CAMERA DEI DEPUTATI N. **2425**

PROPOSTA DI LEGGE

d'iniziativa del deputato MULÈ

Modifiche al codice dell'ordinamento militare, di cui al decreto legislativo 15 marzo 2010, n. 66, e all'articolo 1 della legge 21 luglio 2016, n. 145, nonché introduzione dell'articolo 7-*quater* del decreto-legge 30 ottobre 2015, n. 174, convertito, con modificazioni, dalla legge 11 dicembre 2015, n. 198, concernenti lo spazio cibernetico di interesse nazionale per la difesa e la sicurezza dello Stato e le operazioni delle Forze armate in ambito cibernetico

Presentata il 27 maggio 2025

Onorevoli Colleghi ! – Il quadro normativo nazionale sul tema della difesa e della sicurezza dello Stato in ambito cibernetico, costituito da una serie di provvedimenti diretti a garantire unicità di indirizzo rispetto a un'area di intervento oggettivamente trasversale, necessita di una serie di modifiche volte a consentire al comparto della difesa di pianificare e condurre, nello spazio cibernetico e tramite lo stesso, operazioni militari difensive e offensive, anche in tempo di pace, sia nelle situazioni di conflitto conclamate, ossia di attacco armato, sia nei casi di attacchi alle infrastrutture critiche e, più in generale, agli interessi vitali del Paese, cosiddetti attacchi « sottosoglia ».

Procedendo in tal senso, giova riferire che, sotto un profilo squisitamente giuridico, la materia, ad oggi, è disciplinata:

a) dal codice dell'ordinamento militare, di cui al decreto legislativo 15 marzo 2010, n. 66, e, in particolare, dall'articolo 88, comma 1, ai sensi del quale « lo strumento militare è volto a consentire la permanente disponibilità di strutture di comando e controllo di Forza armata e interforze [...] preposte alla difesa del territorio nazionale, delle vie di comunicazione marittime e aeree, delle infrastrutture spaziali e dello spazio cibernetico in ambito militare »;

b) dal decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla

legge 18 novembre 2019, n. 133, recante disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica e di disciplina dei poteri speciali nei settori di rilevanza strategica, che mira ad assicurare un livello elevato di sicurezza delle reti, dei sistemi informativi e dei servizi informatici delle amministrazioni pubbliche, nonché degli enti e degli operatori nazionali, pubblici e privati, consentendo, al contempo, la più estesa fruizione dei più avanzati strumenti offerti dalle tecnologie dell'informazione e della comunicazione;

c) dal decreto-legge 14 giugno 2021, n. 82, convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109, che, nel riformare l'architettura nazionale di cybersicurezza e, più precisamente, nel prevedere il Presidente del Consiglio dei ministri quale vertice di tale struttura e organo di indirizzo politico-strategico, ha istituito:

il Comitato interministeriale per la cybersicurezza con funzioni di consulenza, proposta e vigilanza circa l'attuazione delle politiche in materia di cybersicurezza;

l'Agenzia per la cybersicurezza nazionale nell'ottica di coordinare il livello politico-strategico con gli attori coinvolti in materia e, dunque, al fine di promuovere iniziative coerenti ed una postura nazionale unitaria;

il Nucleo per la cybersicurezza a supporto del Presidente del Consiglio dei ministri per gli aspetti relativi alla prevenzione e alla preparazione a eventuali situazioni di crisi;

d) dal decreto-legge 30 ottobre 2015, n. 174, convertito, con modificazioni, dalla legge 11 dicembre 2015, n. 198, e, in particolare, dall'articolo 7-*ter* (introdotto dall'articolo 37 del decreto-legge 9 agosto 2022, n. 115, convertito, con modificazioni, dalla legge 21 settembre 2022, n. 142, cosiddetto « decreto aiuti-*bis* ») in forza del quale il Presidente del Consiglio dei ministri emana « disposizioni per l'adozione di misure di *intelligence* di contrasto in ambito cibernetico, in situazioni di crisi o di emergenza a fronte di minacce che coinvolgono aspetti di sicurezza nazionale e non siano fronteggiabili solo con azioni di resilienza [...]. Le disposizioni [...] prevedono la cooperazione del Ministero della difesa e il ricorso alle garanzie funzionali di cui all'articolo 17 della legge 3 agosto 2007 n. 124 »; il medesimo articolo 7-*ter* prevede altresì che: « Le misure di contrasto in ambito cibernetico [...] sono attuate dall'Agenzia informazioni e sicurezza esterna e dall'Agenzia informazioni e sicurezza interna, ferme restando le competenze del Ministero della difesa ai sensi dell'articolo 88 del codice dell'ordinamento militare »;

e) dalla legge 28 giugno 2024, n. 90, recante disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici, che, oltre a dettare norme per sviluppare la capacità nazionale di prevenzione degli incidenti di sicurezza informatica e degli attacchi informatici, nonché di risposta agli stessi, inasprisce la disciplina sanzionatoria in relazione ad alcuni reati, tra cui, a titolo esemplificativo, l'articolo 615-*ter* del codice penale in materia di accesso abusivo a un sistema informatico o telematico;

f) dalla Strategia nazionale di cybersicurezza, di cui all'articolo 9 del decreto legislativo 4 settembre 2024, n. 138, predisposta dall'Agenzia per la cybersicurezza nazionale;

g) dal piano di attuazione della citata Strategia nazionale di cybersicurezza che prevede, per ciascun obiettivo e fattore abilitante, una serie di misure in materia di cybersicurezza da realizzare entro l'anno 2026;

h) dal citato decreto legislativo 4 settembre 2024, n. 138, recante il recepimento della direttiva (UE) 2022/2555, relativa a misure per un livello comune elevato di cibersicurezza nell'Unione (direttiva NIS 2 – *Network and Information Security 2)*, in forza del quale l'Agenzia per la cybersicurezza nazionale è stata riconosciuta quale Autorità nazionale di gestione delle crisi informatiche, per la parte relativa alla resilienza nazionale con funzioni di coordinatore, e il Ministero della difesa è stato riconosciuto quale Autorità nazionale di

gestione delle crisi informatiche, per la parte relativa alla difesa dello Stato, trattandosi di un compito prioritario attribuito dagli articoli 15 e 89 del codice dell'ordinamento militare.

A fronte del citato quadro giuridico di riferimento, che non consente di definire in maniera compiuta le azioni e le operazioni militari da condurre nello spazio cibernetico e tramite lo stesso, appare necessario:

abilitare le azioni e le capacità del comparto della difesa per l'identificazione, la mitigazione e il contrasto delle minacce cibernetiche, dirette o indirette, alla sicurezza nazionale;

legittimare le Forze armate all'utilizzo degli strumenti cibernetici sia nelle ipotesi di risposta alle crisi in cui la gestione e il relativo coordinamento sono in capo al Ministero della difesa sia nelle operazioni promosse in concorso con le autorità civili;

allineare il ruolo del Ministero della difesa a quello del comparto dell'*intelligence* nei casi di adozione e attuazione delle misure di *intelligence* di contrasto in ambito cibernetico in situazioni di crisi o di emergenza;

prevedere lo svolgimento di attività di *intelligence* preparatorie nell'imminenza di un attacco cibernetico a prescindere dall'esistenza di una situazione di crisi o di emergenza e dalla possibilità di fronteggiare tale crisi con azioni di resilienza;

estendere le garanzie funzionali di cui all'articolo 17 della legge 3 agosto 2007, n. 124, al personale delle Forze armate impiegato nella conduzione di operazioni militari nel dominio cibernetico, in territorio nazionale e all'estero, anche quando non opera congiuntamente con il personale addetto ai servizi di informazione per la sicurezza.

Del resto l'attuale contesto geopolitico e gli incidenti già occorsi, anche in ambito nazionale, hanno dimostrato l'insufficienza degli attuali meccanismi tesi a fronteggiare le emergenze; qualsiasi incidente di sicurezza cibernetica su vasta scala o crisi cibernetica può celare una campagna malevola articolata compiuta da Stati ovvero da attori non statali. Per tali ragioni lo strumento militare non può non assumere un ruolo preminente, fin dalle prime evidenze di tali accadimenti, in quanto potenzialmente suscettibili di evolvere, con immediatezza, in un attacco nei confronti dello Stato e dei suoi interessi vitali.

Nel solco di tali determinanti e, dunque, al fine di garantire al comparto della difesa il livello di autonomia operativa necessario per fronteggiare un dominio sempre più conflittuale, la presente proposta di legge, composta da quattro articoli, apporta puntuali modifiche al codice di cui al decreto legislativo 15 marzo 2010, n. 66 (articolo 1), al decreto-legge 30 ottobre 2015, n. 174, convertito, con modificazioni, dalla legge 11 dicembre 2015, n. 198, recante proroga delle missioni internazionali delle Forze armate e di polizia, iniziative di cooperazione allo sviluppo e sostegno ai processi di ricostruzione e partecipazione alle iniziative delle organizzazioni internazionali per il consolidamento dei processi di pace e di stabilizzazione (articolo 2), e alla legge 21 luglio 2016, n. 145, recante disposizioni concernenti la partecipazione dell'Italia alle missioni internazionali (articolo 3), nonché dispone l'invarianza finanziaria del provvedimento.

In particolare, l'articolo 1, comma 1, della presente proposta di legge apporta al codice di cui al decreto legislativo 15 marzo 2010, n. 66, le seguenti modifiche:

alla lettera *a)*, modifica l'articolo 10, comma 1, attribuendo al Ministro della difesa i compiti concernenti l'identificazione e l'aggiornamento periodico dello spazio cibernetico di interesse nazionale per la difesa e la sicurezza dello Stato;

alla lettera *b)*, integra l'articolo 15, comma 2, inserendo tra i compiti e le funzioni del Ministero della difesa la difesa e sicurezza, sin dal tempo di pace, delle infrastrutture spaziali, delle infrastrutture critiche e dello spazio cibernetico di interesse nazionale per la difesa e la sicurezza dello Stato;

alla lettera *c)*, introduce l'articolo aggiuntivo 15-*bis* che reca la definizione di

spazio cibernetico di interesse nazionale per la difesa e la sicurezza dello Stato, inteso come l'insieme delle infrastrutture informatiche e delle relazioni fisiche, logiche e cognitive tra esse, che rappresenta l'ambito entro cui il Ministero della difesa opera per adempiere ai propri compiti istituzionali anche al di fuori dei confini nazionali;

alla lettera *d)*, modifica l'articolo 88, comma 1, assegnando allo strumento militare la responsabilità di organizzare unità specialistiche destinate a operare altresì a difesa dello spazio cibernetico di interesse nazionale per la difesa e la sicurezza dello Stato, estendendone, di fatto, l'ambito di azione oltre il perimetro (ristretto) delle reti militari.

L'articolo 2 introduce l'articolo aggiuntivo 7-*quater* del decreto-legge 30 ottobre 2015, n. 174, convertito, con modificazioni, dalla legge 11 dicembre 2015, n. 198, che estende le garanzie funzionali previste dall'articolo 17 della legge 3 marzo 2007, n. 124, al personale delle Forze armate quando conduce, anche in tempo di pace, operazioni in ambito cibernetico indipendentemente dal fatto che tale personale, come statuito dal comma 7 del medesimo articolo 17 della legge n. 124 del 2007, non sia addetto ai servizi di informazione per la sicurezza né abbia svolto tali attività in concorso con uno o più dipendenti dei servizi di informazione per la sicurezza e che il ricorso alla loro opera da parte dei servizi di informazione per la sicurezza sia risultato indispensabile. Si prevede altresì che al predetto personale si applichino le disposizioni in materia penale previste dall'articolo 19 della legge 21 luglio 2016, n. 145.

L'articolo 3 integra l'articolo 1, comma 1, della legge 21 luglio 2016, n. 145, inserendo nel novero delle missioni internazionali a cui l'Italia partecipa con deliberazione del Consiglio dei ministri, previa comunicazione al Presidente della Repubblica, e autorizzazione delle Camere, anche le missioni finalizzate a operazioni preventive e di contrasto per il controllo e la protezione dello spazio cibernetico di interesse nazionale per la difesa e la sicurezza dello Stato.

L'articolo 4, infine, reca la clausola di invarianza finanziaria.

PROPOSTA DI LEGGE

—

Art. 1.

(Modifiche al codice dell'ordinamento militare, di cui al decreto legislativo 15 marzo 2010, n. 66)

1. Al codice dell'ordinamento militare, di cui al decreto legislativo 15 marzo 2010, n. 66, sono apportate le seguenti modificazioni:

a) all'articolo 10, comma 1, è aggiunta, in fine, la seguente lettera:

« *d-bis)* identifica e periodicamente aggiorna lo spazio cibernetico di interesse nazionale per la difesa e la sicurezza dello Stato di cui all'articolo 15-*bis* »;

b) all'articolo 15, comma 2, dopo le parole: « del territorio nazionale e delle vie di comunicazione marittime e aree » sono inserite le seguenti: « nonché delle infrastrutture spaziali, delle infrastrutture critiche e dello spazio cibernetico di interesse nazionale per la difesa e la sicurezza dello Stato di cui all'articolo 15-*bis* »;

c) dopo l'articolo 15 è inserito il seguente:

« Art. 15-*bis*. – *(Spazio cibernetico di interesse nazionale per la difesa e sicurezza dello Stato) – 1*. Lo spazio cibernetico di interesse nazionale per la difesa e la sicurezza dello Stato è l'insieme delle infrastrutture informatiche IT, comprensive di *hardware*, *software*, capacità, dati, connessioni fisiche e elettromagnetiche, dei sistemi cyber-fisici OT comprensivi di sistemi attuatori di processo, sensori, sistemi di controllo industriale (ICS), apparecchiature mobili dotate di connessione di rete, nonché dei punti di interconnessione, delle rappresentazioni digitali, delle relazioni fisiche, logiche e cognitive stabilite tra essi, entro il quale il Ministero della difesa opera per adempiere i propri compiti istituzionali anche al di fuori dei confini nazionali.

2. Lo spazio cibernetico di interesse nazionale di cui al comma 1 è identificato e periodicamente aggiornato ai sensi dell'articolo 10, comma 1, lettera *d-bis)* »;

d) all'articolo 88, comma 1, le parole: « , delle infrastrutture spaziali e dello spazio cibernetico in ambito militare » sono sostituite dalle seguenti: « , delle infrastrutture spaziali, delle infrastrutture critiche e dello spazio cibernetico di interesse nazionale per la difesa e la sicurezza dello Stato di cui all'articolo 15-*bis* ».

Art. 2.

*(Introduzione dell'articolo 7-*quater *del decreto-legge 30 ottobre 2015, n. 174, convertito, con modificazioni, dalla legge 11 dicembre 2015, n. 198)*

1. Nel capo I del decreto-legge 30 ottobre 2015, n. 174, convertito, con modificazioni, dalla legge 11 dicembre 2015, n. 198, è aggiunto, in fine, il seguente articolo:

« Art. 7-*quater*. – *(Disposizioni in materia di operazioni delle Forze armate in ambito cibernetico) – 1*. Al personale delle Forze armate e al personale civile impiegato dalle Forze armate, impiegato, anche in tempo di pace, nell'assolvimento dei propri compiti istituzionali per la conduzione di operazioni in ambito cibernetico nel territorio nazionale e all'estero, anche quando non opera congiuntamente con il personale addetto ai servizi di informazione per la sicurezza, si applicano le garanzie funzionali di cui all'articolo 17 della legge 3 agosto 2007, n. 124, previa autorizzazione del Presidente del Consiglio dei ministri, o dell'Autorità politica delegata, ove istituita, su richiesta del Ministro della difesa, nel rispetto delle procedure di cui all'articolo 18 della medesima legge n. 124 del 2007, in quanto applicabili.

2. Al personale di cui al comma 1 del presente articolo si applicano altresì le disposizioni dell'articolo 19 della legge 21 luglio 2016, n. 145 ».

Art. 3.

(Modifica all'articolo 1 della legge 21 luglio 2016, n. 145)

1. All'articolo 1, comma 1, della legge 21 luglio 2016, n. 145, dopo le parole: « nonché a missioni finalizzate ad eccezionali interventi umanitari » sono inserite le seguenti: « ovvero a operazioni preventive e di contrasto per il controllo e la protezione delle infrastrutture critiche e dello spazio cibernetico di interesse nazionale per la difesa e la sicurezza dello Stato previsto dall'articolo 15-*bis* del codice dell'ordinamento militare, di cui al decreto legislativo 15 marzo 2010, n. 66 ».

Art. 4.

(Clausola di invarianza finanziaria)

1. Dall'attuazione della presente legge non devono derivare nuovi o maggiori oneri per la finanza pubblica. Le amministrazioni interessate provvedono ai relativi adempimenti nell'ambito delle risorse umane, strumentali e finanziarie disponibili a legislazione vigente.

19PDL0145560