

DOSSIER TECNICO – 18.11.2026

# Cybersicurezza: affrontare le nuove minacce ibride tra competenze e tecnologie

*A cura di Imprese di Talento, Public Affairs & Policy Advisory*

## Cybersicurezza: affrontare le nuove minacce ibride tra competenze e tecnologie

*La cybersicurezza italiana dipenderà sia dalla capacità di difendersi da minacce sempre più sofisticate, sia dalla capacità di trasformare competenze, infrastrutture sicure e il coordinamento istituzionale in resilienza strutturale*.

Le minacce ibride fanno ormai parte della sicurezza quotidiana, sia in Italia sia all'estero. I recenti falsi allarmi bomba nelle scuole italiane dimostrano che anche strumenti semplici possono causare disservizi, creare allarme tra le persone e rendere difficile il coordinamento, soprattutto se impiegati nell'ambito di campagne più ampie volte a destabilizzare. Non tutti gli attacchi informatici sono minacce ibride. Se però si uniscono a sabotaggi, disinformazione o altre forme di pressione, possono diventare strumenti per colpire l'economia, la società e le istituzioni.
Il rischio aumenta perché l'innovazione va più veloce delle competenze necessarie a governarla: l'intelligenza artificiale rende gli attacchi più accessibili e meno costosi, mentre la diffusione di dispositivi connessi, insieme a infrastrutture e competenze obsolete, amplia la superficie di attacco. Il digitale entra in ogni aspetto della vita economica e sociale, dalla scuola agli ospedali, dai trasporti alle imprese fino ai singoli cittadini, la sicurezza informatica è diventata una necessità trasversale.
In questa prospettiva, la resilienza del sistema italiano si basa su tre variabili: il patrimonio di competenze, la resilienza tecnologica delle infrastrutture e l'evoluzione della minaccia. Le prime due si possono rafforzare con interventi specifici e politiche strutturali; la terza resta in gran parte esterna, perché non è del tutto prevedibile né controllabile. Conta quindi non solo come cambieranno le minacce, ma anche quanto velocemente il Paese riuscirà ad adattarsi; dal divario tra la complessità degli attacchi e la capacità di prevenirli, riconoscerli e contenerli dipendono la continuità dei servizi essenziali, la competitività economica e la fiducia nelle istituzioni.

## Analisi: le due variabili che dipendono da noi

### Competenze

La mancanza di competenze digitali rende il sistema nazionale più vulnerabile ai rischi legati all'innovazione tecnologica e limita la capacità di sfruttarne i vantaggi. In Italia, le competenze digitali sono ancora sotto la media europea: secondo i dati 2025 della Commissione europea, solo il 54,3% della popolazione ha almeno competenze digitali di base, contro il 60,4% nell'UE, e gli specialisti ICT rappresentano il 3,8% degli occupati, mentre la media europea è del 5%. Queste differenze evidenziano una debolezza del capitale umano digitale, che può limitare la capacità di adottare e gestire tecnologie avanzate, come l'intelligenza artificiale.
A peggiorare il quadro contribuiscono l'assenza di una strategia organica, la formazione limitata del personale e la diffusa inconsapevolezza digitale tra gli utenti; tali fattori si traducono anche in errori banali, come l'uso di password troppo deboli. La mancanza di competenze non riguarda solo gli utenti, ma anche le organizzazioni, che spesso non riescono a valutare i rischi, a gestire gli incidenti o a utilizzare efficacemente le tecnologie disponibili.

### Tecnologia

Sul piano tecnologico, la vulnerabilità dipende da quanto le infrastrutture digitali riescono a prevenire, gestire e superare gli attacchi; sistemi obsoleti, aggiornamenti rari, scarsa ridondanza e procedure tecniche di ripristino inadeguate possono mettere a rischio la continuità operativa, soprattutto nei settori essenziali. Contano anche le dipendenze da fornitori tecnologici critici; se pochi fornitori concentrano troppi servizi, eventuali disservizi possono avere effetti a catena sulla popolazione e sull'economia.
A ciò si aggiunge che la mancata implementazione degli aggiornamenti e l'insufficiente investimento nell'innovazione tecnologica determinano, da una parte, un aumento del rischio di malfunzionamenti e, dall'altra, una maggiore esposizione delle infrastrutture agli attacchi informatici.
Non basta, tuttavia, disporre di tecnologie avanzate: occorre saperle integrare, aggiornare e governare; investimenti privi di competenze adeguate possono produrre una sicurezza soltanto apparente, mentre

la combinazione di entrambe le leve può trasformare la resilienza digitale in un fattore di competitività industriale.

## La variabile esterna: una minaccia che cambia

Gli attacchi che hanno colpito i sistemi di refrigerazione della grande distribuzione e le celle di conservazione del sangue in Francia, insieme ai falsi allarmi bomba su aerei e nelle scuole, seguono una tendenza precisa: creare disservizi e disagi su larga scala senza rientrare nella definizione tradizionale di aggressione armata. I dati mostrano che il fenomeno è in aumento: Clusit riporta che nel 2025 si sono verificati 5.265 incidenti gravi nel mondo, di cui 507 in Italia, con un aumento del 42% rispetto all'anno precedente. Nel primo semestre del 2026 i casi sono saliti a 4.911, il 71% in più rispetto allo stesso periodo del 2025; in Italia, nello stesso semestre, gli incidenti sono stati 245, in leggero calo rispetto ai 280 dello stesso periodo del 2025; il settore più colpito resta quello manifatturiero. Nonostante la diminuzione a livello nazionale, la rapida crescita globale resta un fattore rilevante.
A rendere la minaccia più insidiosa concorrono due fattori. Il primo è l'attribuzione: identificare con certezza i responsabili, soprattutto quando operano tramite infrastrutture e intermediari digitali, richiede indagini complesse e cooperazione internazionale. Il secondo è l'intelligenza artificiale, sul cui peso le valutazioni divergono: per Clusit non è ancora il fattore determinante della crescita, ma un potenziale acceleratore; per Marco Mazzaglia, docente del Politecnico di Torino, sta già accelerando drasticamente la capacità di violare i sistemi; per ENISA moltiplica tanto le capacità offensive quanto quelle difensive. In ogni caso, la possibilità di automatizzare le attività offensive, ridurne i costi e ampliarne la portata espone al rischio che la capacità degli aggressori cresca più rapidamente di quella di chi è chiamato a difendersi.
Rilevante è anche il costo economico: secondo le stime di Hackmanac, nel primo semestre 2026 i danni associati agli attacchi in Italia ammontano a circa 468 milioni di dollari, cui si aggiungono interruzioni dell'attività, spese di ripristino, conseguenze reputazionali e, nei servizi essenziali, effetti che ricadono direttamente sulla collettività. Proprio perché non è controllabile, l'evoluzione della minaccia è la variabile che più condiziona gli impatti: la stessa vulnerabilità può produrre effetti molto diversi a seconda che la minaccia resti contenuta o entri in una fase di escalation.

## Impatti

Gli effetti delle minacce cyber e ibride non dipendono soltanto dalla gravità del singolo attacco, ma anche dalla centralità del settore colpito e dalla sua interdipendenza con altri servizi essenziali. Il rischio maggiore emerge quando un'interruzione circoscritta ha ripercussioni su più livelli del sistema economico e sociale.

IMPATTI

## Gli effetti delle minacce cyber e ibride per settore

| SETTORE | Minaccia contenuta | Minaccia in escalation |
|---|---|---|
| Scuola | Interruzioni della didattica, falsi allarmi, esposizione di dati di studenti, famiglie e dipendenti | Allarmi coordinati su scala nazionale, blocchi prolungati dei servizi, sfiducia delle famiglie |
| Sanità | Ransomware su strutture ospedaliere, rinvio di prestazioni | Compromissione di catene critiche, rischi diretti per i pazienti |
| Trasporti | Disservizi su biglietteria e informazione ai passeggeri, rallentamento dei servizi | Compromissione dei sistemi informativi e, nei casi più gravi, dei sistemi di controllo operativo, con possibili interruzioni prolungate della mobilità |
| Energia | Attacchi ai sistemi informativi aziendali | Compromissione dei sistemi di controllo degli impianti e delle reti, con possibili interruzioni locali della fornitura |
| Industria | Fermi produttivi e furto di proprietà intellettuale | Compromissione dei sistemi industriali connessi e di controllo dei processi produttivi, con possibili interruzioni della produzione e delle filiere |
| PA | DDoS e indisponibilità dei servizi online | Paralisi di servizi essenziali, compromissione su larga scala dei dati dei cittadini |
| Cittadini | Truffe o phishing | Deepfake, disinformazione mirata, episodi di panico collettivo |

*Elaborazione Imprese di Talento.*

*Nota: gli impatti descritti rappresentano conseguenze potenziali, la cui gravità dipende dalla natura dell'attacco, dalle vulnerabilità dei sistemi colpiti e dalla capacità di risposta. Negli ambiti industriali e infrastrutturali, la compromissione dei sistemi di controllo operativo (OT) può avere ripercussioni anche sui processi fisici e sulla continuità dei servizi.*

La criticità maggiore riguarda la possibilità che incidenti inizialmente circoscritti producano effetti a catena. Un'interruzione delle infrastrutture digitali o energetiche può propagarsi ai trasporti, alla sanità e ai processi produttivi; se accompagnata da campagne di disinformazione o da falsi allarmi, tale evento può inoltre amplificare la percezione di insicurezza e compromettere la fiducia nelle istituzioni. Il rischio cyber assume così una dimensione sistemica, economica e politica.

## Scenari

Dall'incrocio tra competenze, resilienza tecnologica ed evoluzione delle minacce emergono otto possibili scenari per la cybersicurezza italiana. Il modello considera due dimensioni su cui il Paese può intervenire: da un lato, le capacità umane e organizzative; dall'altro, la robustezza delle infrastrutture e la loro capacità di resistere agli attacchi e di garantire il ripristino dei servizi. La terza variabile, rappresentata dall'evoluzione della minaccia, rimane esterna. Gli scenari non costituiscono previsioni, ma configurazioni qualitative utili a valutare le conseguenze di diverse scelte strategiche.




*Elaborazione Imprese di Talento. Valutazioni qualitative, non previsioni.*




*Elaborazione Imprese di Talento. Valutazioni qualitative, non previsioni.*

*Nota metodologica: gli scenari e i relativi livelli di rischio rappresentano valutazioni qualitative, non previsioni probabilistiche. Per autonomia tecnologica si intende la capacità di governare, integrare e mantenere tecnologie sicure e interoperabili, non necessariamente la loro produzione nazionale.*

Gli scenari evidenziano che il rafforzamento tecnologico, da solo, non garantisce una maggiore sicurezza. In assenza di competenze adeguate, anche le infrastrutture avanzate possono risultare vulnerabili agli errori umani e organizzativi; allo stesso tempo, competenze elevate non bastano a compensare sistemi obsoleti o privi di adeguate misure di protezione. La condizione più favorevole emerge quando le capacità umane e la resilienza tecnologica si rafforzano reciprocamente, consentendo di contenere gli incidenti e garantire la continuità dei servizi anche in presenza di minacce più sofisticate.




*Nota metodologica: Le traiettorie sono illustrative e non costituiscono proiezioni statistiche; il passaggio tra gli scenari dipende da ipotesi relative agli investimenti, alle capacità organizzative e alla loro attuazione nel tempo. I due esiti del 2041 dipendono dall'evoluzione della minaccia, che può cambiare anche prima di tale data.*

Le tre traiettorie mostrano come scelte diverse possano produrre risultati progressivamente divergenti. Un approccio prevalentemente reattivo tende a mantenere il Paese in una condizione di vulnerabilità strutturale; gli investimenti concentrati sulle competenze possono migliorare la resilienza, senza però risolvere le dipendenze tecnologiche. Una strategia integrata, invece, può rafforzare progressivamente la capacità nazionale di prevenzione, di risposta e di sviluppo industriale. La differenza tra le traiettorie non riguarda quindi soltanto le risorse investite, ma anche la continuità e la coerenza delle politiche adottate.
La direzione intrapresa dall'Italia potrà essere valutata in base all'evoluzione delle competenze specialistiche, delle dipendenze tecnologiche e della capacità di prevenire e gestire gli incidenti; saranno questi gli indicatori decisivi per comprendere se il Paese stia procedendo verso una maggiore resilienza o stia mantenendo vulnerabilità strutturali.

## Dove si colloca l'italia oggi?

Le evidenze disponibili delineano un quadro articolato: secondo il Digital Decade 2026 della Commissione europea, l'Italia presenta livelli di competenze digitali inferiori alla media dell'UE: il 54,3% della popolazione possiede almeno competenze di base, contro il 60,4% a livello europeo, mentre gli specialisti ICT rappresentano il 3,8% degli occupati, rispetto al 5% dell'Unione. La valutazione della resilienza tecnologica risulta invece più complessa: alla diffusione di infrastrutture e servizi digitali

avanzati si aggiungono vulnerabilità legate all'obsolescenza di alcuni sistemi, all'eterogeneità delle misure di protezione e alle dipendenze tecnologiche critiche.
Il quadro non è tuttavia univocamente negativo: nel Global Cybersecurity Index 2024 dell'ITU, l'Italia figura nella fascia più alta per l'impegno istituzionale nella cybersicurezza. Emerge quindi una possibile distanza tra il rafforzamento delle capacità nazionali di governance e la diffusione delle competenze all'interno del sistema economico e sociale.
Nel modello proposto, queste condizioni suggeriscono una possibile prossimità allo scenario di «Esposizione cronica», pur non consentendo una collocazione quantitativa definitiva.

L'attenzione istituzionale è confermata anche dall'informativa urgente tenutasi il 18 novembre alla Camera dei deputati del Ministro della Difesa, Guido Crosetto, sulla guerra ibrida e cognitiva, che ha delineato il quadro delle minacce emergenti e le relative implicazioni per la sicurezza nazionale.

Il Ministro ha fotografato una minaccia che si articola in modo coordinato su diversi livelli (militare, economico e informativo) con l'obiettivo di frammentare la società ed erodere progressivamente la fiducia nelle istituzioni. La combinazione di disinformazione, algoritmi e intelligenza artificiale, unitamente a tecniche di profilazione sempre più sofisticate consente di orientare comportamenti e decisioni collettive, spesso in modo impercettibile ai destinatari stessi; da qui deriva la necessità, sottolineata dal Ministro, di superare un approccio meramente reattivo a favore di una strategia preventiva, capace di individuare tempestivamente le campagne ostili e di aumentare il costo delle azioni avverse per gli attori critici.
In questa prospettiva, nessuna istituzione può realisticamente sostenere da sola l'onere di tale strategia: sono pertanto indispensabili la collaborazione tra gli enti, la cooperazione in ambito europeo e G7, nonché investimenti mirati allo sviluppo delle competenze, dalla formazione di specialisti cyber militari fino all'educazione digitale nelle scuole. Tali indicazioni risultano pienamente coerenti con alcune delle leve individuate nell'analisi: diffusione delle competenze, capacità di rilevamento e di risposta, protocolli e comunicazione coordinata.

Nel corso dell'intervento è emerso, inoltre, che il confronto tra le diverse forze politiche di maggioranza e di opposizione su questi temi si è sviluppato in modo costruttivo, a conferma della trasversalità della questione e del suo limitato grado di politicizzazione; come sottolineato dal Ministro, infatti, gli attori ostili fanno leva sulle divisioni interne, mentre la natura di tali minacce prescinde da qualsiasi appartenenza politica.

## Conclusione

Le prossime scelte si inseriscono in un'agenda già definita. A livello europeo, il pacchetto presentato dalla Commissione il 20 gennaio 2026 (revisione del Cybersecurity Act, modifiche mirate alla NIS2 e rafforzamento di ENISA) è in esame presso il Parlamento europeo, con particolare attenzione alla certificazione e alla sicurezza delle catene di approvvigionamento. La revisione potrebbe incidere non soltanto sugli obblighi di sicurezza, ma anche sui criteri di affidabilità delle filiere e sulla competitività delle imprese del mercato digitale. In Italia, la scadenza della Strategia nazionale di cybersicurezza 2022-2026 rappresenta l'occasione per valutare i risultati raggiunti e fissare le priorità per i prossimi anni: lo sviluppo delle competenze, la riduzione delle dipendenze tecnologiche critiche e la capacità di risposta agli incidenti. Sul fronte delle risorse, il Ministro dell'Economia Giancarlo Giorgetti ha auspicato che le regole europee consentano di includere le spese per la difesa dagli attacchi informatici nella clausola nazionale di salvaguardia (NEC) per la difesa; un'apertura in questa direzione amplierebbe gli spazi per l'investimento pubblico nel settore.
Gli strumenti, tuttavia, contano quanto la loro continuità. Lo stanziamento di 12 milioni di euro da parte del Ministero dell'Università e della Ricerca per progetti di cybersicurezza è un intervento positivo; resta aperta la possibilità di tradurre le iniziative settoriali in un rafforzamento strutturale delle competenze, attraverso la formazione continua, il trasferimento tecnologico e il coordinamento tra università, imprese e pubbliche amministrazioni. Investire nella cybersicurezza, inoltre, non è soltanto

una spesa di protezione: può diventare un'opportunità di crescita, anche grazie a servizi esportabili, intrecciando così la dimensione difensiva con quella industriale. Resilienza tecnologica e autonomia strategica restano obiettivi complementari ma distinti: la prima riguarda la capacità di proteggere e mantenere operativi i sistemi; la seconda, il controllo delle dipendenze critiche e la valorizzazione delle capacità industriali nazionali ed europee.
Infine, la dimensione cognitiva delle minacce ibride, cioè la manipolazione delle informazioni attraverso strumenti digitali, resa più rapida e insidiosa dall'intreccio tra i social media e l'intelligenza artificiale, impone di considerare la sicurezza dell'ecosistema informativo come parte della resilienza democratica, soprattutto nei periodi elettorali. Servono regole efficaci da parte delle istituzioni e delle piattaforme, competenze tecniche per individuare le campagne coordinate e una maggiore consapevolezza degli utenti; serve anche una comunicazione istituzionale tempestiva e coordinata. Lo ha mostrato l'emergenza dei falsi allarmi nelle scuole: le diverse reazioni iniziali hanno evidenziato difficoltà di coordinamento e di valutazione del rischio. Il Governo ha risposto con indicazioni che hanno culminato nella direttiva del Ministero dell'Interno del 13 novembre, che introduce criteri comuni per la gestione di segnalazioni massicce e potenzialmente infondate.

## Punti chiave

- **Leve sulle competenze:** definire una strategia organica per lo sviluppo delle competenze digitali e specialistiche; rafforzare la formazione continua nella PA e nelle imprese; promuovere la consapevolezza digitale dei cittadini, a partire dalla scuola.
- **Leve sulla tecnologia:** accelerare l'aggiornamento e la messa in sicurezza delle infrastrutture; rafforzare la ridondanza, le capacità di ripristino e la continuità operativa; ridurre la concentrazione delle dipendenze tecnologiche critiche e sostenere lo sviluppo di soluzioni italiane ed europee competitive e affidabili.
- **Preparazione alla minaccia:** adottare protocolli condivisi per la prevenzione, la gestione e la comunicazione delle crisi; rafforzare le capacità di rilevamento, risposta e attribuzione degli attacchi; sviluppare procedure operative comuni nei settori essenziali, con particolare attenzione alle scuole, alla sanità e alle pubbliche amministrazioni.

La priorità non è quindi soltanto aumentare gli investimenti, ma garantirne il coordinamento e la continuità nel tempo: questi fenomeni non sono più emergenze isolate, ma una nuova normalità, che richiede strategie sistemiche e strutturali capaci di tradurre il rafforzamento delle competenze e delle capacità tecnologiche in una maggiore resilienza del sistema Paese.

## Fonte


• Commissione europea, *Proposta di regolamento relativo all'Agenzia dell'Unione europea per la cibersicurezza (ENISA), al quadro europeo di certificazione della cibersicurezza e alla sicurezza delle catene di approvvigionamento ICT (Cybersecurity Act 2)*, COM(2026) 11 final, 20 gennaio 2026.
• Commissione europea, *Proposta di direttiva che modifica la direttiva (UE) 2022/2555 (NIS2) per quanto riguarda misure di semplificazione e l'allineamento al Cybersecurity Act 2*, COM(2026) 13 final, 20 gennaio 2026.
• Commissione europea, *Commission strengthens EU cybersecurity resilience and capabilities*, comunicato del 20 gennaio 2026.
• Parlamento europeo, Osservatorio legislativo, procedura 2026/0011(COD), *Cybersecurity Act 2*, documentazione relativa all'iter della proposta COM(2026) 11.
• Parlamento europeo, *European Software and Cyber Dependencies*, studio sulle dipendenze tecnologiche e digitali dell'Unione europea, 2025.
• ENISA – Agenzia dell'Unione europea per la cibersicurezza, *ENISA Threat Landscape 2026*, 22 settembre 2026.
• ENISA – Agenzia dell'Unione europea per la cibersicurezza, *ENISA Threat Landscape 2025*, 2025.
• ENISA – Agenzia dell'Unione europea per la cibersicurezza, *2024 Report on the State of Cybersecurity in the Union*, dicembre 2024.

• ENISA – Agenzia dell'Unione europea per la cibersicurezza, *The EU Cybersecurity Index 2024*, rapporto sulla postura di cybersicurezza degli Stati membri e dell'Unione europea, 2024.
• CLUSIT – Associazione Italiana per la Sicurezza Informatica, *Rapporto Clusit 2026 sulla sicurezza ICT in Italia e nel mondo*, marzo 2026.