IV COMMISSIONE PERMANENTE

(Difesa)

S O M M A R I O

SEDE CONSULTIVA

Martedì 8 ottobre 2019. — Presidenza del presidente Gianluca RIZZO. – Interviene il sottosegretario di Stato per la difesa, Angelo Tofalo.

La seduta comincia alle 11.45.

Sulla pubblicità dei lavori.

Gianluca RIZZO, *presidente*, avverte che è pervenuta la richiesta che della seduta sia data pubblicità anche mediante gli impianti audiovisivi a circuito chiuso. Non essendovi obiezioni, ne dispone l'attivazione.

DL 105/2019: Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica.
C. 2100 Governo.
(Parere alle Commissioni riunite I e IX).

(Esame e rinvio).

La Commissione inizia l'esame del provvedimento.

Gianluca RIZZO, *presidente*, rammenta che, presso le Commissioni riunite affari costituzionali e trasporti, si è appena svolta l'audizione del Sottosegretario Tofalo, il cui intervento – per comodità dei colleghi che non sono potuti intervenire – è in distribuzione.

Luigi IOVINO (M5S), *relatore*, rileva, innanzitutto, che le misure contenute nel provvedimento si inseriscono nel più generale quadro strategico nazionale per la sicurezza e la difesa cibernetica. Considerati i molti ambiti di competenza e il carattere trasversale e asimmetrico della minaccia cibernetica, tale quadro coinvolge una pluralità di soggetti istituzionali. A questo riguardo, ricorda che in tutti i principali contesti nazionali, europei ed internazionali, nei quali si analizzano le principali sfide alla stabilità, alla sicurezza e alla crescita dei popoli, la minaccia cibernetica viene da tempo considerata insidiosissima, mutevole nei suoi tratti essenziali, in continua evoluzione, rapida nel

bersaglio da aggredire e capace di produrre effetti a distanze non raggiungibili con gli ordinari strumenti di attacco. Gli attacchi cibernetici possono, infatti, originare da qualsiasi punto della rete globale. Per le loro peculiarità, sono idonei a produrre danni al funzionamento di servizi essenziali per la società, paragonabili a quelli prodotti nell'ambito di un conflitto combattuto con armi convenzionali.

Osserva, quindi, che, con riferimento al comparto della Difesa, il nostro Paese sta da tempo rafforzando le proprie capacità militari nel dominio cibernetico. Si tratta di un elemento essenziale di sicurezza per la condotta delle operazioni, la protezione delle informazioni e la tutela delle Forze armate. Il potenziamento di tali capacità svolge un ruolo essenziale nell'architettura strategica nazionale di *cyber defence*. A questo riguardo, rappresentano misure concrete volte a rafforzare le capacità *cyber* della Difesa, sia l'istituzione del Comando interforze per le operazioni cibernetiche (CIOC), deputato alla protezione dei sistemi e delle reti del Dicastero della difesa e all'effettuazione delle operazioni in campo cibernetico, sia l'istituzione, nello stato di previsione del Ministero della difesa, di uno specifico Fondo per il finanziamento di iniziative nell'ambito della difesa cibernetica, allo scopo di dotare tale Dicastero di piena autonomia di spesa per lo sviluppo di una efficace e propria capacità cibernetica.

Gli attacchi *cyber* hanno infatti una diretta incidenza nei confronti di tutti gli ambiti di interesse della Difesa, come l'organizzazione della sicurezza, la gestione dei sistemi d'arma sempre più dipendenti dall'ambito informatico e, soprattutto, la condotta di operazioni militari. Proprio queste considerazioni hanno stimolato lo sviluppo della strategia difensiva cibernetica della NATO, introdotta nel vertice del Galles e confermata con la determinazione del *summit* di Varsavia nel luglio 2016, nel corso del quale « gli attacchi informatici » sono stati considerati come « una sfida chiara alla sicurezza dell'Alleanza e (...) un pericolo per la società moderna, al pari di un attacco convenzionale ». Il successivo *summit* di Bruxelles dell'11 luglio 2018 ha segnato un ulteriore, importante rafforzamento delle capacità cibernetiche della NATO. Il *summit* ha, infatti, stabilito la nascita di un Cyber Operations Center con l'obiettivo di coordinare le operazioni degli alleati nel dominio cibernetico.

Sottolinea, poi, che, nell'ambito del rafforzamento dell'architettura strategica nazionale per la protezione cibernetica, il decreto-legge assegna nuove competenze al Dicastero della difesa, che tengono conto della specificità del comparto nelle diverse misure strategiche del provvedimento.

In primo luogo e in estrema sintesi, l'articolo 1 istituisce il perimetro di sicurezza nazionale cibernetica, al fine di assicurare la sicurezza delle reti, dei sistemi informativi e dei servizi informatici necessari allo svolgimento di funzioni o alla prestazione di servizi dalla cui discontinuità possa derivare un pregiudizio alla sicurezza nazionale. L'individuazione dei soggetti inclusi nel perimetro di sicurezza nazionale cibernetica è demandata ad un decreto del Presidente del Consiglio dei ministri, adottato su proposta del Comitato interministeriale per la sicurezza della Repubblica (CISR), entro quattro mesi dalla data di entrata in vigore della legge di conversione del decreto-legge. Ricorda, a questo riguardo, che il Ministro della difesa è uno dei membri di tale Comitato interministeriale per la sicurezza della Repubblica.

Il medesimo decreto del Presidente del Consiglio dei ministri fissa anche i criteri che i soggetti inclusi nel perimetro dovranno seguire nel compilare l'elenco – il cui aggiornamento avverrà con cadenza almeno annuale – delle reti, dei sistemi e dei servizi rilevanti ai fini della presente disciplina. Entro sei mesi dall'entrata in vigore del decreto del Presidente del Consiglio dei ministri, gli elenchi così predisposti verranno inviati alla Presidenza del Consiglio dei ministri o al Ministero dello sviluppo economico, che dovranno successivamente inoltrarli al Dipartimento delle informazioni per la sicurezza (DIS) e all'organo per la regolarità e sicurezza dei

servizi di telecomunicazione presso il Ministero dell'interno. Ad un ulteriore decreto del Presidente del Consiglio dei ministri – da adottare entro dieci mesi dalla conversione del decreto-legge e soggetto ad aggiornamento almeno biennale – è poi demandata la definizione delle procedure secondo cui i soggetti del perimetro di sicurezza nazionale cibernetica segnalano gli incidenti aventi impatto su reti, sistemi informativi e sistemi informatici, nonché le misure volte a garantirne elevati livelli di sicurezza.

In particolare, l'elaborazione delle misure di sicurezza è realizzata, secondo l'ambito di propria competenza, dal Ministero per lo sviluppo economico e dalla Presidenza del Consiglio. È prevista l'intesa con il Ministero della difesa, il Ministero dell'interno, il Ministero dell'economia e finanze, il Dipartimento delle informazioni per la sicurezza.

Specifiche disposizioni regolano, poi, le forniture di beni, sistemi e servizi relativi a tecnologie per l'informazione e la comunicazione (ICT) destinati ad essere impiegati sulle reti o i sistemi informativi della Difesa e i servizi informatici d'interesse del Ministero della difesa.

In relazione a tali forniture, il citato Ministero si avvale di un proprio Centro di valutazione, in raccordo con la Presidenza del Consiglio dei ministri e con il Ministero dello sviluppo economico; per l'attività di tale Centro si provvede senza nuovi o maggiori oneri per la finanza pubblica. Vengono inoltre riservate alle strutture specializzate del Dicastero della difesa le attività di ispezione e verifica sulle reti, i sistemi e i servizi informatici delle Forze armate e delle Forze di polizia.

Ulteriori disposizioni di interesse della Difesa sono contenute nella parte del provvedimento (articolo 2) dove si prevede che, per l'espletamento delle attività del Centro di valutazione e certificazione nazionale del Ministero dello sviluppo economico, tale dicastero possa avvalersi di un contingente di personale non dirigenziale appartenente alle pubbliche amministrazioni, fatto salvo il personale impiegato in operazioni condotte dalle Forze armate, anche in ambito NATO. Tale eccezione è prevista anche con riferimento alle unità di personale di cui la Presidenza del Consiglio, nelle more delle assunzioni previste dal medesimo decreto-legge, può avvalersi per lo svolgimento delle funzioni in materia di digitalizzazione. Il Ministero dello sviluppo economico può inoltre avvalersi, in posizione di comando, di personale che non risulti impiegato in compiti operativi o specialistici con qualifiche o gradi non dirigenziali del comparto sicurezza-difesa, fino a un massimo di 20 unità.

Segnala, inoltre, che un importante profilo di interesse della Difesa è ravvisabile anche nell'articolo 3, che detta disposizioni di raccordo tra il decreto-legge e la normativa in materia di esercizio dei poteri speciali governativi sui servizi di comunicazione a banda larga basati sulla tecnologia 5G, di cui all'articolo 1 del decreto-legge n. 22 del 2019. Al riguardo, ricorda che il richiamato decreto-legge attribuisce poteri speciali al Presidente del Consiglio dei ministri nei confronti dei soggetti operanti con la nuova tecnologia 5G.

In relazione a questo potere, il nuovo decreto-legge ne estende l'ambito di applicazione ai soggetti inclusi nel perimetro di sicurezza nazionale cibernetica, pur se la disponibilità della nuova tecnologia 5G derivi da contratti già conclusi. Tali poteri speciali, fino alla data di entrata in vigore del regolamento previsto dall'articolo 1, comma 6, sono esercitati, previa valutazione degli elementi indicanti la presenza di fattori di vulnerabilità che potrebbero compromettere l'integrità e la sicurezza delle reti e dei dati che vi transitano. La valutazione di tali elementi di rischio – per quel che concerne i richiamati acquisti delle dotazioni della Difesa – è rimessa all'apposito Centro di valutazione del dicastero della difesa.

Per i contenuti dei restanti articoli, che non sono di diretto impatto sulle competenze del Ministero della difesa, rinvia alla documentazione in distribuzione.

In conclusione, nel sottolineare l'importanza del provvedimento, ricorda che sul tema della difesa cibernetica questa Commissione ha svolto nella precedente legislatura un'indagine conoscitiva, che è

orientata a rinnovare anche nella legislatura in corso ed invita, pertanto, i colleghi ad approfondire questa tematica anche alla luce degli apporti che saranno forniti dalle persone che verranno ascoltate nel corso delle audizioni.

Il sottosegretario Angelo TOFALO evidenzia come il Ministero della difesa disponga, per le proprie esigenze, di una rete infrastrutturale autonoma, per la protezione della quale è operativo un apposito Centro di valutazione interno al dicastero. Al riguardo, desidera rimarcare la competenza e la professionalità dei militari, uomini e donne, impegnati in questo settore, che rappresentano anche una preziosa risorsa a disposizione del Paese in caso di verifica di eventi critici. Nel manifestare, quindi, un orientamento favorevole del dicastero sul provvedimento, auspica che nella prossima legge di bilancio possano essere reperite nuove risorse economiche per il potenziamento della sicurezza della rete cibernetica della Difesa.

Elio VITO (FI), nel preannunciare un voto favorevole da parte del gruppo di Forza Italia, segnala l'opportunità di coinvolgere adeguatamente le Camere anche nella fase successiva all'entrata in vigore del provvedimento, prevedendo l'espressione del parere sui decreti attuativi, da parte delle competenti Commissioni parlamentari.

Gianluca RIZZO, *presidente*, nessun altro chiedendo di intervenire, rinvia il seguito dell'esame ad altra seduta.

La seduta termina alle 12.

AUDIZIONI INFORMALI

Martedì 8 ottobre 2019.

Nell'ambito dell'esame, in sede consultiva, del DL 105/2019: Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica.

Audizione di un esperto della materia.

L'audizione informale è stata svolta dalle 12.15 alle 13.10.

SEDE CONSULTIVA

Martedì 8 ottobre 2019. — Presidenza del presidente Gianluca RIZZO. – Intervengono i sottosegretari di Stato per la difesa, Angelo Tofalo e Giulio Calvisi.

La seduta comincia alle 13.10.

Sulla pubblicità dei lavori.

Gianluca RIZZO, *presidente*, avverte che è pervenuta la richiesta che della seduta sia data pubblicità anche mediante gli impianti audiovisivi a circuito chiuso. Non essendovi obiezioni, ne dispone l'attivazione.

Nota di aggiornamento al Documento di economia e finanza 2019.
Doc. LVII, n. 2-*bis* con Annesso e Allegati.
(Parere alla V Commissione).

(Esame e rinvio).

La Commissione inizia l'esame del provvedimento.

Giovanni RUSSO (M5S), *relatore*, riferisce, ai fini del parere da rendere alla Commissione bilancio, sulla Nota di aggiornamento al DEF, rammentando che la politica economica del Governo, in omaggio al metodo della programmazione degli interventi e del rispetto del Patto di stabilità e crescita europeo, è esposta, in primavera, nel Documento di Economia e Finanza (DEF), per poi essere adeguata e rifinita del mese di settembre con la relativa Nota di Aggiornamento, la quale dà conto di come l'andamento congiunturale annuale abbia inciso sulle previsioni iniziali. La Nota di Aggiornamento, con i suoi allegati, è quindi presentata al Parlamento ed è ivi esaminata con le medesime procedure del DEF.

Passando al comparto della Difesa, che riguarda più specificamente le competenze della nostra Commissione, segnala che la Nota sottolinea la validità e l'efficacia del processo di revisione dello strumento militare in corso da alcuni anni e volto a conseguire, in un arco temporale definito, il miglioramento del livello qualitativo e tecnologico dello strumento militare nazionale, pienamente integrato con il sistema di difesa e sicurezza dell'Unione europea e dell'Alleanza atlantica. La Difesa proseguirà, pertanto, nella realizzazione di un modello di difesa moderno, in grado di acquisire, sviluppare e sostenere nel tempo le capacità più idonee per comprendere le cause della moderna conflittualità ed intervenire efficacemente per la gestione delle situazioni di crisi e per l'eliminazione di eventuali minacce alla sicurezza e agli interessi del Paese.

Particolare attenzione sarà data alla valorizzazione del personale della Difesa, alla salvaguardia della salute e alla tutela della sicurezza, mentre la capacità dello strumento militare sarà valorizzata da un corretto bilanciamento delle dimensioni quantitative e qualitative. Al riguardo, la Nota ricorda che sul finire della XVI legislatura è stata adottata la legge n. 244 del 2012, volta a realizzare una revisione in senso riduttivo del modello di difesa nazionale, che ha conferito al Governo un'ampia delega volta a conseguire: una riduzione generale a 150.000 unità di personale militare delle tre Forze armate, da attuare entro l'anno 2024; una riduzione delle dotazioni organiche del personale civile della Difesa dalle attuali 30.000 unità a 20.000 unità, da conseguire sempre entro l'anno 2024; una contrazione complessiva del 30 per cento delle strutture operative, logistiche, formative, territoriali e periferiche della Difesa; infine, il riequilibrio generale del bilancio della « Funzione Difesa », ripartendolo orientativamente in misura del 50 per cento a favore del settore del personale, 25 per cento per il settore dell'esercizio e 25 per cento per quello dell'investimento.

Per quanto riguarda, invece, il quadro generale delle minacce, la Nota presta particolare attenzione all'evoluzione della minaccia cibernetica. In linea con le preoccupazioni espresse su questo tema nel Libro bianco per la difesa e la sicurezza internazionale 2015, il Governo fa presente che sarà potenziata e ammodernata la sicurezza cibernetica delle reti di comunicazione e di comando e controllo coerentemente con le iniziative del Governo in tema di innovazione e digitalizzazione, con importanti ricadute sullo sviluppo di nuove tecnologie, sulla competitività e sui livelli occupazionali del sistema Paese.

In particolare, per quanto concerne le più recenti iniziative assunte in questo settore, la Nota ricorda la recente adozione del decreto-legge n. 105 del 2019, in corso di conversione, finalizzato 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, attraverso l'istituzione di un perimetro di sicurezza nazionale cibernetica e la previsione di misure idonee a garantire i necessari standard di sicurezza rivolti a minimizzare i rischi di attacchi cibernetici. Al riguardo evidenzia che, per quanto concerne il tema della fornitura di servizi ICT (*Information and Communication Technology*) da impiegare su reti, sistemi informativi e servizi informatici del Ministero della difesa, il decreto prevede che il Ministero proceda attraverso un proprio Centro di valutazione, in raccordo con la Presidenza del Consiglio dei ministri e il Ministero dello sviluppo economico per i profili di rispettiva competenza. I fornitori di beni, sistemi e servizi destinati alle reti, ai sistemi informativi e ai servizi informatici individuati nell'elenco che deve essere trasmesso alla Presidenza del Consiglio dei ministri e al Ministero dello sviluppo economico, assicurano al Centro di valutazione e certificazione nazionale (CVCN) e, limitatamente agli ambiti di specifica competenza, al Centro di valutazione operante presso il Ministero della difesa, la propria collaborazione per l'effettuazione delle attività di test, sostenendone gli oneri.

Passando al comparto industriale della Difesa, la Nota ricorda le opportunità offerte dal Fondo Europeo della Difesa (*European Defence Fund* – EDF), che prevede, tra l'altro, finanziamenti sia per la ricerca tecnologica, sia per lo sviluppo di capacità strategiche, nonché dal Programma Europeo di Sviluppo Industriale per la Difesa (E*uropean Defence Industrial Development Programme* – EDIDP), finalizzato a supportare progetti di cooperazione industriale multilaterale tra aziende europee nel settore. Nello specifico, ricorda che il Fondo europeo per la difesa si colloca nell'ambito della più generale cooperazione strutturata permanente (PESCO) istituita con la decisione dell'11 dicembre 2017 del Consiglio dell'Unione europea, evidenziando che la PESCO non si traduce nella creazione di un esercito europeo, né equivale alla realizzazione della difesa comune, bensì in una cornice istituzionale e procedimentale, tendenzialmente aperta a tutti i membri, per realizzare in comune progetti in materia di difesa.

Conclude segnalando che nella parte della Nota dedicata al processo di alienazione degli immobili pubblici, viene fatto presente che l'Agenzia del demanio ha individuato circa 1.200 beni da immettere sul mercato a cui si aggiungono circa 40 immobili in uso al Ministero della difesa, per un valore stimato di 160 milioni.

Gianluca RIZZO, *presidente*, nessun altro chiedendo di intervenire, rinvia il seguito dell'esame ad altra seduta.

La seduta termina alle 13.20.