le condizioni lo consentono**. In presenza di una scelta autentica e di informazioni sufficienti, i consumatori europei propendono per i prodotti europei. Gli ISP non agiscono in violazione della legge. Stanno prendendo decisioni di acquisto razionali all'interno di un quadro che non richiede loro di valutare la giurisdizione del produttore, la provenienza del firmware o i rischi legati alla catena di approvvigionamento. Le raccomandazioni esposte in questo articolo sono volte a garantire che consumatori, ISP e istituzioni pubbliche operino tutti sulla base delle stesse informazioni relative ai dispositivi che entrano nelle case europee e che i produttori europei e di Paesi terzi competano in un quadro di reale trasparenza. Laddove tali informazioni sono disponibili e i consumatori possono agire di conseguenza, il mercato ha già dimostrato da che parte propendono.

**Immagine 2: Consapevolezza del brand vs. Net Promoter Score per produttore di router**




**Fonti:** Awareness: sondaggio condotto da M&R, 2024; NPS: sondaggio condotto da YouGov, 2025

Tuttavia, la resilienza dei produttori europei nei segmenti in cui competono oggi non deve essere confusa con una sicurezza strutturale. Le attuali tendenze di mercato, guidate dalle dinamiche dei prezzi e dal sostegno industriale esaminati nella sezione seguente, stanno erodendo attivamente le condizioni che rendono possibile tale concorrenza. Se tali tendenze dovessero continuare senza controllo, il margine di tempo in cui le alternative europee rimangono praticabili si ridurrà, e con esso la libertà di scelta dei consumatori a cui gli europei tengono tanto.

12 Regolamento (UE) 2015/2120, disponibile all'indirizzo: https://eur-lex.europa.eu/eli/reg/2015/2120/oj/eng

13 Freie Routerwahl, Ministero federale dell'Economia e dell'Energia della Repubblica Federale di Germania, disponibile all'indirizzo https://www.bundeswirtschaftsministerium.de/Redaktion/DE/Artikel/ Digitale-Welt/freie-routerwahl.html

14 Delibera 348/18/CONS, Autorità per le garanzie nelle comunicazioni, disponibile all'indirizzo https://www.agcom.it/provvedimenti/delibera-348-18-cons

### 3.3 Un mercato in evoluzione

Le quote di mercato sopra descritte non rappresentano un quadro statico. Esse riflettono un mercato che si sta attivamente spostando verso una maggiore concentrazione nelle mani dei produttori con sede nella Repubblica Popolare Cinese, e le dinamiche che guidano tale spostamento stanno accelerando.

I produttori cinesi di dispositivi di rete sono oggetto di indagini per aver beneficiato di prezzi sovvenzionati dal governo cinese che hanno influenzato in modo sleale il mercato a scapito dei produttori occidentali di apparecchiature di comunicazione. Il Dipartimento di Giustizia degli Stati Uniti ha avviato un'indagine penale antitrust per verificare se TP-Link abbia praticato prezzi predatori vendendo router al di sotto del costo[15] , una pratica di determinazione dei prezzi che, se confermata, rifletterebbe quel tipo di sostegno statale strutturale che i produttori europei e taiwanesi finanziati con capitali privati non possono assorbire né eguagliare. Se confermata, la conseguenza sarebbe una graduale esclusione dei produttori europei e di quelli non europei di fiducia da un segmento che costituisce il fondamento dell'economia digitale.

Tale esclusione è ora aggravata da pressioni esterne. A seguito della decisione della Commissione Federale delle Comunicazioni degli Stati Uniti del marzo 2026 di vietare tutti i router di consumo fabbricati all'estero per motivi di sicurezza nazionale, i produttori cinesi esclusi dal mercato statunitense rappresentano una notevole capacità industriale che ora non ha altra destinazione se non quella di altri mercati aperti. Gli elevati dazi statunitensi sulle importazioni dalla Cina hanno già portato a un aumento misurabile delle esportazioni cinesi verso l'UE, con i mercati europei che assorbono la capacità reindirizzata in una vasta gamma di categorie di prodotti.[16] Se l'Europa non prende coscienza della propria vulnerabilità e non interviene, diventerà la destinazione naturale di un'ondata di router cinesi che persino gli Stati Uniti hanno ritenuto un rischio per la sicurezza troppo elevato per consentirne l'uso sulle proprie reti. La domanda è: cosa comporta effettivamente tale vulnerabilità per la sicurezza europea? Questo è l'argomento della sezione successiva.

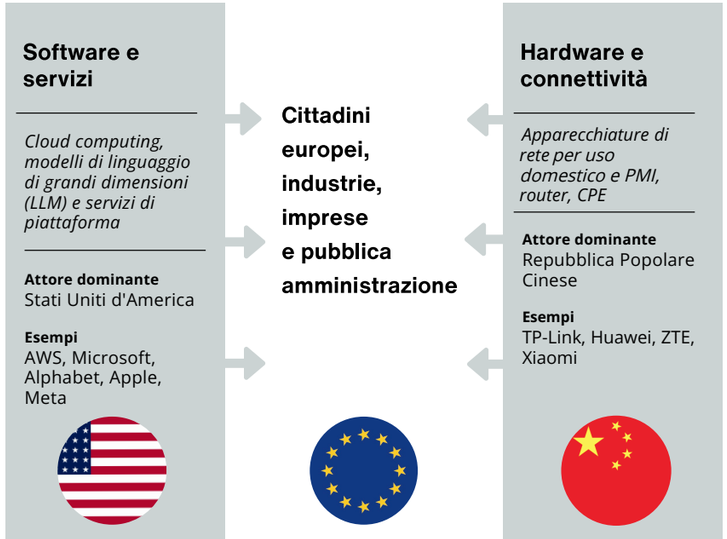
**15** Bloomberg, Il produttore di router TP-Link è oggetto di un'indagine penale antitrust negli Stati Uniti, 24 aprile 2025, disponibile all'indirizzo https://www.bloomberg.com/news/articles/2025-04-24/router-maker-tp-link faces-us-criminal-antitrust-investigation

**16** CEPR VoxEU, Tariffe, flussi commerciali, effetti di diversione ed esportazioni cinesi verso l'UE, febbraio 2026, disponibile all'indirizzo cepr.org/voxeu/columns/tarifs-trade-fows-diversion-efects-and chinas-exports-eu

# 4
# IL QUADRO DELLE MINACCE

COME GIÀ DISCUSSO IN PRECEDENZA, l'Europa si trova in una posizione strutturalmente vulnerabile nella catena delle infrastrutture digitali. Ai livelli superiori, il cloud computing, le infrastrutture di intelligenza artificiale e i servizi di piattaforma sono dominati da aziende statunitensi, una dipendenza che ha determinato un decennio di risposte in materia di politica normativa e industriale. A livello di base hardware, la produzione di apparecchiature di rete per i consumatori è sempre più dominata da aziende con sede nella Repubblica Popolare Cinese. I cittadini europei e le istituzioni europee si trovano tra questi due poli tecnologici extraeuropei, dipendendo da uno per il software e dall'altro per l'hardware attraverso cui tutto ciò transita.

**La doppia dipendenza europea dal software americano e dall'hardware cinese**




Le sezioni che seguono esaminano cosa comporti, per la sicurezza e la sovranità europee, la concentrazione di mercato dei produttori di hardware con sede in Cina documentata nella sezione precedente, in tre dimensioni distinte ma interconnesse, che coprono le minacce convenzionali alla si-

curezza informatica, i rischi geopolitici e a livello statale, nonché i rischi strutturali per la sovranità industriale europea.

### 4.1 Sicurezza informatica. Botnet, vulnerabilità e sfruttamento a fini criminali

I router prodotti da qualsiasi fornitore possono contenere, e di fatto contengono, vulnerabilità. L'ENISA ha costantemente identificato router, dispositivi di rete e altre infrastrutture di rete connesse a Internet come superfici di attacco significative nel panorama delle minacce informatiche in Europa[17] . I database pubblici sulle vulnerabilità, tra cui il programma MITRE CVE[18] e il National Vulnerability Database (NVD) degli Stati Uniti[19], documentano ulteriormente un flusso costante di vulnerabilità rese note che interessano router e apparecchiature di rete integrate di diversi fornitori.

Un prossimo studio della Gesellschaft für Informatik (GI), il principale ente professionale tedesco nel campo dell'informatica, fornisce la valutazione delle vulnerabilità a livello di fornitore più dettagliata mai realizzata fino ad oggi per il mercato tedesco. Analizzando l'NVD per il periodo 2020–2025, lo studio ha identificato 2.190 Common Vulnerabilities and Exposures (CVE) univoci che interessano i router dei principali fornitori in Germania: Netgear (USA), D-Link (Taiwan), TP-Link (Cina) e AVM FRITZ! (Germania). La distribuzione è sorprendente. Netgear conta 1016 CVE (46%) e D-Link 955 (44%), mentre TP-Link ne registra 218 (10%). FRITZ!, il produttore tedesco, registra un solo CVE nell'intero periodo di sei anni. La divergenza diventa più marcata se si esamina la gravità. Tra i CVE classificati come critici – quelli con un punteggio CVSS (Common Vulnerability Scoring System) pari o superiore a 9,0, che indicano accesso remoto non autenticato, presa di controllo totale del sistema o esecuzione di codice arbitrario – D-Link ne conta 280 (il 29% del proprio totale), TP-Link ne registra 60 (il 28% del proprio totale) e Netgear 149 (il 15% del proprio totale). Quasi una vulnerabilità su tre segnalata per D-Link raggiunge la classificazione di gravità più elevata. Lo studio rileva che TP-Link, nonostante un numero assoluto di CVE inferiore, presenta una proporzione relativa di vulnerabilità critiche quasi doppia rispetto a Netgear, il che suggerisce debolezze strutturali nei meccanismi di sicurezza fondamentali, quali l'autenticazione e la convalida degli input, piuttosto che difetti accidentali o secondari.

Il rischio specifico associato ai fornitori con un'elevata quota di mercato è quello della concentrazione. Quando l'architettura del firmware di un singolo produttore contiene una vulnerabilità, introdotta per negligenza o deliberatamente, la portata dell'esposizione è proporzionale alla quota di mercato. Una vulnerabilità in un fornitore che controlla dal 20 al 50% delle installazioni di router in Europa offre una potenziale superficie di attacco che abbraccia contemporaneamente decine di milioni di dispositivi connessi. La campagna malware "VPN Filter", attribuita dalle autorità statunitensi e britanniche ad attori statali russi, ha dimostrato proprio questa dinamica attraverso un'unica operazione coordinata che ha compromesso router su piattaforme di diversi fornitori, interessando centinaia di migliaia di dispositivi in 54 Paesi[20] . L'attacco del 2016 all'infrastruttura dei router di Deutsche Telekom, in cui una vulnerabilità nella funzione di gestione remota ha causato il crash di circa 900.000 dispositivi e interrotto la connessione di quasi un milione di clienti[21] , offre un esempio analogo su scala nazionale.

La portata dei crimini informatici basati sui router è notevole. Le botnet create utilizzando router compromessi sono state responsabili di alcuni dei più grandi attacchi DDoS mai registrati, compresi attacchi prolungati contro infrastrutture nazionali critiche, servizi finanziari e sistemi sanitari. La botnet Mirai, che nel 2016 ha temporaneamente compromesso ampie porzioni dell'infrastruttura Internet negli Stati Uniti e in Europa,

17 Panorama delle minacce all'infrastruttura Internet secondo l'ENISA, disponibile all'indirizzo: https://www.enisa.europa.eu/sites/default/files/all_files/Detailed%20Mind%20Map%20for%20Internet%20Infrastructure%20Assets.pdf
18 Disponibile all'indirizzo: https://www.cvedetails.com
19 National Vulnerability Database, disponibile all'indirizzo: https://nvd.nist.gov

20 Avviso US-CERT TA16-288A, Aumento della minaccia DDoS rappresentata da Mirai e altre botnet, Agenzia americana per la difesa informatica, disponibile all'indirizzo https://www.cisa.gov/news-events/alerts/2016/10/14/heightened-ddos-threat-posed-mirai-and-other-botnets
21 Attacco globale a Internet, riportato da Deutsche Welle, disponibile all'indirizzo: https://www.dw.com/en/deutsche-telekom-hack-part-of-global-internet-attack/a-36574934

era costituita principalmente da dispositivi connessi compromessi, tra cui i router rappresentavano una componente significativa[22] ,[23] .

Successive famiglie di botnet, tra cui Meris, Mantis e i loro successori, hanno dimostrato la stessa architettura di vulnerabilità su scala ancora più ampia.

Al di là degli attacchi su larga scala, il controllo di singoli router consente una sorveglianza persistente e mirata. Un router compromesso situato nell'abitazione o nell'ufficio di bersagli di alto profilo, come funzionari governativi, giornalisti, avvocati o dirigenti d'azienda, apre la strada a un accesso duraturo e poco visibile a tutte le attività di rete. A differenza del malware per endpoint, le vulnerabilità dei router a livello di firmware sono estremamente difficili da rilevare e possono sopravvivere ai riavvii di routine dei dispositivi.

Anche il quadro delle minacce si sta evolvendo. Man mano che gli strumenti di intelligenza artificiale diventano sempre più accessibili, aumenta di conseguenza la capacità di sfruttare su larga scala le infrastrutture compromesse. Una botnet composta da milioni di router compromessi, coordinata tramite comandi e controllo assistiti dall'IA, rappresenta una minaccia qualitativamente diversa rispetto alla stessa botnet gestita con mezzi convenzionali. Le capacità dell'IA vengono applicate anche all'individuazione delle vulnerabilità, con l'effetto pratico che il tempo che intercorre tra la scoperta di una vulnerabilità nel firmware di un router e il suo sfruttamento su larga scala si sta riducendo. Il calcolo di sicurezza che si applica oggi si intensificherà con la proliferazione delle capacità di IA, il che rafforza la necessità di agire mentre la concentrazione delle quote di mercato rimane affrontabile attraverso strumenti politici ordinari.

### 4.2 Rischi geopolitici e a livello statale. L'architettura giuridica della dipendenza

I rischi di sicurezza informatica sopra descritti si applicano, in misura variabile, a qualsiasi produttore con pratiche di sicurezza carenti. La preoccupazione legata specificamente ai produttori con sede nella Repubblica Popolare Cinese deriva da una causa strutturale. Il contesto giuridico e politico in cui operano tali aziende crea obblighi che nessuna buona volontà aziendale o accordo contrattuale può superare. Lo studio di GI citato in precedenza, basandosi sulle interviste a esperti, rileva che l'attribuzione in questo ambito è strutturalmente complicata dal fatto che gli stessi gruppi di attori operano spesso contemporaneamente sia come entità criminali sia come operatori guidati dallo Stato, il che complica la distinzione binaria tra crimine informatico commerciale e rischio geopolitico.

La Legge nazionale sull'intelligence (2017) e la Legge sul controspionaggio (2023) della Repubblica Popolare Cinese[24] impongono a tutti i cittadini e alle organizzazioni della Repubblica Popolare Cinese obblighi giuridicamente vincolanti di sostenere, assistere e cooperare con le attività di intelligence dello Stato cinese. Tali obblighi si applicano alle aziende cinesi indipendentemente dal luogo in cui operano. Un produttore di router con sede nella Repubblica Popolare Cinese, che detiene una quota compresa tra il 20 e il 25% del mercato europeo, è, ai sensi della legislazione cinese, un potenziale strumento dei servizi di intelligence statali della Repubblica Popolare Cinese, e tale status riflette un obbligo giuridico che non può essere escluso mediante contratto.

Il caso Huawei ha messo in luce questa preoccupazione nel contesto delle infrastrutture 5G con sufficiente chiarezza da stimolare un'azione politica coordinata in tutta l'Unione Europea e tra i suoi principali alleati. La stessa Huawei è un produttore di router per uso domestico e per le PMI ed è presente nei canali retail e canali ISP europei. L'analisi giuridica che ha sostenuto le restrizioni nei confronti di Huawei per le apparecchiature di rete centrali si applica con la stessa logica ai produttori cinesi di router per uso domestico e per le PMI. La questione rilevante riguarda il fatto che il quadro giuridico che disciplina un produttore crei una condizione strutturale di potenziale costrizione che sia incompatibile con i requisiti di sicurezza delle infrastrutture critiche.

22 Avviso ufficiale su Mirai, CISA, disponibile all'indirizzo: https://www.cisa.gov/news-events/alerts/2016/10/14/heightened-ddos-threat-posed-mirai-and-other-botnets

23 Che cos'è la botnet Meris?, guida informativa di Akamai su Meris, disponibile all'indirizzo: https://www.akamai.com/glossary/what-is-the-meris-botnet

24 Legge della Repubblica Popolare Cinese sull'intelligence nazionale (2017), articoli 7 e 14; Legge antispionaggio della Repubblica Popolare Cinese (rivista nel 2023), disponibile all'indirizzo: https://www.chinalawtranslate.com/en/national-intelligence-law-of-the-p-r-c-2017

Lo scenario del “kill switch” rappresenta l’espressione più estrema di questo rischio e non è una preoccupazione ipotetica. Come già citato, i produttori cinesi rappresentano complessivamente circa il 37% del mercato europeo complessivo di router e ripetitori, il che significa che un comando firmware coordinato inviato a tale base installata potrebbe interrompere simultaneamente la connettività Internet per decine di milioni di famiglie e PMI europee. Un produttore con sede nella Repubblica Popolare Cinese (RPC) e con un tale livello di presenza sul mercato, soggetto all’autorità statale cinese e che gestisce dispositivi dotati di funzionalità di aggiornamento remoto del firmware, rappresenta un potenziale vettore per un’interruzione coordinata delle infrastrutture su scala nazionale o europea. La decisione della Commissione del maggio 2026 di sospendere i finanziamenti a progetti che utilizzano inverter solari cinesi, citando esplicitamente il rischio di una manipolazione remota coordinata che causi instabilità della rete, dimostra che i responsabili politici europei riconoscono già questo vettore di minaccia come reale e perseguibile.

Sono state documentate ripetutamente operazioni informatiche sponsorizzate a livello statale che sfruttano l’infrastruttura dei router. L’avviso congiunto del 2023 emesso dalla NSA, dalla CISA e dall’FBI statunitensi, insieme ai partner del gruppo Five Eyes, ha attribuito una campagna prolungata di sfruttamento dei router ad attori legati allo Stato cinese. È emerso che la campagna “Volt Typhoon” del 2024 aveva preposizionato codice dannoso all’interno delle infrastrutture critiche degli Stati Uniti attraverso dispositivi di perimetro di rete compromessi.[25] Nel 2025, il ministero degli Esteri ceco ha pubblicamente attribuito un attacco informatico prolungato ad attori statali della Repubblica Popolare Cinese. Nello stesso anno, le autorità statunitensi hanno confermato che la campagna “Salt Typhoon”, attribuita a hacker statali della Repubblica Popolare Cinese, aveva compromesso le infrastrutture di telecomunicazione in almeno 80 Paesi.[26]

**25** Avviso congiunto sulla sicurezza informatica – Attori informatici sponsorizzati dallo Stato della Repubblica Popolare Cinese sfruttano i fornitori di rete e i dispositivi. NSA, CISA, FBI e partner, disponibile all’indirizzo: CISA – Attori informatici sponsorizzati dallo Stato della Repubblica Popolare Cinese sfruttano i fornitori di rete e i dispositivi (AA22-158A)

**26** Autorità statunitensi: hacker cinesi nel settore delle telecomunicazioni attivi in 80 paesi, Deutschlandfunk, disponibile all’indirizzo: https://www.deutschlandfunk.de/us-behoerden-chinesische-telekom-hacker-in 80-laendern-aktiv-102.html



È opportuno dedicare una breve nota a Taiwan, dato che i produttori taiwanesi detengono una quota di mercato comparabile. Taiwan opera nell’ambito di un ordine costituzionale democratico e di un sistema giudiziario indipendente, senza alcuna legge equivalente alla Legge nazionale sull’intelligence della Repubblica Popolare Cinese del 2017 che obblighi le aziende private a cooperare segretamente con le operazioni di intelligence statali. Nell’ambito del quadro dell’UE in materia di riduzione dei rischi e sicurezza economica, Taiwan è considerata un partner piuttosto che un rivale sistemico. L’esposizione geopolitica di Taiwan alla Repubblica Popolare Cinese e la prevalenza di firmware di provenienza cinese nei prodotti a marchio taiwanese rimangono fattori da tenere in considerazione; per questo motivo le raccomandazioni della Sezione 7 riguardano la provenienza del firmware e il controllo dei canali di aggiornamento, oltre all’origine dell’assemblaggio dell’hardware.

### 4.3 Sovranità strategica e dimensione della competitività

La terza dimensione del quadro delle minacce è meno immediata ma non per questo meno rilevante. Chi produce l’hardware fisico determina non solo chi si aggiudica il valore economico del mercato dei dispositivi di rete, ma anche chi controlla le fondamenta su cui si basano i livelli del firmware e dei canali di aggiornamento. Perdere il livello hardware significa perdere la capacità di governare i livelli sovrastanti.

I produttori europei di router competono in un mercato aperto contro fornitori le cui strutture di costo riflettono un sostegno statale costante piuttosto che la sola concorrenza di mercato. La valutazione del Rhodium Group del maggio 2025 ha concluso che la strategia della Cina è stata quella di estendere sistematicamente il proprio dominio nei settori manifatturieri avanzati attraverso una combinazione di sussidi statali, accesso preferenziale al mercato ed esclusione dei concorrenti stranieri dal mercato interno.[27] La conseguenza per i produttori europei di dispositivi di rete è una graduale esclusione da un mercato che è sia economicamente significativo che strategicamente critico.

**27** “Was Made in China 2025 Successful”, redatto per la Camera di commercio degli Stati Uniti, disponibile all’indirizzo rhg.com/wp-content/uploads/2025/05/Was-MIC25-Successful.pdf

La divergenza tra gli approcci statunitense ed europeo aggrava questa dinamica. I produttori cinesi esclusi dal mercato statunitense hanno intensificato la loro attenzione sul mercato europeo, accelerando proprio quella dinamica di concentrazione che crea rischi per la sicurezza. L'infrastruttura europea sta diventando l'eccezione globale, l'unica grande economia sviluppata che mantiene le porte aperte ai fornitori esclusi altrove per motivi di sicurezza. L'Europa ha ancora una presenza significativa nel mercato dei router. Ma questa finestra non rimarrà aperta a tempo indeterminato.

L'analisi di mercato del segmento tedesco dei router contenuta nello studio di GI fornisce un contrappunto illustrativo. In Germania, dove l'abolizione nel 2016 dell'obbligo di fornitura del router ha conferito ai consumatori il diritto legale di scegliere il proprio router, i produttori europei competono con successo sulla base dei meriti dei propri prodotti. Aziende come Devolo, FRITZ! e Lancom mantengono posizioni solide nei segmenti retail e specializzati, mentre il principale fornitore di banda larga, Deutsche Telekom, detiene solo il 19% del mercato dei router nonostante controlli oltre il 40% delle connessioni a banda larga. Questa asimmetria dimostra che, laddove vige la libertà di scelta dei consumatori, i produttori europei possono mantenere e difendere una quota di mercato significativa contro fornitori che competono esclusivamente sul prezzo. Al contrario, nei segmenti e nelle giurisdizioni in cui la libertà di scelta dei consumatori non è garantita, i vantaggi strutturali dei concorrenti sovvenzionati dallo Stato si traducono più direttamente in uno spostamento del mercato.

Le tre dimensioni di rischio descritte in questa sezione, considerate nel loro insieme, costituiscono un profilo che i responsabili politici europei hanno già affrontato in passato e hanno già dimostrato di saper gestire. L'obbligatorietà giuridica nei confronti dei produttori stranieri, la concentrazione della quota di mercato nelle mani di fornitori provenienti da un'unica giurisdizione non alleata e la difficoltà strutturale di allentare la dipendenza una volta che questa si è consolidata erano proprio le condizioni che hanno plasmato il dibattito sulle infrastrutture di rete 5G tra il 2018 e il 2020. L'Europa ha affrontato tale sfida attraverso un quadro coordinato e basato sul rischio che si è dimostrato sia praticabile che efficace.



Le sezioni che seguono esaminano come tale quadro sia stato costruito, come sia stato successivamente esteso ad altri settori e perché lo stesso approccio applicato ai router porti alla stessa conclusione.

# 5
# L'ANALOGIA CON IL 5G E UN MODELLO DI AZIONE

## 5.1 Come l'UE ha affrontato la sicurezza della catena di approvvigionamento del 5G

L'approccio dell'Unione Europea alla sicurezza della catena di approvvigionamento del 5G rappresenta il precedente più rilevante per l'azione raccomandata dal presente articolo. Costituisce inoltre una dimostrazione concreta del fatto che un'azione normativa coordinata e basata sul rischio in materia di infrastrutture di rete può avere successo.

Il "5G Cybersecurity Toolbox", adottato dal Gruppo di cooperazione NIS nel gennaio 2020 e avallato dalla Comunicazione della Commissione europea sul 5G sicuro, ha definito un quadro basato su tre elementi che si rafforzano a vicenda. In primo luogo, una metodologia comune di valutazione dei rischi che gli Stati membri erano tenuti ad applicare alle proprie catene di approvvigionamento 5G. In secondo luogo, una serie di misure strategiche, tra cui l'identificazione dei fornitori ad alto rischio e la possibilità di limitare o escludere tali fornitori dalle parti centrali e sensibili della rete. In terzo luogo, un processo coordinato di attuazione da parte degli Stati membri, supportato dagli orientamenti della Commissione, che ha portato all'esclusione di fatto di Huawei e ZTE dall'infrastruttura di rete 5G centrale nella grande maggioranza degli Stati membri dell'UE. Entrambe le società sono presenti anche come produttori di dispositivi di rete per uso domestico e per le PMI, con una quota di mercato combinata significativa nei canali europei di vendita al dettaglio e degli ISP.

La lezione fondamentale del 5G Toolbox è che non ha richiesto all'UE di dimostrare che si fosse verificata una violazione specifica. È stata sufficiente una valutazione basata sul rischio volta a stabilire se le condizioni giuridiche, tecniche e geopolitiche relative a un determinato fornitore creassero un'esposizione al rischio inaccettabile per le infrastrutture critiche. Su questa base, sono state intraprese azioni e i mercati sono stati efficacemente rimodellati. La combinazione di classificazione di sicurezza, norme sugli appalti e segnali di mercato ha contribuito a produrre un risultato che nessun singolo strumento avrebbe potuto ottenere da solo.

**Il 5G Toolbox non ha atteso che si verificasse una violazione. È stato invece implementato un quadro basato sul rischio per prevenirla. Lo stesso quadro applicato ai router porta alla stessa conclusione e alla stessa necessità di agire.**

Lo stesso quadro analitico, applicato ai router domestici e delle PMI, porta alla stessa conclusione. Le condizioni giuridiche applicabili ai produttori di router con sede nella Repubblica Popolare Cinese sono identiche a quelle applicabili ai fornitori di apparecchiature 5G con sede nella Repubblica Popolare Cinese. I vettori di rischio, tra cui l'intercettazione dei dati, la funzionalità di "kill switch" e la possibilità di imposizione da parte dello Stato, sono strutturalmente analoghi. La concentrazione del mercato è documentata. Esiste ora una finestra di opportunità per agire prima che la dipendenza diventi irreversibile, così come è avvenuto per il 5G nel 2019 e nel 2020.

## 5.2 Un modello di azione coerente in tutti i settori

Il caso del 5G è tutt'altro che isolato. Se esaminata trasversalmente ai vari settori, la politica dell'Unione Europea e degli Stati membri rivela una logica coerente e sempre più applicata. Laddove i produttori cinesi detengono una quota di mercato significativa nell'hardware con capacità di accesso remoto e implicazioni per le infrastrutture critiche, l'Europa si è mossa per limitare, regolamentare o ridurre i rischi. Il caso dei router rappresenta l'eccezione più evidente.

La tabella nelle pagine seguenti illustra le azioni documentate dell'UE e degli Stati membri nei vari settori in cui il rischio legato alla catena di approvvigionamento cinese ha determinato una risposta normativa.

**Tabella 1. Confronto intersettoriale delle azioni dell'UE e dei partner relative alla presenza di fornitori provenienti da giurisdizioni ad alto rischio nelle categorie di hardware critico, dal 2020 al 2026.**

| Settore | Motivazione | Azione dell'UE | Equivalenti extra-UE |
|---|---|---|---|
| **Inverter solari** | Rischio di manipolazione coordinata del firmware da remoto che causi interruzioni su scala di rete. La maggior parte degli inverter installati nell'UE è prodotta in Cina.[28] | Decisione della Commissione di aprile-maggio 2026 di sospendere i finanziamenti dell'UE nell'ambito degli strumenti di coesione e di ripresa per progetti che utilizzano inverter fabbricati in giurisdizioni ad alto rischio, tra cui la Repubblica Popolare Cinese, la Russia, l'Iran e la Corea del Nord; comunicata alle istituzioni finanziarie a partire dal 1° maggio 2026 e formalizzata nelle linee guida della Commissione del 13 maggio 2026.[29] | **Cina:** produttori nazionali quali Huawei, Sungrow e Ginlong hanno raggiunto posizioni dominanti nel mercato globale degli inverter, sostenuti dalla politica industriale "Made in China 2025", dagli appalti guidati dalle imprese statali e dai vantaggi strutturali di scala[30] che hanno notevolmente limitato la posizione competitiva dei fornitori europei nel mercato cinese.<br><br>**Stati Uniti:** nel novembre 2025, oltre 54 deputati repubblicani della Camera dei Rappresentanti hanno formalmente richiesto restrizioni alle importazioni di inverter cinesi, citando rischi critici per la sicurezza della rete, tra cui il ritrovamento di dispositivi di comunicazione non autorizzati in inverter di fabbricazione cinese in grado di consentire l'accesso remoto alle infrastrutture di rete.[31]<br><br>**Giappone:** Il METI e l'ANRE hanno intensificato l'attenzione sui rischi legati alla catena di approvvigionamento e alla sicurezza informatica nel settore energetico, pubblicando nel giugno 2025 linee guida sulla sicurezza della catena di approvvigionamento per i sistemi di controllo dell'energia. Ai sensi della Legge sulla promozione della sicurezza economica del 2022, gli operatori di infrastrutture critiche designati in settori quali quello energetico sono soggetti a obblighi di notifica preventiva e a screening governativo prima dell'installazione di specifiche strutture critiche, un quadro normativo che può comprendere le apparecchiature utilizzate nei sistemi elettrici, compresa l'installazione di inverter.[32] |

28 La Commissione blocca i finanziamenti dell'UE a Huawei, Politico, disponibile all'indirizzo: https://www.politico.eu/article/commission-blocks-eu-funding-for-huawei-solar-tech

29 Servizio di Euronews sugli inverter ad alto rischio, disponibile all'indirizzo: https://www.euronews.com/my-europe/ 2026/05/04/eu-moves-to-ban-high-risk-inverters-from-china-over-cybersecurity-threats

30 Lo sconvolgimento dell'industria solare cinese avrà ripercussioni globali, disponibile all'indirizzo: https://www.csis.org/analysis/chinas-solar-industry-upheaval-effects-will-be-global

31 I repubblicani statunitensi fanno pressione su Trump affinché blocchi le importazioni di inverter cinesi, disponibile all'indirizzo: https://rsc-pfluger.house.gov/media/press-releases/rsc-calls-out-chinese-solar-inverters-security-risk-us-energy-infrastructure

32 Pubblicata la guida alle misure di sicurezza della catena di approvvigionamento per i sistemi di controllo dell'energia, METI, disponibile all'indirizzo: https://www.meti.go.jp/english/press/2025/0603_007

| Settore | Motivazione | Azione dell'UE | Equivalenti extra-UE |
|---|---|---|---|
| **Rete core 5G** | Obblighi legali a carico dei produttori ai sensi della legislazione statale cinese, possibilità di aggiornamento remoto del firmware, rischio legato alla concentrazione dei fornitori | 5G Toolbox 2020. Restrizioni degli Stati membri nei confronti dei fornitori ad alto rischio, esclusione di fatto di Huawei e ZTE nella maggior parte degli Stati membri[33] | **Cina**: A seguito della revisione del 2022 delle Misure di revisione sulla sicurezza informatica della Cina[34] , che ha esteso la supervisione di CAC agli appalti da parte degli operatori di infrastrutture informatiche critiche, i contratti di Nokia ed Ericsson sono stati sottoposti a revisioni di sicurezza nazionale con criteri non resi noti. La quota di mercato combinata di entrambi i fornitori nelle reti mobili cinesi è scesa da circa il 12% nel 2020 a circa il 3% entro il 2025. I ricavi di Nokia nella Grande Cina sono diminuiti del 58% tra il 2019 e il 2025, passando da circa 2,2 miliardi di euro a 913 milioni di euro[35].<br><br>**Stati Uniti:** Secure and Trusted Communications Networks Act del 2019 e FCC Covered List che designano Huawei e ZTE; Secure Equipment Act del 2021 che vieta ulteriori autorizzazioni da parte della FCC per le apparecchiature incluse nell'elenco.[36]<br><br>**Regno Unito:** Divieto di nuove apparecchiature Huawei nel 5G a partire dal 2021, rimozione completa entro la fine del 2027.<br><br>**Australia:** Huawei e ZTE escluse dal 2018.<br><br>**Canada**: Huawei e ZTE vietate nel 5G e nel 4G a partire da maggio 2022, con rimozione entro il 2027. |

►

| Settore | Motivazione | Azione dell'UE | Equivalenti extra-UE |
|---|---|---|---|
| **Veicoli elettrici in prossimità di siti critici** | Telemetria remota, geolocalizzazione persistente, raccolta di dati dai sensori di bordo e possibilità di disattivazione o interferenza da remoto; assoggettabilità dei produttori con sede nella Repubblica Popolare Cinese alla legislazione statale cinese. | Polonia (in prima linea), altri Stati membri stanno elaborando restrizioni sui veicoli elettrici prodotti in Cina in prossimità di infrastrutture sensibili[37] | **Cina:** A partire dal 2021, le autorità cinesi hanno vietato l'accesso dei veicoli Tesla alle basi militari, agli edifici governativi, agli aeroporti e a una gamma sempre più ampia di strutture affiliate allo Stato, adducendo motivi di sicurezza dei dati relativi ai sensori e alla connettività dei veicoli. Tesla è rimasta esclusa dalla maggior parte degli elenchi degli appalti pubblici e non le è stato consentito di trasferire i dati dei veicoli al di fuori della Cina senza l'approvazione delle autorità competenti.[38]<br><br>**Stati Uniti:** Regola definitiva del Dipartimento del Commercio del gennaio 2025, emanata nell'ambito dell'autorità in materia di tecnologie e servizi dell'informazione e della comunicazione, che vieta l'importazione e la vendita di veicoli connessi che incorporino sistemi di connettività veicolare (hardware e software) collegati alla Repubblica Popolare Cinese o alla Russia, nonché software per sistemi di guida automatizzata, con entrata in vigore graduale a partire dall'anno di modello 2027 (software) e dall'anno di modello 2030 (hardware VCS).[39]<br><br>**Regno Unito:** è in corso un'indagine governativa a seguito delle segnalazioni del gennaio 2023 relative al ritrovamento di dispositivi di localizzazione fabbricati in Cina integrati in veicoli governativi.[40] |

CONTINUA ►

33 Toolbox 5G dell'UE e comunicazione della Commissione su Huawei e ZTE: https://digital-strategy.ec.europa.eu/en/library/communication-commission-implementation5g-cybersecurity-toolbox
34 La Cina ha emanato nuove misure per la revisione della sicurezza informatica nel 2022, disponibile all'indirizzo: https://www.whitecase.com/insight-alert/china-issued-new-measures-cybersecurity-review-2022
35 Ericsson e Nokia registrano un crollo delle vendite in Cina, disponibile all'indirizzo: https://www.lightreading.com/5g/ericsson-and-nokia-see-their-sales-in-china-fall-of-a-clif
36 Legge sulle reti di comunicazione sicure e affidabili del 2019, disponibile all'indirizzo https://www.congress.gov/bill/116th-congress/house-bill/4998
Elenco della FCC (designazioni di Huawei e ZTE), disponibile all'indirizzo: https://www.fcc.gov/supplychain/coveredlist
Legge sulle apparecchiature sicure del 2021, disponibile all'indirizzo: https://www.congress.gov/bill/117th-congress/ house-bill/3919

37 La Polonia vieta l'accesso delle auto cinesi alle basi militari: https://www.fdd.org/analysis/2026/02/20/ poland-bans-chinese-cars-from-military-sites-over-spying-fears
38 Le auto Tesla rischiano ulteriori divieti di ingresso in Cina a causa dell'intensificarsi delle «preoccupazioni in materia di sicurezza», disponibile all'indirizzo: https://asia.nikkei.com/spotlight/supply-chain/tesla-cars-face-more-entry-bans-in-china-as le-preoccupazioni-in-materia-di-sicurezza-si-intensificano
39 Registro Federale degli Stati Uniti, disponibile all'indirizzo: https://www.federalregister.gov/ documents/2025/01/16/2025-00592/securing-the-information-and-communications technology-and-services-supply-chain-connected-vehicles
40 Un dispositivo di localizzazione cinese nascosto «rinvenuto in un'auto del governo britannico» suscita timori per la sicurezza nazionale, disponibile all'indirizzo: https://inews.co.uk/news/hidden-chinese-tracking-device-government-car sicurezza-nazionale-2070152

| Settore | Motivazione | Azione dell'UE | Equivalenti extra-UE |
|---|---|---|---|
| **Dispositivi di rete (router per consumatori e PMI)** | **Vettori di rischio identici a quelli dei settori sopra citati:** possibilità per i produttori con sede nella Repubblica Popolare Cinese di imporre per via legale la capacità di aggiornamento remoto del firmware, concentrazione di mercato paragonabile o superiore a quella delle reti 5G core al momento dell'intervento dell'UE e base installata sostanzialmente più ampia. | **Non esiste un quadro coordinato dell'UE paragonabile al "5G Toolbox" che si applichi alle apparecchiature di rete per consumatori e PMI.** Strumenti orizzontali, tra cui il Cyber Resilience Act e l'atto delegato della direttiva sulle apparecchiature radio, si applicano ai router per consumatori, ma nessuno dei due prevede un meccanismo di classificazione dei rischi della catena di approvvigionamento . La proposta di Cybersecurity Act 2 introduce tale meccanismo per le catene di approvvigionamento critiche delle TIC, ma, nella sua formulazione attuale, non si estende alle apparecchiature di rete per consumatori e PMI. | **Cina:** Nel 2014, a seguito delle rivelazioni di Snowden sulla sorveglianza da parte dell'NSA delle apparecchiature vendute all'estero, il Centro del governo centrale cinese per gli appalti pubblici ha rimosso Cisco, Apple, Intel, McAfee e Citrix dal proprio elenco di fornitori approvati[41]<br><br>**Stati Uniti:** decisione della FCC[42] del 23 marzo 2026 che aggiunge tutti i router di fascia consumer di fabbricazione estera all'elenco coperto dalla FCC (FCC Covered List), vietando l'autorizzazione di nuovi modelli; i dispositivi esistenti beneficiano di una clausola di salvaguardia, con una deroga per l'aggiornamento del software a favore dei produttori valida fino al 1° marzo 2027. L'indagine penale antitrust del Dipartimento di Giustizia degli Stati Uniti su TP-Link è stata avviata alla fine del 2024.[43]<br><br>**Regno Unito, Canada e Australia** hanno emanato, ciascuno, linee guida o restrizioni operative relative alle apparecchiature di rete ad alto rischio; in ciascuna giurisdizione sono in fase di sviluppo quadri normativi formali riguardanti i router. |

41 La Cina "elimina i giganti tecnologici statunitensi" dall'elenco approvato, disponibile all'indirizzo: https://www.bbc.com/news/technology-31640539

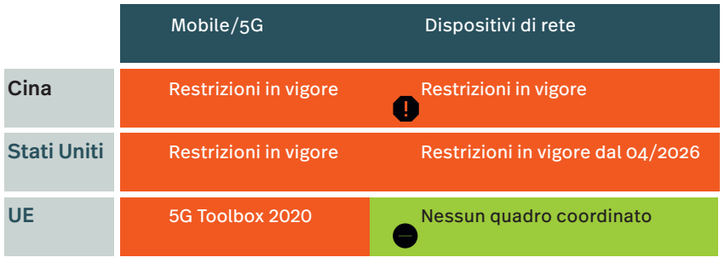
42 La FCC aggiorna l'elenco dei prodotti soggetti a regolamentazione per includere i router di consumo di fabbricazione estera, vietando l'approvazione di nuovi modelli, disponibile all'indirizzo: https://docs.fcc.gov/public/attachments/DOC-420034A1.pdf

43 Gli Stati Uniti stanno conducendo un'indagine penale antitrust su TP-Link, disponibile all'indirizzo: https://www.reuters.com/technology/tp-link-faces-us-criminal-antitrust-investigation-bloomberg-news-reports-2025-04-25



Il quadro tra le diverse giurisdizioni è sorprendente. In ogni settore sopra elencato, l'Unione Europea ha agito in linea con i suoi principali partner democratici, con un'unica eccezione: per quanto riguarda i dispositivi di rete, l'Europa si distingue tra le principali economie sviluppate nel mantenere un accesso aperto al mercato per i fornitori che altrove sono stati soggetti a restrizioni per identici motivi di sicurezza, specialmente quando si tratta di proteggere le reti. Questa non è una posizione neutrale. Applicare la logica di rischio del 5G Toolbox alle reti mobili lasciando al contempo i dispositivi di rete senza regolamentazione costituisce un'incoerenza che nessuna giurisdizione alleata ha scelto di mantenere, e che diventa sempre più difficile da giustificare con il passare dei mesi.

**Immagine 3: Un caso a sé stante tra i pari: l'UE non dispone di un quadro normativo per la sicurezza dei dispositivi di rete domestici**




Nel 2020 l'UE ha applicato la logica della sicurezza della catena di approvvigionamento al 5G.
Non ha applicato la stessa logica ai dispositivi di rete a banda larga su linea fissa.
Ogni giurisdizione comparabile è più avanti dell'Europa o si sta muovendo in quella direzione.

Questa contraddizione strutturale è inoltre difficile da difendere pubblicamente. L'Europa limita l'uso degli inverter solari cinesi per proteggere la rete elettrica, limita l'uso di apparecchiature cinesi nelle reti 5G per proteggere le infrastrutture di comunicazione e sta valutando restrizioni sui veicoli cinesi in prossimità di siti sensibili, ma consente l'installazione senza restrizioni di router cinesi che gestiscono la connettività Internet di ogni abitazione e azienda europea.

# 6
# CIÒ CHE È GIÀ IN ATTO

L'ESIGENZA DI INTERVENIRE in materia di sicurezza delle reti non richiede di partire da zero dal punto di vista normativo. Esiste già un corpus sostanziale di legislazione dell'UE che affronta alcuni aspetti del problema, stabilisce obblighi pertinenti e, in diversi casi, evidenzia la lacuna che uno strumento dedicato alla sicurezza dei router andrebbe a colmare. Comprendere ciò che è già in atto è importante quanto identificare ciò che manca.

**Tabella 2. Strumenti dell'UE relativi alla sicurezza della catena di approvvigionamento dei dispositivi di rete. Analisi dei contributi e delle lacune.**

| Strumento | Rilevanza | Contributo e lacune |
|---|---|---|
| **Cybersecurity Act 2 (proposta, COM (2026) 11)** | Molto alta | Attualmente nelle prime fasi della procedura legislativa ordinaria. Istituisce un quadro di riferimento per una catena di approvvigionamento delle TIC affidabile, con la designazione dei fornitori ad alto rischio e poteri di divieto. Lo strumento legislativo attraverso il quale è possibile attuare la raccomandazione a lungo termine contenuta nel presente articolo. |
| **Industrial Accelerator Act (proposta)** | Alta | Proposta della Commissione pubblicata nel marzo 2026 nell'ambito dell'attuazione del "Clean Industrial Deal" e della "Bussola per la competitività". Porta avanti le preferenze di appalto "Made in EU", ma il suo ambito di applicazione è limitato alle industrie ad alto consumo energetico (acciaio, cemento, alluminio), ai veicoli elettrici e alle tecnologie a zero emissioni nette. I router e le apparecchiature ICT non rientrano attualmente nel campo di applicazione; l'allineamento con i dispositivi di rete richiede una decisione politica specifica. |
| **Revisione delle direttive sugli appalti pubblici (Public Procurement Directives revision)** | Alta | Revisione della direttiva 2014/24/UE in fase di preparazione. Fornisce il principale strumento giuridico per le preferenze negli appalti neutrali dal punto di vista settoriale e per le esclusioni giustificate da motivi di sicurezza nazionale, anche per i dispositivi di rete. |
| **Pacchetto sulla sovranità tecnologica** | Media | Comunicazione della Commissione e misure di accompagnamento, 2026. Definisce il quadro strategico per le azioni trasversali in materia di sovranità digitale nell'ambito del mandato della Commissione. I dispositivi di rete non sono attualmente indicati come linea di lavoro prioritaria. |

| | | |
|---|---|---|
| **Legge sulla ciberresilienza (Cyber Resilience Act)** | Molto Alta | Requisiti minimi obbligatori di sicurezza informatica per i prodotti connessi, compresi i router. Indipendente dall'origine. Valuta se un dispositivo opera in modo sicuro e non si occupa della possibilità di obbligare il produttore a modificarne il comportamento. |
| **Direttiva NIS2** | Media | Obbliga gli operatori di telecomunicazioni a gestire il rischio della catena di approvvigionamento. Gli obblighi non dovrebbero fermarsi al punto di terminazione della rete e pertanto non riguardano la decisione di acquisto dei dispositivi di rete. |
| **Atto delegato RED e regolamento sull'accesso a un'Internet aperta** | Media | Il regolamento delegato RED impone ai dispositivi wireless di proteggere i dati degli utenti e il funzionamento della rete, con obbligo di applicazione a partire dall'agosto 2025. L'articolo 3, paragrafo 1, del regolamento sull'accesso a un'Internet aperta stabilisce il diritto dell'utente di scegliere l'apparecchiatura terminale. Fornisce il fondamento giuridico per gli obblighi di trasparenza sui router forniti dagli ISP. |
| **Regolamento SAFE e STEP** | Media | Preferenze negli appalti per le tecnologie critiche prodotte nell'UE e meccanismi di investimento per le tecnologie strategiche. L'estensione ai router destinati al mercato di massa richiede una decisione politica specifica. |
| **5G Cybersecurity Toolbox** | Alta (per analogia) | Il precedente in termini di definizione, che comprende la classificazione dei fornitori ad alto rischio fondata sul rischio, l'attuazione da parte degli Stati membri e l'autorità di limitare il mercato. Direttamente applicabile come modello. |

### 6.1 Perché la legge sulla ciberresilienza (Cyber Resilience Act) da sola non è sufficiente

L'obiezione istituzionale più prevedibile alle raccomandazioni contenute nel presente articolo è che il Cyber Resilience Act,[44] entrato in vigore nel dicembre 2024 e applicabile a partire dal dicembre 2027, imponga già requisiti minimi di sicurezza informatica per i prodotti connessi, inclusi router e gateway per uso domestico. Se un router è conforme al CRA, si sostiene, perché sono necessarie ulteriori misure?

L'obiezione confonde due superfici di rischio categoricamente diverse. Il CRA valuta se un dispositivo si comporti in modo sicuro durante il normale funzionamento. Impone principi di sicurezza fin dalla progettazione, gestione delle vulnerabilità, documentazione della distinta dei materiali software e valutazione di conformità. Si tratta di obblighi necessari e auspicabili. La governance della catena di approvvigionamento valuta invece se il produttore possa essere legittimamente indotto da uno Stato estero a far funzionare il dispositivo in modo diverso. Si concentra sul quadro giuridico che disciplina il soggetto che controlla il firmware del dispositivo per tutta la sua vita utile, piuttosto che sul comportamento predefinito del dispositivo stesso.

Un dispositivo di rete prodotto da un'azienda soggetta alla Legge nazionale sull'intelligence della Repubblica Popolare Cinese può essere pienamente conforme a tutti i requisiti tecnici del CRA e rimanere, in termini giuridici, un potenziale strumento dell'intelligence di Stato cinese. La valutazione di conformità al CRA viene effettuata in base al comportamento osservabile del dispositivo in un determinato momento. Per sua stessa natura, non può valutare la possibilità giuridica di imporre obblighi al soggetto che controlla il canale di aggiornamento del dispositivo. Il CRA è uno strumento di sicurezza dei prodotti tecnologicamente neutro, volutamente indipendente dall'origine. Il 5G Cybersecurity Toolbox è stato adottato nel 2020 proprio perché la sola valutazione di conformità non era in grado di cogliere i rischi non tecnici. La proposta di legge sulla sicurezza informatica (Cybersecurity Act 2) del gennaio 2026 riflette la stessa intuizione, istituendo un quadro di governance orizzontale della catena di approvvigionamento al di sopra e parallelamente all'attuale architettura di sicurezza dei prodotti.

**Il quadro normativo UE esistente si chiede se un dispositivo sia sicuro. È necessario uno strumento di governance della catena di approvvigionamento modellato sul 5G Toolbox per valutare se il produttore possa essere indotto a renderlo insicuro.**

### 6.2 Il divario cumulativo e lo slancio politico

Le ragioni a favore della governance della catena di approvvigionamento non si basano esclusivamente sull'analisi giuridica. L'opinione pubblica si è mossa nella stessa direzione dell'architettura legislativa e, per certi aspetti, l'ha addirittura anticipata. L'esame dell'attuale architettura

**44** Regolamento (UE) 2024/2847 del 23 ottobre 2024 sui requisiti orizzontali di sicurezza informatica per i prodotti con elementi digitali (Cyber Resilience Act).

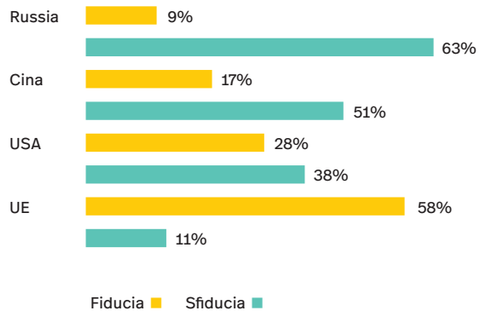
normativa rivela uno schema coerente. Ciascuno strumento affronta elementi importanti relativi alla sicurezza dei dispositivi, all'accesso al mercato o alla resilienza delle reti. Nessuno, tuttavia, affronta la specifica combinazione di fattori che può rendere i dispositivi di rete soggetti alla giurisdizione della Repubblica Popolare Cinese un rischio strategico: **l'intersezione tra elevata concentrazione di mercato, capacità di accesso remoto e la potenziale obbligatorietà dei produttori ai sensi della legislazione cinese in materia di sicurezza nazionale e intelligence.** Al di là dell'architettura normativa formale, il più ampio contesto politico all'interno dell'Unione Europea è diventato sempre più favorevole a misure volte a ridurre le dipendenze strategiche in settori critici.

Questo cambiamento trova riscontro nella Comunicazione congiunta sulla strategia europea per la sicurezza economica[45], che identifica la sicurezza economica, la resilienza della catena di approvvigionamento e la protezione delle infrastrutture critiche come priorità strategiche fondamentali per l'Unione. L'enfasi della strategia sulla riduzione dei rischi, sulla resilienza tecnologica e sulla salvaguardia delle infrastrutture sensibili fornisce una giustificazione politica più ampia per un maggiore controllo delle apparecchiature di rete di fabbricazione straniera in ambienti di comunicazione strategicamente significativi.

Le condizioni politiche sono ulteriormente rafforzate dall'opinione pubblica. Secondo un sondaggio POLITICO European Pulse condotto nel marzo 2026 su 6.698 europei, circa l'84% degli intervistati dichiara di non fidarsi delle aziende tecnologiche statunitensi per quanto riguarda i propri dati personali, mentre il 93% esprime la stessa opinione riguardo alle aziende cinesi. In Germania, la sfiducia è tra le più elevate del campione[46] . Uno studio eupinions della Bertelsmann Stiftung pubblicato[47] nel maggio di quest'anno rileva che il 61% degli europei vede negativamente l'influenza globale della Cina. Lo stesso studio riporta che il 67% degli intervistati ritiene che il proprio paese sia economicamente dipendente dalla Cina. Tra coloro che percepiscono tale dipendenza, il 77% è favorevole a ridurla anche a costo di sacrifici economici. Questi risultati indicano sia una diffusa preoccupazione riguardo al ruolo globale della Cina sia un forte sostegno pubblico alle politiche volte a ridurre la dipendenza strategica ed economica.

La sfiducia dell'opinione pubblica nei confronti delle aziende tecnologiche straniere si estende direttamente ai dispositivi che gestiscono le reti domestiche europee. Un sondaggio YouGov del 2025 condotto su oltre 16.000 intervistati negli Stati membri dell'UE ha rilevato che una netta maggioranza ha espresso sfiducia nei confronti, in particolare, dei produttori cinesi e russi di router, classificandoli come le fonti meno affidabili di apparecchiature per reti domestiche tra tutte le provenienze dei produttori presentate.

**Fiducia e sfiducia nei confronti dei produttori di router (dati ponderati)**

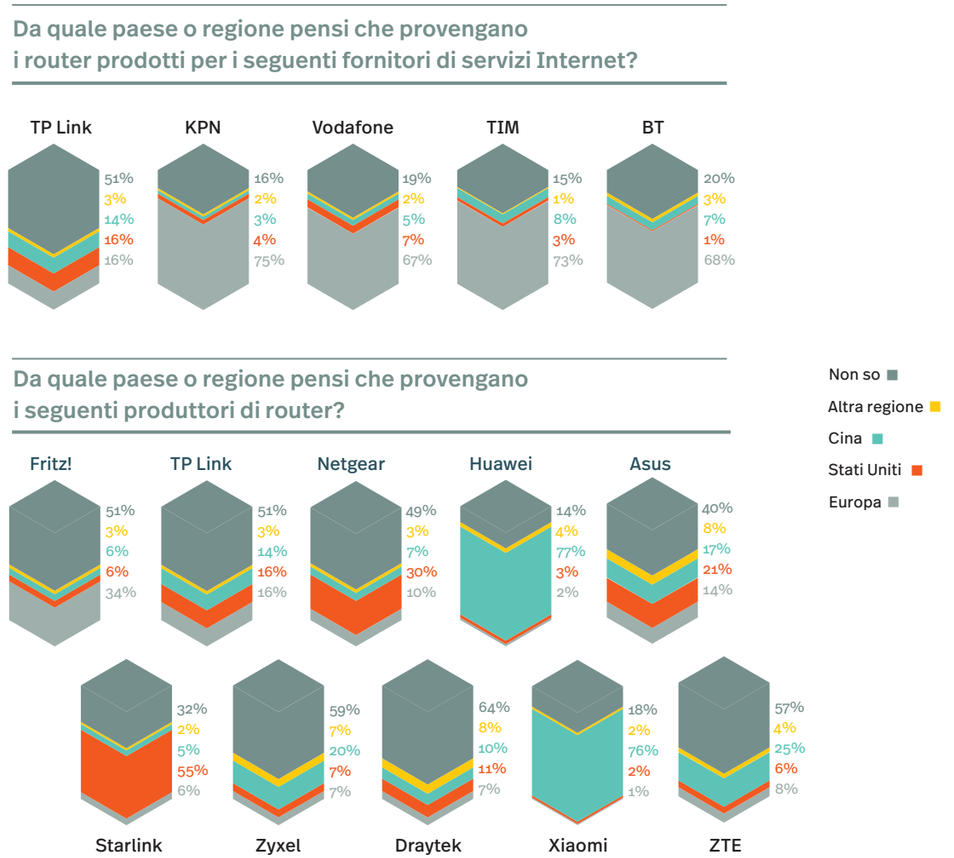



45 COMUNICAZIONE CONGIUNTA AL PARLAMENTO EUROPEO, AL CONSIGLIO EUROPEO E AL CONSIGLIO SULLA «STRATEGIA EUROPEA PER LA SICUREZZA ECONOMICA», disponibile all'indirizzo https://op.europa. eu/en/publication-detail/-/publication/3948446b-101c-11ee-b12e-01aa75ed71a1

46 POLITICO: 8 europei su 10 non si fidano delle aziende statunitensi e cinesi per quanto riguarda i dati, disponibile all'indirizzo: https://www.politico.eu/article/8-in-10-europeans-dont-trust-us-chinese-frms-with-data

47 Studio «Europe's Call for Greater Independence», disponibile all'indirizzo: https://bst-europe.eu/europe-in-the-world/europes-call-for-greater-independence

Forse non sorprende che, quando viene chiesto loro da dove provenga il router fornito dal proprio ISP, la maggior parte dei consumatori europei dia per scontato che il dispositivo presente in casa sia di provenienza europea. Gli stessi cittadini che esprimono forte scetticismo nei confronti della tecnologia cinese sono in gran parte ignari del fatto che il proprio router possa essere stato prodotto proprio dalle aziende di cui diffidano. Una volta colmato questo divario, attraverso le misure di trasparenza raccomandate nel presente articolo, diventa molto difficile resistere alla logica politica che spinge ad agire ulteriormente. Su questo tema, l'opinione pubblica è già più avanti rispetto al quadro normativo.



# 7
# RACCO-MANDAZIONI

LA COALIZIONE SAFENET presenta un quadro d'azione in quattro parti che copre l'intera gamma di strumenti a disposizione delle istituzioni europee e dei governi degli Stati membri per colmare il divario in materia di sovranità dei router. I quattro ambiti **(trasparenza, riforma degli appalti, governance della catena di approvvigionamento e capacità industriale)**, se considerati nel loro insieme e perseguiti con determinazione, garantiranno che le apparecchiature di rete per uso domestico e per le PMI rientrino nell'architettura della sovranità digitale europea e che il 93% del traffico Internet europeo che transita attraverso dispositivi di rete non costituisca più una lacuna irrisolta.

## 7.1 Trasparenza e sensibilizzazione

I cittadini, le imprese e le autorità pubbliche europee non possono prendere decisioni informate su apparecchiature di rete che non sono in grado di identificare, e le autorità di regolamentazione non possono governare mercati che non riescono a vedere. Raccomandiamo le seguenti azioni:

### Etichettatura obbligatoria del Paese di origine e della giurisdizione per i dispositivi di rete

I produttori e i distributori di router e dispositivi di rete per uso domestico e per le PMI dovrebbero essere tenuti a indicare, in modo chiaro e in un formato standardizzato, il Paese di fabbricazione dell'hardware del dispositivo, il Paese di giurisdizione dello sviluppatore del firmware e il Paese di giurisdizione del gestore del canale di aggiornamento. Tale etichettatura dovrebbe essere applicata nei punti vendita, nei termini contrattuali degli ISP e sulla confezione dei dispositivi.

### Obblighi di informativa degli ISP sulla provenienza dell'hardware e del firmware

I fornitori di servizi Internet che forniscono dispositivi di rete a clienti residenziali e alle PMI nell'ambito di contratti di banda larga dovrebbero essere tenuti a indicare, in un linguaggio semplice e accessibile ai consumatori, l'origine del produttore del dispositivo, la giurisdizione che disciplina il produttore e la catena di approvvigionamento del firmware. Tale obbligo dovrebbe estendersi al livello del firmware e del sistema operativo, dove la provenienza è spesso poco chiara persino agli stessi ISP, e non limitarsi al solo hardware fisico.

### Elenco obbligatorio dei componenti software (SBOM) per il firmware dei dispositivi di rete

I produttori di dispositivi di rete che immettono dispositivi sul mercato dell'UE dovrebbero essere tenuti a fornire una distinta dei materiali software (Software Bill of Materials, SBOM) per tutto il firmware, che copra l'intero grafico delle dipendenze transitive anziché limitarsi alle dipendenze di primo livello, affrontando così i rischi della catena di approvvigionamento non pienamente contemplati dagli attuali requisiti di cui all'allegato I, parte II, punto 1, del Cyber Resilience Act, e a rendere tale SBOM accessibile agli ISP e ai grandi acquirenti istituzionali, oltre che alle autorità di vigilanza del mercato. Tale requisito integra l'obbligo di divulgazione della provenienza dell'hardware e interviene a livello firmware, dove il rischio operativo di manipolazione remota è più acuto.

### Iniziativa di sensibilizzazione dei consumatori sulla sicurezza dei router

La Commissione e le agenzie di comunicazione degli Stati membri dovrebbero sostenere una campagna mirata di sensibilizzazione pubblica, coordinata con l'ENISA e le autorità nazionali di sicurezza informatica, sulle implicazioni per la sicurezza della provenienza dei router per uso domestico. La campagna dovrebbe colmare il divario tra le preoccupazioni dei consumatori riguardo alla tecnologia cinese e la consapevolezza dei consumatori circa l'effettiva provenienza dei dispositivi forniti dai loro ISP. È stato dimostrato che le campagne di sensibilizzazione, nel contesto del GDPR e delle buone pratiche di sicurezza informatica, determinano cambiamenti significativi nel comportamento dei consumatori.

## 7.2 Riforma degli appalti

Le misure di trasparenza creano visibilità, mentre la riforma degli appalti crea gli incentivi commerciali necessari per modificare la struttura del mercato. L'UE è il principale acquirente singolo di apparecchiature di rete nel mercato europeo se si considerano complessivamente gli appalti della pubblica amministrazione, della sanità, dell'istruzione e delle infrastrutture critiche, e le condizioni che essa impone a tali appalti influenzano direttamente gli incentivi dei fornitori.

### Requisiti di affidabilità per gli appalti del settore pubblico e delle infrastrutture critiche

Le autorità pubbliche, gli operatori di infrastrutture critiche regolamentate e le istituzioni finanziate con fondi pubblici dovrebbero essere tenuti ad acquistare dispositivi di rete da produttori non soggetti alle condizioni di vincolatività giuridica identificate come motivo di esclusione nel contesto del 5G Toolbox. In attesa dell'istituzione di un meccanismo formale di classificazione dei fornitori ad alto rischio ai sensi della raccomandazione sulla governance della catena di approvvigionamento di cui al punto 7.3, le amministrazioni contraenti possono applicare per analogia i criteri di rischio del 5G Toolbox. Il requisito dovrebbe essere attuato attraverso la futura legge sugli appalti pubblici e specifiche linee guida di attuazione della direttiva NIS2 relative al rischio della catena di approvvigionamento per i dispositivi di rete. Il principio dovrebbe essere in primo luogo quello di "Buy Trusted" (acquistare da fornitori affidabili), con una preferenza per i prodotti europei laddove l'offerta europea affidabile soddisfi i requisiti funzionali e commerciali. Questi criteri potranno acquisire efficacia vincolante per i router una volta che entrerà in vigore il quadro CSA2.

### Linee guida europee di base per la certificazione della sicurezza informatica dei dispositivi di rete

L'ENISA, in collaborazione con la Commissione e le autorità nazionali di sicurezza informatica, dovrebbe sviluppare uno schema europeo dedicato di certificazione in materia di sicurezza informatica per i router nell'ambito del quadro europeo, basandosi sui requisiti di sicurezza stabiliti dal Cyber Resilience Act e integrando i requisiti essenziali applicabili alle apparecchiature radio ai sensi della Radio Equipment Directive, ma estendendoli per includere la provenienza della catena di approvvigionamento e i criteri di classificazione dei fornitori ad alto rischio.

### Incentivi strutturati alla sostituzione dell'hardware ad alto rischio in contesti prioritari

Dovrebbero essere messi a disposizione incentivi finanziari strutturati, analoghi a quelli utilizzati per facilitare l'eliminazione graduale delle apparecchiature Huawei dalle reti 5G, al fine di sostenere la sostituzione dei dispositivi di rete ad alto rischio in settori prioritari quali la pubblica amministrazione, la sanità, l'istruzione e gli operatori di infrastrutture

critiche. Lo strumento può essere attuato attraverso il meccanismo STEP, tramite i piani nazionali di ripresa e resilienza o tramite stanziamenti mirati del Connecting Europe Facility.

### 7.3 Governance della catena di approvvigionamento

La trasparenza e gli appalti sono necessari ma non sufficienti. Un quadro di governance della catena di approvvigionamento paragonabile a quello che l'UE ha costruito per il 5G tra il 2019 e il 2020 è lo strumento adeguato per affrontare la questione della capacità di imposizione dei produttori, la concentrazione strutturale del mercato dei router e il problema di coordinamento tra gli Stati membri che sorge quando ogni contesto nazionale di appalto prende decisioni in modo isolato.

#### Inserire le apparecchiature di rete domestiche e delle PMI nel dibattito legislativo sul Cybersecurity Act 2

Man mano che il Cybersecurity Act 2 procede nel percorso legislativo, il Parlamento e il Consiglio dovrebbero valutare come affrontare i rischi presenti nella catena di approvvigionamento dei router. Il segmento delle apparecchiature CPE presenta questioni relative all'applicabilità della normativa di natura analoga a quelle che il 5G Toolbox era stato concepito per affrontare, e l'architettura emergente del quadro normativo del Cybersecurity Act 2 offre uno strumento naturale attraverso il quale tali questioni possono essere esaminate. L'iter legislativo rappresenta un'opportunità per garantire che gli aspetti relativi alla catena di approvvigionamento delle apparecchiature di rete domestiche e per le PMI non rimangano, per impostazione predefinita, al di fuori dell'ambito di applicazione del quadro normativo orizzontale dell'UE in materia di sicurezza delle TIC.

#### Una raccomandazione della Commissione sulla valutazione dei rischi nella catena di approvvigionamento dei router

La Commissione può emanare una raccomandazione ai sensi dell'articolo 292 del TFUE che imponga agli Stati membri di applicare la logica di valutazione dei rischi del 5G Toolbox alle catene di approvvigionamento dei router senza attendere la conclusione del processo legislativo. In parallelo, all'ENISA può essere affidato, attraverso il suo programma di lavoro annuale ai sensi del Cybersecurity Act, il compito di elaborare una valutazione specifica del panorama delle minacce relative ai rischi della catena di approvvigionamento dei dispositivi di rete, creando così le basi analitiche per l'azione del Gruppo di cooperazione secondo le proprie tempistiche.

#### Un Toolbox per la sicurezza dei router

L'UE dovrebbe sviluppare un Toolbox per la sicurezza dei router modellato esplicitamente sul "5G Cybersecurity Toolbox". Il Toolbox dovrebbe stabilire una metodologia comune di valutazione dei rischi per le catene di approvvigionamento dei dispositivi di rete, un meccanismo per l'individuazione dei fornitori ad alto rischio e la limitazione dell'impiego dei loro prodotti in contesti sensibili dal punto di vista della sicurezza, nonché un processo coordinato di attuazione da parte degli Stati membri. Il quadro CSA2, una volta adottato, fornirà l'architettura giuridica attraverso la quale le misure del Toolbox potranno essere rese operative come atti di esecuzione vincolanti ai sensi degli articoli da 101 a 104. A differenza del 5G Toolbox, che si applicava principalmente agli operatori di rete professionali, il Toolbox per la sicurezza dei router deve affrontare la dimensione del mercato di massa, rivolta ai consumatori, del mercato dei router.

#### Meccanismo di classificazione dei fornitori ad alto rischio

Basandosi sul riconoscimento CSA2 e sul Toolbox per la sicurezza dei router, l'UE dovrebbe istituire un meccanismo di classificazione dei fornitori ad alto rischio per la catena di approvvigionamento dei router. Il meccanismo dovrebbe applicare l'approccio di valutazione dei fornitori basato sul rischio del 5G Toolbox al contesto dei dispositivi di rete, creando una base giuridica per requisiti differenziati di certificazione e appalto che tengano conto della giurisdizione del produttore.

### 7.4 Trasformazione della capacità industriale

Le misure normative sul versante della domanda devono essere accompagnate da investimenti sul versante dell'offerta e dall'espansione dei segmenti di mercato in cui i produttori europei competono già con successo. L'obiettivo non è l'autarchia europea nel settore dei dispositivi di rete, ma garantire che i produttori europei e alleati di fiducia possano competere efficacemente in un mercato attualmente caratterizzato da un sostegno statale asimmetrico.

### A breve termine: stimolo della domanda mediante l'armonizzazione della libertà di scelta del router

La leva più immediatamente disponibile sul versante dell'offerta non richiede nuove spese. L'armonizzazione della libertà di scelta del router in tutti gli Stati membri secondo lo standard stabilito dalla "Freie Routerwahl" tedesca e dalle disposizioni italiane del 2018 amplierebbe i segmenti di mercato in cui i produttori europei già superano i concorrenti cinesi in termini di preferenze dei consumatori. Laddove la decisione di acquisto spetta al consumatore, i produttori europei mantengono la loro posizione. Accelerare il recepimento completo dell'articolo 3, paragrafo 1, del regolamento 2015/2120 negli Stati membri in ritardo rappresenta quindi la misura dal lato dell'offerta disponibile che comporta il minor costo e agisce più rapidamente.

### Investimenti dell'UE nella capacità produttiva europea di router

Le misure normative sul lato della domanda devono essere accompagnate da investimenti sul lato dell'offerta per garantire che alternative europee affidabili possano soddisfare la domanda di mercato. La Commissione e gli Stati membri dovrebbero sviluppare una strategia industriale per la produzione europea di router, che includa un sostegno mirato attraverso InvestEU, i meccanismi dei Progetti di Importante Interesse Comune Europeo (IPCEI) e i quadri di partenariato pubblico-privato. Produttori europei come FRITZ!, Sagemcom, Vantiva e Lancom dimostrano che esiste già una base industriale competitiva che vale la pena difendere. L'obiettivo non è l'autarchia europea nel settore dei dispositivi di rete, ma garantire che i produttori europei e alleati affidabili possano competere efficacemente in un mercato attualmente caratterizzato da un sostegno statale asimmetrico.

## Un quadro a quattro pilastri per la sicurezza dei dispositivi di rete per uso domestico e per le PMI in Europa

### Trasparenza

Informare sulle decisioni

**Etichettatura di origine e giurisdizione**
Rendere obbligatoria la divulgazione dell'origine dell'hardware, della giurisdizione dello sviluppatore del firmware e dell'operatore del canale di aggiornamento al momento della vendita, nei contratti con gli ISP e sulle confezioni.

**Strumento** – contratti CRA / ISP / imballaggio

**Divulgazione della provenienza dell'ISP**
Richiedere agli ISP di indicare in modo chiaro l'origine del produttore, la giurisdizione competente e la catena di fornitura del firmware.

**Strumento** – contratti per la banda larga

**Requisito di SBOM del firmware**
Richiedere una Software Bill of Materials (SBOM) completa per tutto il firmware, affrontando i rischi della supply chain oltre CRA Allegato I, Parte II.

**Strumento** – CRA Allegato I Parte II (esteso)

**Campagna di sensibilizzazione per i consumatori**
Avviare una campagna pubblica di sensibilizzazione sulla sicurezza e sulla provenienza, coordinata da ENISA e autorità nazionali.

**Strumento** – ENISA / autorità nazionali

### Riforma degli appalti

Reindirizzare il potere di mercato

**Acquistare requisiti affidabili**
Richiedere che le autorità pubbliche e gli operatori di infrastrutture critiche acquistino dispositivi di rete da produttori non soggetti a condizioni di incompatibilità legale (criteri del 5G Toolbox per analogia).

**Strumento** – direttiva su appalti pubblici / orientamento NIS2

**Principio** – prima "Buy Trusted", poi "Buy European" se praticabile.

**Certificazione UE di cybersicurezza**
Affidare a ENISA il compito di sviluppare uno schema europeo di certificazione della cybersicurezza per i router destinati al mercato UE, basato sul Cybersecurity Certification Framework, sulla CRA e sulla Direttiva sulle apparecchiature radio.

**Strumento** – quadro EUCCF

**Incentivi alla sostituzione**
Introdurre incentivi finanziari strutturati per sostituire dispositivi ad alto rischio nelle infrastrutture critiche: energia, sanità pubblica, istruzione e infrastrutture critiche.

**Strumento** – STEP/RRP / meccanismo "Connecting Europe"

### Governance della catena di approvvigionamento

Costruire regole durature

**Portare le apparecchiature di rete per uso domestico e per PMI nel processo legislativo CSA2 dell'UE**
Assicurare che le apparecchiature di rete per uso domestico e per PMI siano considerate nell'atto legislativo in materia di cybersecurity CSA2 e nel quadro normativo emergente per la sicurezza ICT.

**Strumento** – processo legislativo CSA2

**Raccomandazione della Commissione sulla valutazione del rischio della catena di approvvigionamento per i router**
Applicare la logica di valutazione del rischio della catena di approvvigionamento del 5G Toolbox ai router attraverso una Raccomandazione della Commissione, mentre la legislazione è in corso di sviluppo.

**Strumento**– art. 292 TFUE

**Router Security Toolbox**
Sviluppare una toolbox dedicata alla sicurezza dei router con una metodologia comune di gestione del rischio, valutazione dei fornitori e implementazione coordinata.

**Strumento** – CSA2 articoli 101–104

**Meccanismo di classificazione dei fornitori ad alto rischio**
Istituire un meccanismo UE per classificare i fornitori di router ad alto rischio in base a fattori giurisdizionali e di rischio della catena di approvvigionamento.

**Strumento** – Router Security Toolbox / CSA2

### Capacità industriale

Garantire una fornitura affidabile

**Armonizzazione della libertà di scelta del router**
Accelerare il pieno recepimento di Art. 19(7) del Reg. 2015/2120, consentendo agli Stati membri in ritardo di abilitare la scelta del router da parte dell'utente finale.

**Strumento** – Reg. 2015/2120

**Investimenti nella produzione UE**
Attuare una strategia industriale per la produzione europea di CPE con sostegno InvestEU e IPCEI.

**Strumento** – InvestEU / IPCEI

I quattro pilastri si rafforzano a vicenda. La trasparenza abilita gli appalti;
gli appalti creano domanda per la governance della catena di approvvigionamento;
la governance rende praticabili gli investimenti industriali.

# 8
# CONCLUSIONE – DALLA CONSAPEVOLEZZA ALL'AZIONE

L'EUROPA DEVE AGIRE SUBITO. I rischi per la sicurezza, la sovranità tecnica e le ragioni economiche a sostegno delle industrie tecnologiche europee richiedono un intervento immediato. L'Europa ha costruito i quadri istituzionali, gli strumenti legislativi, i meccanismi di coordinamento e, nel 5G Toolbox, il collaudato manuale operativo. L'analisi secondo cui i router per uso domestico e per le PMI rappresentano una lacuna infrastrutturale critica nell'architettura della sovranità digitale europea non è contestata da chiunque esamini le prove, i dati di mercato, la documentazione sulle minacce, l'esposizione legale e l'evidente incoerenza con le azioni già intraprese in altri settori.

Ciò che occorre è una volontà politica incentrata sulla questione specifica della sicurezza dei router. Tale questione è stata messa in secondo piano, nei successivi programmi di lavoro della Commissione, nei dibattiti sull'attuazione della direttiva NIS2 e nei negoziati sul Cyber Resilience Act, da sfide alla sovranità digitale più ampie, più visibili e, per certi aspetti, meno gestibili. Anche se la governance dell'intelligenza artificiale e la dipendenza dal cloud richiedono giustamente una notevole attenzione, non si può permettere che le componenti critiche dell'infrastruttura di rete sottostante, attraverso la quale fluisce tutto il valore digitale, rimangano un aspetto secondario. I router si trovano, letteralmente, al punto di ingresso di ogni abitazione e azienda europea. Sono il gateway hardware attraverso il quale si accede all'intera architettura della sovranità digitale, e l'unico livello di tale architettura che attualmente non è disciplinato da alcun quadro europeo coordinato.

I costi del mancato intervento sono estremamente elevati. Ogni anno che passa senza un quadro normativo per la sicurezza dei router è un anno in cui i produttori cinesi consolidano la loro posizione di mercato, in cui le decisioni di acquisto degli ISP vincolano l'uso di hardware ad alto rischio per un altro decennio di vita utile, e in cui la dinamica di concentrazione guidata dalla chiusura del mercato statunitense amplifica l'esposizione europea. La finestra per un'azione preventiva ed economicamente vantaggiosa, la stessa finestra che esisteva per il 5G nel 2019, è aperta ora. Non rimarrà aperta a tempo indeterminato.

**L'Europa dispone degli strumenti, del precedente e del momento politico favorevole. La domanda è se agirà prima che la dipendenza diventi irreversibile.**

La Coalizione SAFENet esorta le istituzioni dell'UE e i governi degli Stati membri a considerare i router per uso domestico e per le PMI come il punto critico della catena di approvvigionamento dei servizi digitali che effettivamente sono, ad applicare la stessa logica coerente di sicurezza e sovranità già applicata ovunque altrove e ad agire prima che la finestra si chiuda. I produttori europei, le organizzazioni di sicurezza informatica e i difensori dei diritti digitali rappresentati nella Coalizione SAFENet condividono un unico obiettivo: un'Europa in cui l'infrastruttura fondamentale della vita digitale sia gestita con la serietà e la lungimiranza che il suo ruolo richiede.

# 9
# INFORMAZIONI SUL PRESENTE DOCUMENTO

## 9.1 Informazioni sulla coalizione SAFENet

La Sovereignty Alliance for European Network Technology (SAFENet) è un'alleanza strategica tra le principali aziende europee nel settore delle tecnologie di rete. SAFENet considera la tecnologia di rete come la spina dorsale dell'ecosistema digitale. L'alleanza rappresenta gli interessi dei produttori europei nei processi politici e normativi, contribuendo così alla sovranità digitale e alla sicurezza a lungo termine dell'infrastruttura digitale propria dell'Europa. Il suo obiettivo è un'Europa digitale autodeterminata, resiliente e a prova di futuro.

## 9.2 Informazioni sulla Fondazione Innovate Europe (IE.F)

L'IE.F è un think tank indipendente guidato da un gruppo di figure di spicco del mondo tecnologico europeo che si sono unite per difendere il ruolo dell'Europa nell'economia globale. Con sede a Berlino, opera come organizzatore di forum e interlocutore privilegiato, sostenendo gli interessi dell'economia digitale e tecnologica europea.

## 9.3 Informazioni su iconomy

iconomy è una società di consulenza e venture builder con sede a Berlino che opera all'incrocio tra la politica industriale europea e la regolamentazione digitale. Profondamente radicata nell'ecosistema europeo delle startup e delle scaleup e situata al crocevia tra venture building e regolamentazione digitale, iconomy fornisce consulenza ai clienti e sostiene gli imprenditori nelle fasi critiche dei mercati tecnologici più importanti dal punto di vista strategico in Europa.

## 9.4 Copyright e citazioni

 Il presente articolo può essere citato come IE.F and SAFENet Coalition, Who Controls Europe's Internet? | Home Routers, Supply Chain Risk and the Case for European Action (IE.F, May 2026).

## Editore

**Innovate Europe Foundation (IE.F)**
Schönhauser Allee 43a
10435 Berlino
www.ie.foundation

## Autori

**Clark Parsons**
IE.F

**Gustav Robrahn**
iconomy

**Kira Terstappen-Richter**
SAFENet

## Contatti

Clark Parsons
Fondazione Innovate Europe (IE.F)
c.parsons@ie.foundation

## Pubblicazione

Giugno 2026