IV COMMISSIONE PERMANENTE

(Difesa)

S O M M A R I O

INDAGINE CONOSCITIVA

Mercoledì 8 novembre 2023. — Presidenza del presidente Antonino MINARDO.

La seduta comincia alle 8.40.

Indagine conoscitiva sulle condizioni di lavoro e di vita dei volontari in ferma prefissata dopo la sospensione del servizio di leva obbligatorio e l'ingresso delle donne nelle Forze Armate, nonché a undici anni dalla legge n. 244 del 31 dicembre 2012 sulla revisione dello strumento militare.

(Deliberazione di una proroga del termine).

Antonino MINARDO, *presidente*, avverte che essendo stata raggiunta l'intesa con il Presidente della Camera, ai sensi dell'articolo 144, comma 1, del Regolamento, sulla proroga del termine dell'indagine conoscitiva « Sulle condizioni di lavoro e di vita dei volontari in ferma prefissata dopo la sospensione del servizio di leva obbligatorio e l'ingresso delle donne nelle Forze Armate, nonché a undici anni dalla legge n. 244 del 31 dicembre 2012 sulla revisione dello strumento militare », la Commissione è chiamata a procedere alla relativa deliberazione.

Se non vi sono obiezioni, pone, pertanto, in votazione la proposta di proroga del termine al 30 aprile 2024 della suddetta indagine conoscitiva.

Nessuno chiedendo di intervenire, la Commissione approva.

Indagine conoscitiva sulla difesa cibernetica: nuovi profili e criticità.

(Deliberazione).

Antonino MINARDO, *presidente*, ricorda che nella riunione del 31 ottobre 2023 l'Ufficio di presidenza, integrato dai rappresentanti dei gruppi, ha convenuto sull'opportunità di procedere allo svolgimento dell'indagine conoscitiva « Sulla difesa cibernetica: nuovi profili e criticità ».

Avverte, quindi, che essendo stata raggiunta l'intesa con il Presidente della Camera ai sensi dell'articolo 144, comma 1, del Regolamento, la Commissione è chiamata a deliberare lo svolgimento di tale indagine sulla base di una proposta di

programma che sarà allegata al resoconto sommario di questa seduta *(vedi allegato)*.

Pone, dunque, in votazione la deliberazione di svolgimento della suddetta indagine conoscitiva.

Nessuno chiedendo di intervenire, la Commissione delibera lo svolgimento dell'indagine conoscitiva.

La seduta termina alle 8.45.

UFFICIO DI PRESIDENZA INTEGRATO DAI RAPPRESENTANTI DEI GRUPPI

Mercoledì 8 novembre 2023.

L'ufficio di presidenza si è riunito dalle 8.45 alle 8.55.

ALLEGATO

Indagine conoscitiva sulla difesa cibernetica: nuovi profili e criticità.

PROGRAMMA

Il tema della difesa cibernetica ha assunto rilevanza crescente in Italia, a fronte dell'elevato numero di gravi attacchi informatici, sia verso soggetti privati, sia contro le Forze armate e la pubblica amministrazione. L'Italia ha affrontato il tema con l'istituzione, nell'ambito della Difesa, del Comando per le Operazioni in Rete (Cor) e, su un piano più generale, con una più ampia riforma della *governance* del settore che, nella scorsa Legislatura, ha portato alla definizione del perimetro di sicurezza cibernetica nazionale e alla creazione dell'Agenzia per la Cybersicurezza Nazionale (Acn).

La difesa cibernetica si sostanzia in uno spettro di competenze dello Stato di natura prettamente militare, da inquadrare in una più ampia strategia nazionale per la sicurezza cibernetica, la cui architettura si è andata componendo grazie a una serie di interventi normativi.

In linea generale, la sicurezza cibernetica a livello europeo è regolata dalla direttiva (UE) 2016/1148 del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione (c.d. direttiva NIS – *Network and Information Security*), al fine di conseguire un « livello elevato di sicurezza della rete e dei sistemi informativi in ambito nazionale, contribuendo ad incrementare il livello comune di sicurezza nell'Unione europea ».

La direttiva è stata recepita nell'ordinamento italiano nella XVIII Legislatura con il decreto legislativo n. 65 del 18 maggio 2018, che detta la cornice legislativa delle misure da adottare per la sicurezza delle reti e dei sistemi informativi ed individua i soggetti competenti per dare attuazione agli obblighi previsti dalla direttiva NIS.

Successivamente, è stato adottato il decreto-legge n. 105 del 2019, al fine di 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, attraverso l'istituzione di un perimetro di sicurezza nazionale cibernetica e la previsione di misure volte a garantire i necessari *standard* di sicurezza rivolti a minimizzare i rischi. Talune modifiche a tale provvedimento sono state apportate dal decreto-legge n. 162 del 2019, in materia di proroga dei termini e altre disposizioni sulla pubblica amministrazione.

Infine, con il decreto-legge n. 82 del 2021, si è proceduto alla definizione dell'architettura nazionale di cybersicurezza e all'istituzione dell'Agenzia per la cybersicurezza nazionale, in attuazione di precisi obiettivi del PNRR. La sicurezza cibernetica costituisce infatti uno dei principali interventi previsti dal Piano nazionale di ripresa e resilienza (PNRR) nell'ambito della trasformazione digitale della P.A. e della digitalizzazione del Paese.

In questo contesto, la Commissione Difesa era stata chiamata ad esprimere il parere sia sul disegno di legge C. 2100, di conversione del decreto-legge n. 105 del 2019, recante disposizioni urgenti in materia di perimetro di sicurezza cibernetica, sia sul disegno di legge (C. 3161), di conversione del decreto-legge n. 82 del 2021, recante disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia nazionale di cybersicurezza. Inoltre, la Commissione ha espresso i propri rilievi anche sullo schema di decreto del Presidente del Consiglio di ministri in materia di perimetro di sicurezza nazionale cibernetica (Atto n. 177), sullo schema di decreto del Presidente del Consiglio di ministri recante regolamento in

materia degli incidenti aventi impatto su reti, sistemi informativi e servizi informatici di cui all'articolo 1, comma 3, lettera *b*) del decreto-legge 21 settembre 2019 n. 105 (Atto n. 246), sullo schema di decreto del Presidente del Consiglio di ministri recante il regolamento di organizzazione e funzionamento dell'Agenzia per la cybersicurezza nazionale (Atto n. 325), nonché sullo schema di decreto del Presidente del Consiglio dei ministri recante il regolamento del personale dell'Agenzia per la cybersicurezza nazionale (Atto n. 326).

Proseguendo sul versante normativo, con specifico riguardo all'ambito di competenza della Commissione Difesa, il decreto-legge n. 50 del 2022 (all'articolo 51, comma 8, lettera *e*) ha aggiunto nell'articolo 88 del Codice dell'ordinamento militare (emanato con il decreto legislativo n. 66 del 2010), oltre ai domini tradizionali (terrestre, marittimo e aereo), anche i domini cibernetico e aero-spaziale tra gli ambiti tutelati dalla difesa nazionale, quale funzione propria e principale dello strumento militare. Sono state al contempo adeguate (alla lettera *f*) le funzioni di concorso delle Forze armate includendo quelle previste, sempre in ambito di cybersicurezza, dall'articolo 5, comma 5, del decreto-legge 14 giugno 2021, n. 82.

Sono state inoltre adottate alcune misure volte a potenziare la capacità di contrasto in ambito cibernetico in situazioni di crisi o emergenza a fronte di minacce che coinvolgano aspetti di sicurezza nazionale e non siano fronteggiabili solo con azioni di resilienza, anche in attuazione di obblighi assunti a livello internazionale. A questo fine si segnala l'articolo 37 del decreto-legge n. 115 del 2022 (c.d. decreto « Aiuti *bis* », come modificato in sede di conversione), che ha attribuito al Presidente del Consiglio il potere di autorizzare l'adozione di particolari misure di intelligence di contrasto in ambito cibernetico.

In linea con le direttrici di sviluppo in ambito NATO, UE e in applicazione del PNRR (Missione M1C1-digitalizzazione, innovazione e sicurezza nella pubblica amministrazione), l'Italia ha quindi avviato un processo inteso a rafforzare le proprie capacità nel dominio cibernetico, comprese quelle militari. Ciò, in particolare, in linea con il NATO *Wales Summit* del 2016, in cui lo spazio cibernetico è riconosciuto come dominio di operazioni da presidiare e difendere, stanti i frequenti attacchi alle reti paragonabili a quelli propri di un conflitto con armi convenzionali.

In particolare, dal momento che riguarda in via esclusiva la c.d. *cyber defence* – intesa come difesa cibernetica di natura militare dello Stato – l'introduzione nel COM della difesa dello spazio cibernetico tra gli ambiti tutelati dalla difesa nazionale opera nel rispetto delle competenze di tutte le altre amministrazioni coinvolte nello specifico settore: *cyber resilience*, in capo all'Agenzia per la Cybersicurezza Nazionale, *cyber intelligence*, di competenza del Dipartimento Informazioni per la Sicurezza e le collegate Agenzie, *cyber crime & investigation*, attestata al Ministero dell'Interno. Allo stesso modo, afferendo esclusivamente ai profili di tutela militare delle infrastrutture spaziali (antenne satelliti strutture per la comunicazione satellitare, ecc.) strettamente connessi alla funzione di difesa nazionale, anche l'inclusione del dominio aerospaziale non implica contrasti o sovrapposizioni di competenze, ma solo l'adeguamento dell'ambito di interesse della difesa nazionale.

Passando al piano internazionale, occorre rilevare come sia i principali alleati NATO sia l'Alleanza nel suo complesso stiano sviluppando un proprio approccio alla *cyber defence*, mentre si apre una riflessione strategica e dottrinale rispetto a questo « nuovo dominio operativo » – definizione da tempo utilizzata proprio in ambito NATO – che deve essere presidiato e difeso al pari dei tradizionali domini operativi. Un dominio nel quale il ruolo della tecnologia e del settore privato cresce in modo esponenziale, richiedendo nuove forme i dialogo e collaborazione tra le istituzioni e l'industria nazionale.

Nel quadro dell'Alleanza atlantica, in particolare – per la quale un attacco cibernetico può portare all'attivazione della clausola della difesa collettiva, *ex* articolo 5, con possibili conseguenze anche nel « mondo reale » – si lavora sulla creazione

di un approccio condiviso tra i suoi stati membri. Questi ultimi tuttavia divergono per strutture e capacità nazionali preposte alla difesa cibernetica, così come per postura nazionale in relazione alle possibili operazioni di risposta. È peraltro innegabile che proprio in quest'ultimo anno, all'indomani dello scoppio del conflitto russo-ucraino, che ha trasformato l'assetto degli equilibri geopolitici globali, il contesto NATO e il complesso delle sfide connesse alla tenuta dell'Alleanza e all'efficacia delle sue difese rendono sempre più urgente la necessità di una funzione di aggiornamento, quasi in tempo reale, dei parlamenti nazionali su questo importante versante della difesa cibernetica, in tutte le sue possibili implicazioni a livello collettivo.

Dal punto di vista della difesa, il dominio cibernetico rappresenta quindi una sfida da affrontare e un'opportunità da sfruttare che non possono essere lasciate in secondo piano. In ambito militare, la difesa da potenziali attacchi cibernetici può interessare diverse strutture, dal personale dispiegato nelle missioni internazionali, ai sistemi ed equipaggiamenti in uso, alle Forze armate sia sul suolo nazionale sia all'estero, fino alla protezione delle informazioni di rilevanza strategica e alla difesa effettiva da attacchi, siano essi rivolti alle strutture militari o aventi come obiettivo più ampio la sicurezza di una nazione.

È in questo quadro che si inserisce la difesa cibernetica dell'Italia. Il Comando per le Operazioni in Rete (Cor), istituito nel 2020 e a valenza interforze, è l'organo preposto al contrasto di attacchi cibernetici alle strutture della Difesa e in caso di attacchi di rilevanza nazionale. Tuttavia, così come avviene negli altri Paesi di principale interesse per l'Italia, la difesa cibernetica italiana è solo un aspetto del più ampio contesto della sicurezza nello spazio cibernetico, in cui una molteplicità di attori – prima tra tutti la nuova Agenzia per la Cybersicurezza Nazionale (Acn) – sono chiamati a intervenire a vario titolo, con l'obiettivo di incrementare la resilienza del Paese e le capacità e rapidità di risposta in caso di crisi cibernetiche.

In tale ampio contesto lo svolgimento di un'apposita indagine conoscitiva da parte della Commissione Difesa sul tema delle nuove tecnologie della difesa applicate al dominio cibernetico consentirebbe di comprendere al meglio le diverse sfaccettature di questa nuova minaccia asimmetrica e di acquisire il parere di autorevoli soggetti del mondo accademico e delle istituzioni in merito alle più adeguate forme di difesa.

Un ulteriore profilo meritevole di approfondimento riguarda, infine, il tema della formazione di personale d'eccellenza nel campo della difesa cibernetica e la necessità di individuare forme di diffusione della cultura cibernetica nelle nuove generazioni.

In ultimo, non possono essere tralasciati i crescenti profili di rilievo internazionale connessi a questo delicato settore della difesa nazionale e alla necessità/opportunità di concepire un approccio concertato nell'ambito dei paesi europei e facenti parte dell'Alleanza atlantica.

Peraltro, il tasso di rapida evoluzione ed obsolescenza dello stato dell'arte nella materia rende opportuno prevedere un campo di indagine quanto più ampio e flessibile possibile, in modo da coprire ogni eventuale esigenza informativa della Commissione che si presentasse in corso d'opera.

Al fine di acquisire elementi di conoscenza pertinenti all'oggetto dell'indagine e al proprio ambito di competenza, la Commissione procederebbe all'audizione dei seguenti soggetti:

il Ministro della difesa e il sottosegretario alla difesa con delega per la *cyber*;

i vertici delle Forze armate (Capo di Stato maggiore della difesa, Capi di Stato maggiore delle singole Forze armate, Segretario generale della difesa e Direttore nazionale degli armamenti, ufficiali con incarichi direttivi in unità specializzate);

il Comandante per le Operazioni in Rete (COR);

il Consigliere militare del Presidente del Consiglio dei ministri e il direttore dell'Agenzia per la Cybersicurezza Nazionale (Acn);

il Presidente dell'Autorità Garante per la protezione dei dati personali;

rappresentanti del Dis, dell'Agenzia Informazioni e Sicurezza Interna (Aisi), dell'Agenzia Informazioni e Sicurezza Esterna (Aise), di ciascuno dei Ministeri inclusi nel Cisr19 e rappresentanti del Ministero dell'Università e della Ricerca, del Ministro delegato per l'Innovazione Tecnologica e la Transizione Digitale, nonché della Protezione Civile;

dirigenti di altre pubbliche amministrazioni e organismi dello Stato operanti a diverso titolo nella materia oggetto dell'indagine;

l'Alto rappresentante per gli affari esteri e la politica di sicurezza dell'Unione europea;

Parlamentari di Commissioni del Parlamento europeo competenti in materia;

rappresentanti delle agenzie dell'Unione europea competenti nella materia;

rappresentanti di istituti ed enti di ricerca (come IAI, CESI), docenti universitari ed altri esperti;

esponenti di imprese operanti nel settore della sicurezza e della difesa cibernetiche;

esponenti della Scuola di Telecomunicazioni delle Forze Armate (STELMILIT) di Chiavari.

La Commissione potrebbe, inoltre, svolgere, previa autorizzazione del Presidente della Camera, missioni di studio sul territorio nazionale per visitare le sedi del Comando C4 Difesa e del Centro Intelligence Interforze (CII), a Roma, nonché del *Security Operation Center* (SOC) di Leonardo Spa, a Chieti. Ove risultasse utile in corso di indagine, si potrebbe svolgere anche una missione all'estero, presso le predette agenzie europee e/o eventuali ulteriori centri di ricerca, per approfondire eventuali profili di interesse della Commissione, anche al fine di mutuare modelli operativi o normativi già sperimentati con successo altrove.

L'indagine dovrebbe concludersi entro il 30 giugno 2024.