



Cybersecurity: l'Esercito Italiano potrà assumere hacker per operazioni digitali

Pubblicato il 20/09/2025

È stato presentato alla Camera dei Deputati un disegno di legge che amplia il ruolo delle **Forze armate nel dominio cibernetico**, riconosciuto ormai come un vero e proprio **spazio strategico** al pari di terra, mare, aria e spazio. Il provvedimento, primo firmatario il presidente della Commissione Difesa **Nino Minardo**, nasce in un contesto segnato dal forte incremento delle **minacce digitali** rilevato dall'Agenzia per la Cybersicurezza Nazionale (ACN).

Il contesto: minacce in crescita

Secondo l'**Operational Summary dell'ACN**, nei primi sei mesi del 2025 sono stati registrati **1.549 eventi cyber** (+53% rispetto al 2024), di cui **346 con impatto confermato**. Particolarmente significativo l'aumento degli **attacchi DDoS** (598 episodi), mentre i casi di **ransomware** restano stabili ma con effetti rilevanti su settori sensibili come pubblica

amministrazione, sanità, università ed energia.

Alla luce di questi dati, il ddl attribuisce alla Difesa la possibilità di condurre **operazioni digitali anche in tempo di pace**, rafforzando la capacità di protezione di **istituzioni, infrastrutture critiche e cittadini**.

I punti salienti del disegno di legge

Il provvedimento introduce alcune novità di rilievo:

- **Operazioni digitali delle Forze armate:** facoltà di intervenire in scenari di crisi anche non bellici, con procedure autorizzative chiare e coordinamento con le autorità civili.
- **Formazione militare:** inserimento di percorsi specifici di **cyber defence** nelle scuole e negli istituti militari.
- **Supporto esterno qualificato:** possibilità di avvalersi di esperti altamente specializzati (anche hacker), attraverso meccanismi di ingaggio vigilati da strutture pubbliche.
- **Controllo democratico:** obbligo per il **ministro della Difesa** di riferire periodicamente alle Commissioni parlamentari e al COPASIR.

Cyber spazio come dominio strategico

Il riconoscimento del **cyber spazio** come dominio operativo risale al vertice **NATO di Varsavia 2016**, rafforzato a Bruxelles nel 2018 con la creazione del **Cyber Operations Center**. L'Italia, allineandosi a questo percorso, intende consolidare la propria postura difensiva e offensiva in un settore cruciale per la sicurezza nazionale ed euro-atlantica.

Aspetti giuridici e cautele

Il ddl richiede una definizione precisa delle condizioni in cui le Forze armate potranno intervenire **in tempo di pace**: catena di comando, livelli autorizzativi, raccordo con l'autorità giudiziaria. Particolare attenzione dovrà essere riservata all'uso di **esperti esterni**, con criteri di affidabilità, trasparenza nella gestione di informazioni classificate e tracciabilità delle operazioni.

Coordinamento con l'ecosistema civile

La Difesa non agirà in autonomia, ma in stretto raccordo con **ACN, CSIRT Italia** e altre strutture settoriali, per evitare duplicazioni e garantire continuità operativa. L'intervento militare dovrà inserirsi nei piani nazionali di risposta, con **protocolli di cooperazione** e **piattaforme di condivisione dati**.

Formazione e resilienza

Il rafforzamento dei percorsi formativi mira a creare **competenze stabili** e a ridurre la dipendenza da soluzioni emergenziali. La possibilità di ricorrere a **supporti esterni specializzati** resta uno strumento di flessibilità, da utilizzare entro **regole di ingaggio rigorose** e coerenti con gli obiettivi pubblici.

Prospettive

L'iniziativa legislativa si colloca lungo una traiettoria che vede la **cybersicurezza** come elemento cardine della difesa nazionale e internazionale. La combinazione di **capacità interne, supporto esterno, formazione e controllo parlamentare** potrebbe contribuire a colmare il divario di competenze e a incrementare la **resilienza del sistema Paese**.

L'iter parlamentare definirà in dettaglio condizioni operative, limiti e responsabilità, assicurando coerenza con l'ordinamento interno e con gli impegni internazionali.

Link notizia: <https://www.cybersecurity360.it/news/cyber-security-e-difesa-il-ddl-minardo-su-hacker-e-forze-armate-i-punti-essenziali/>