MEMORIA SOTTOSEGRETARIO TOFALO

Gentile Presidente,

nel ringraziarla per l'opportunità che mi è stata concessa di condividere con i colleghi della Camera dei deputati le modalità con cui l'amministrazione che rappresento ha lavorato alla costruzione di un decreto legge così strategico per il nostro Paese, approfitto per portare a Lei e a tutti i presenti i saluti del Ministro Guerini.

Ritengo che questo particolare ciclo di audizioni sia uno strsumento indispensabile per consentire che tra il Governo ed il Parlamento sovrano si riesca a costruire una proficua sinergia utile ad affrontare un cambiamento epocale in tema sociale, politico ed economico e sono lusingato che il Ministro mi abbia voluto delegare questo compito.

Ho avuto modo di visionare le altre audizioni tenutesi nei primi giorni di ottobre e condivido molte delle preoccupazioni che si celano dietro ad un progetto così ambizioso.

La costruzione di un perimetro di sicurezza nazionale cibernetica è, però, un'esigenza non più procrastinabile per un Paese che vuole cogliere tutte le opportunità tecnologiche, senza dover rinunciare ad un livello di sicurezza adeguato.

Sin dalla mia prima esperienza da membro del Comitato Parlamentare per la Sicurezza della Repubblica ho cercato di stimolare i colleghi parlamentari nella ricerca di soluzioni che potessero mettere a sistema i cittadini, le aziende e le pubbliche amministrazioni, con la finalità di costruire un Sistema Paese solido.

Questo decreto affronta finalmente in modo organico le connessioni che devono esserci tra questi tre nodi e le responsabilità che cadono su ognuno di essi.

Come ha ben rappresentato, infatti, il Col. Cesare Forte della GDF "solo garantendo la robustezza dell'intera catena si proteggono i singoli anelli costituenti il perimetro" ed io aggiungerei che questa garanzia deve essere reciproca.

Le parole pronunciate in questa sede dalla dott.ssa Nunzia Ciardi, Direttrice del Servizio di Polizia Postale e delle Comunicazioni del Ministero dell'Interno, e dal Generale Pierangelo Iannotti, Capo del III reparto del Comando generale, ci permettono di capire quanto sia necessario segmentare le risposte alle differenti minacce che possono impedire la fruizione, da parte del cittadino, di servizi ormai ritenuti essenziali.

Tutte le pubbliche amministrazioni, per garantire l'operatività nell'esercizio delle funzioni espletate, necessitano l'integrità e la sicurezza delle proprie infrastrutture tecnologiche. In particolar modo, chi ha compiti estremamente delicati, deve garantire una strategia finalizzata alla continuità operativa.

In questo percorso il Ministero della Difesa già collabora attivamente nell'ambito della sicurezza nazionale cibernetica e, in ragione delle competenze e delle capacità sviluppate, contribuisce alle attività nazionali promosse anche in seno al Nucleo per la Sicurezza Cibernetica.

Sottolineo che il Dicastero della Difesa opera su proprie reti e negli anni ha acquisito un notevole know-how gestendo DIFENET.

A titolo di esempio, in recepimento degli indirizzi del Quadro Strategico Nazionale e del discendente Piano Nazionale per la Protezione Cibernetica e la Sicurezza Informatica, la Difesa Cibernetica fu devoluta al Comando Interforze per le Operazioni Cibernetiche (CIOC), che presto sarà assorbito da un nuovo Comando di vertice alle dirette dipendenze del Capo di Stato Maggiore della Difesa.

Il CIOC fu creato nell'ambito del rafforzamento delle capacità di difesa delle Forze Armate da attacchi cibernetici, attraverso la protezione delle reti militari quale Cyber Command nazionale, abilitato a svolgere operazioni militari nel dominio cibernetico.

Tale spinta all'innovazione e alla collaborazione, nel più ampio disegno di difesa nazionale, è stata ribadita nella costruzione del Decreto Legge in esame che prevede, rispetto alle competenze elencate nel più recente Piano Nazionale, l'estensione delle capacità di verifica e validazione anche per le forniture dei beni e servizi dei sistemi

valutati di rilievo in termini di sicurezza nazionale cibernetica, valorizzando e salvaguardando le competenze e le capacità delle nostre pregiate risorse umane.

Non dobbiamo nasconderci però che l'aumento delle responsabilità in capo al Dicastero, ed il supporto che dovrà essere dato in termini di tempo e risorse anche alle altre amministrazioni, dovrà essere necessariamente supportato da un piano di ampliamento del numero di risorse da formare ed integrare alle eccellenze che sono già operanti.

Per quanto sopra riportato la predisposizione dei contenuti del DL n.105 del 2019 (promosso dal DIS e presentato al Parlamento dal precedente Governo) è stata finalizzata all'esito di approfondimenti tecnici avvenuti a livello di singola Amministrazione e all'esito di interlocuzioni avvenute, in sede di CISR Tecnico, tra le Amministrazioni interessate.

Il provvedimento, infatti, valorizza i contributi elaborati dalla Difesa che, recependo le istanze provenienti dall'Area Tecnica Operativa e dall'Area Tecnica Amministrativa, si sono principalmente incentrati sulla necessità di riconoscere le competenze tecniche dell'Amministrazione Difesa in materia di sicurezza cibernetica e, in particolare, in tema di:

• misure di sicurezza e politiche di sicurezza;

• prevenzione, mitigazione e gestione degli incidenti aventi impatti sulle reti, sistemi informativi e servizi informatici propri della difesa;

• struttura organizzativa per la gestione del rischio cibernetico e per la protezione fisica e logica;

• integrità delle reti e dei sistemi informativi;

• continuità operativa;

• monitoraggio, test e controllo;

• formazione.

Alle riunioni interne all'Amministrazione Difesa, coordinate dagli Uffici di diretta collaborazione, hanno partecipato: SMD II RIS, SMD VI, CIOC, CEVA, SMD UGAG, SGD TELEDIFE.

Il testo del DL include, quindi, le proposte della Difesa che si sono soffermate in particolare su:

• il coinvolgimento della Difesa in sede di definizione delle misure volte a garantire elevati livelli di sicurezza delle reti;

• attribuzione al Centro di Valutazione di sicurezza di prodotti o di sistemi informatici della Difesa (CEVA Difesa) delle attività di screening tecnologico sugli operatori economici che forniscono beni, sistemi e servizi ICT alla Difesa;

• attribuzione alle strutture tecniche della Difesa delle attività ispettive e di verifica da condurre su reti, sistemi e servizi connessi alla difesa e sicurezza militare dello Stato.

Le proposte formulate dalla Difesa (e dalle altre Amministrazioni interessate) sono state discusse in sede di CISR tecnico e successivamente si è pervenuti al testo finale del provvedimento.

Dopo aver affrontato i cambiamenti dettati da GDPR, NIS e Golden power ci troviamo davanti ad una nuova e importante sfida.

Allineare il livello d'ambizione che questo percorso prevede alle risorse da mettere in campo sarà un lavoro molto complesso e il Ministero della Difesa è pronto a fare la sua parte.

Già in questi mesi abbiamo avviato un processo di riorganizzazione delle competenze e razionalizzazione delle risorse in ambito cibernetico, per trovarci pronti alla gestione delle minacce presenti nel quinto dominio.

Sono certo che questo processo verrà gestito egregiamente dalla Presidenza del Consiglio attraverso il Dipartimento delle Informazioni per la Sicurezza (DIS), per dar voce a tutte le autorevoli istanze dei partecipanti.

Ribadisco con forza che l'Amministrazione Difesa vuole partecipare attivamente nel dare il proprio contributo alla scrittura dei decreti attuativi che delineeranno i parametri di valutazione del rischio e definiranno i tempi e le procedure per l'adeguamento agli standard minimi di sicurezza.

Resta chiaro che un aggravio dei compiti in capo alle proprie strutture e al proprio personale dovrà essere sopperito da un rafforzamento delle risorse disponibili.

Grazie a tutti per l'attenzione.