COMMISSIONI RIUNITE
AFFARI COSTITUZIONALI DELLA PRESIDENZA DEL CONSIGLIO E INTERNI (I)
TRASPORTI, POSTE E TELECOMUNICAZIONI (IX)

RESOCONTO STENOGRAFICO

AUDIZIONE

1.

SEDUTA DI MARTEDÌ 8 OTTOBRE 2019

PRESIDENZA DEL PRESIDENTE DELLA IX COMMISSIONE **ALESSANDRO MORELLI**

INDICE

N. B. Sigle dei gruppi parlamentari: MoVimento 5 Stelle: M5S; Lega - Salvini Premier: Lega; Forza Italia - Berlusconi Presidente: FI; Partito Democratico: PD; Fratelli d'Italia: FdI; Italia Viva: IV; Liberi e Uguali: LeU; Misto: Misto; Misto-Cambiamo !-10 Volte Meglio: Misto-C10VM; Misto-Minoranze Linguistiche: Misto-Min.Ling.; Misto-Noi con l'Italia-USEI: Misto-NcI-USEI; Misto-+Europa-Centro Democratico: Misto-+E-CD; Misto-MAIE - Movimento Associativo Italiani all'Estero: Misto-MAIE.

PRESIDENZA DEL PRESIDENTE DELLA IX COMMISSIONE ALESSANDRO MORELLI

La seduta comincia alle 10.45.

Sulla pubblicità dei lavori.

PRESIDENTE. Avverto che la pubblicità dei lavori della seduta odierna sarà assicurata, oltre che attraverso l'attivazione di impianti audiovisivi a circuito chiuso, anche mediante la trasmissione televisiva sul canale satellitare della Camera dei deputati e la trasmissione diretta sulla *web-tv* della Camera dei deputati.

Audizione del Sottosegretario di Stato per la Difesa, Angelo Tofalo, nell'ambito dell'esame del disegno di legge C. 2100, di conversione del decreto-legge 21 settembre 2019, n. 105, recante « Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica ».

PRESIDENTE. Ringrazio il Presidente De Lorenzis per avermi sostituito in questi giorni.

L'ordine del giorno reca l'audizione, ai sensi dell'articolo 143, comma 2, del Regolamento della Camera dei deputati, del Sottosegretario di Stato per la Difesa, Angelo Tofalo, nell'ambito dell'esame del disegno di legge C. 2100, di conversione del decreto-legge 21 settembre 2019, n. 105, recante « Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica ».

Ringrazio il Sottosegretario Tofalo per aver accolto l'invito della Commissione e gli do subito la parola.

ANGELO TOFALO, *Sottosegretario di Stato per la Difesa*. Signor 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 strumento indispensabile per consentire che tra il Governo e 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 del fatto che il Ministro mi abbia voluto delegare questo compito. Ho avuto modo di visionare le altre audizioni tenutesi nei giorni scorsi 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 vuol cogliere tutte le opportunità tecnologiche senza dover rinunciare ad un livello di sicurezza adeguato. Sin dalla mia prima esperienza da componente 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. Il decreto-legge in esame affronta finalmente in modo organico le connessioni che devono esserci tra questi tre nodi e le responsabilità che cadono su ognuno di essi. Sento spesso parlare di sistema-Paese, che viene semplificato con tre nodi che si possono definire concentrici: il singolo cittadino; le

aziende, sia pubbliche sia private; le istituzioni e lo Stato. Ciascuno di questi tre nodi è fondamentale per il sistema. Come ha ben rappresentato, infatti, il colonnello Cesare Forte della Guardia di finanza, solo garantendo la robustezza dell'intera catena si proteggono i singoli anelli costituenti il perimetro. Aggiungerei che questa garanzia deve essere reciproca: rafforzando ogni singolo anello si rende robusta la catena complessiva. Le parole pronunciate in questa sede dalla dottoressa Nunzia Ciardi, direttrice del Servizio di polizia postale e delle comunicazioni del Ministero dell'interno, e dal generale Pierangelo Iannotti, capo del Terzo reparto del Comando generale dell'Arma dei carabinieri, 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 dell'integrità e della sicurezza delle proprie infrastrutture tecnologiche. In particolar modo, chi ha compiti estremamente delicati deve garantire una strategia finalizzata alla continuità operativa.

Vorrei anche approfittare di questa occasione e di questa sede per sensibilizzare tutti gli autorevoli componenti delle Commissioni sul concetto di *business continuity*, di cui, purtroppo, pochi parlano, anche a livello parlamentare, e ovviamente la Difesa è un settore e un Dicastero strategico: siamo all'avanguardia su questo, ma ritengo che tutta la pubblica amministrazione debba essere in grado di fornire e continuare a fornire i servizi e i beni essenziali dopo aver subìto un evento critico. 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 (NSC). Sottolineo una cosa semplice e banale, nota a tutti, però mi preme ricordare, soprattutto ai cittadini che ci ascoltano, che il Dicastero della difesa opera su reti proprie e negli anni ha acquisito un notevole *know how* gestendo Difnet. Quindi, il Dicastero della difesa, al di là delle reti nazionali pubbliche e private, ha una propria rete strategica, un'infrastruttura critica che è Difnet.

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, quali il Cybercom nazionale, abilitato a svolgere operazioni militari nel dominio cibernetico. Questo fu fatto, così come in altri Paesi appartenenti all'Unione, dopo il summit NATO di Varsavia del 2016, che riconosceva ufficialmente il quinto dominio, quello cibernetico, come dominio per operazioni militari. 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 di 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 e 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 e da integrare con le eccellenze che già sono operanti all'interno del nostro Dicastero.

Per quanto sopra riportato, la predisposizione dei contenuti del decreto-legge in esame, promossa dal DIS e curata anche dal precedente Governo, è stata finalizzata all'esito di approfondimenti tecnici avve-

nuti a livello di singola amministrazione e all'esito di interlocuzione, avvenuta 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 della difesa in materia di sicurezza cibernetica, 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, come detto poc'anzi; monitoraggio, test e controllo; formazione. Alle riunioni interne dell'Amministrazione della difesa, coordinate dagli uffici di diretta collaborazione, hanno partecipato lo Stato Maggiore Difesa – II reparto (Reparto informazioni e sicurezza – RIS), lo Stato Maggiore Difesa – VI reparto, il CIOC, il Ce.Va., lo Stato Maggiore Difesa – Ufficio affari generali e giuridici e Teledife del Segretariato generale della Difesa. Il testo del decreto-legge include, quindi, le proposte della Difesa, che si sono soffermate, in particolare, sul coinvolgimento della Difesa in sede di definizione delle misure volte a garantire elevati livelli di sicurezza delle reti, sull'attribuzione al Ce.Va (Centro di valutazione della difesa), al quale spetta la valutazione di sicurezza di prodotti o di sistemi informatici della Difesa, dell'attività di *screening* tecnologico sugli operatori economici che forniscono beni, sistemi e servizi ITC alla Difesa, e l'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.

Apro una velocissima parentesi: io parlo per conto esclusivo del Ministero della difesa, ma sicuramente chi rappresenta il Ministero dello sviluppo economico parlerà di più del CVCN. Come Difesa noi già abbiamo da sempre il Ce.Va., che certifica le reti nostre classificate come strategiche, e che quindi sarà sovraccaricato di un ulteriore lavoro, che faremo ben volentieri, però questo deve essere fatto presente, perché già svolge un lavoro molto complicato, che quindi sarà ancora più cospicuo.

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 ed importante sfida: allineare il livello di ambizione che questo percorso prevede alle risorse da mettere in campo sarà un lavoro molto complesso, ma 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.

Mi avvio a concludere, Presidente. Sono certo che questo processo verrà gestito egregiamente dalla Presidenza del Consiglio attraverso il DIS (Dipartimento delle informazioni per la sicurezza) per dar voce a tutte le autorevoli istanze dei partecipanti, e quindi dei vari dicasteri. Ribadisco con forza – l'ho già sottolineato due volte ma lo faccio anche nel finale – che l'Amministrazione della 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, e ovviamente sono a disposizione per eventuali domande.

PRESIDENTE. Nel ringraziare il Sottosegretario Tofalo, do la parola ai deputati che intendano porre quesiti o formulare osservazioni.

MAURIZIO CATTOI. Grazie, Presidente. Ringrazio il Sottosegretario per la velocissima, puntualissima ed esaustiva relazione. Mi soffermo brevemente su un aspetto sul quale siamo stati sollecitati nelle audizioni dei giorni scorsi, che ha suscitato un po' l'impressione, se non di confusione, quanto meno di sovrapposizione per quanto concerne i ruoli delle Forze di polizia e delle Forze armate, cioè delle strutture che presiedono alla prevenzione e repressione dei reati in questo specifico settore, tra Arma dei carabinieri, Polizia di Stato (con la specialità della Polizia postale) e Guardia di finanza. Vale a dire, esiste una compartimentazione di fatto di competenze rispettive, quindi l'Arma dei carabinieri per l'ambito militare e la Polizia di Stato per l'ambito generale (funzione che adesso esercita, credo, la Polizia postale), e la Guardia di finanza per quanto riguarda le notifiche che hanno rilevanza sotto il profilo economico-finanziario. Chiedo se questa definizione degli ambiti sia ancora valida o se questo nuovo perimetro di fatto, nella formulazione che appare dai margini un po' larghi, consente alle varie amministrazioni di fare un po' tutti tutto, determinando quindi, in pratica, una tendenziale sovrapposizione dei compiti ed anche delle spese.

VINCENZA BRUNO BOSSIO. Ringrazio il Sottosegretario, tra l'altro apprezzo la sua competenza sulla questione non solo della sicurezza ma soprattutto della *cyber security*, e quindi può dare un contributo anche al di là della rappresentanza del Ministero. In particolare, rispetto alla conversione del decreto-legge in esame le aziende, in linea di massima soprattutto quelle che dovranno rapidamente lavorare sullo sviluppo del 5G, hanno una serie di preoccupazioni. Innanzitutto, sul CVCN la certezza dei tempi di risposta; inoltre, i tempi dei provvedimenti attuativi: il DIS ha detto che dieci mesi è un tempo massimo, chiedo come si può fare per accelerare questa tempistica

Sul tema delicato del *golden power*, nessuno ha messo in discussione l'esigenza anche di verifiche. Quello che invece viene messo in discussione io credo che sia una cosa che dobbiamo accogliere, vale a dire che queste notifiche possano riguardare dei lavori già svolti, delle attività già realizzate, che se avevano un senso prima, evidentemente non hanno più un senso adesso che si parte dalla collaborazione pubblico-privato: quindi, come fare in modo che, ferma restando questa collaborazione pubblico-privato che è presente in maniera forte, giustamente, nel decreto, poi non si crei comunque una messa in discussione di un lavoro che invece magari è stato anche discusso all'interno di quelle sedi o che, comunque, le aziende hanno già avviato, nuocendo non solo alle aziende, ma anche allo sviluppo del Paese, perché il tema del 5G è un tema che riguarda lo sviluppo del Paese.

FEDERICA ZANELLA. Mi associo alla domanda della collega Bruno Bossio e ne aggiungo una molto pratica. Sono previste coperture specifiche per il personale per il CVCN, per quanto concerne il Ministero dello sviluppo economico, per una decina di persone che possono essere assunte al di fuori delle assunzioni normali alla Presidenza del Consiglio. Non ritenete di avere professionalità all'interno che possono essere in grado, senza assunzioni esterne, di sopperire a questo, anche ovviamente con competenze già formate all'interno delle forze dell'ordine, magari con delle risorse in più da utilizzare per loro, piuttosto che assumere personale di altro tipo ?

Inoltre, non so è pertinente specificamente al decreto-legge in esame, ma ieri Leonardo ha svolto un'interessante audizione, offrendosi come partner industriale a fianco delle istituzioni, e ha parlato molto della possibilità di arrivare a un *quantum computing* come protezione dati in modalità inattaccabile, su cui potrebbero essere un partner importante. Ritenete possibile questa cosa, sotto il profilo dell'attaccabilità dei dati, la state valutando ? Hanno ricordato che forniscono tecnologia alla NATO per quanto concerne la *cyber security*: in che modo la *partnership* con Leonardo potrà essere attivata sulla sicurezza cibernetica ?

LUIGI IOVINO. Signor Sottosegretario, volevo porre alcuni quesiti relativi alle ma-

terie di competenza del Dicastero della difesa. Riguardo al centro di valutazione che dovrebbe essere appartenente al Ministero della difesa, volevo chiedere se si hanno maggiori informazioni sulla sua composizione e soprattutto su quali compiti svolgerà, ma in particolare sulla sua composizione, anche per avere un quadro un po' più ampio riguardo alle assunzioni, perché si parlava di fondi già esistenti, quindi di nessun aggravio per la finanza pubblica, e capire se il centro si avvarrà solamente di personale militare o anche di personale civile.

Inoltre, formulo un quesito partendo dal fatto che lei ha posto l'attenzione sulla formazione, vale a dire sull'elemento più importante in materia di *cyber security*, questo perché il nostro Paese ha di fronte delle esigenze, e quindi è necessario formare prima di tutto il personale della pubblica amministrazione, ma anche e soprattutto le nuove generazioni. Chiedo, quindi, se è possibile prevedere, se già il Ministero ha previsto qualche convenzione o *partnership*, oppure altri tipi di collaborazione con le università, con gli istituti di istruzione, con i licei, per formare le nuove generazioni e in particolare per cercare di attrarre queste nuove competenze, farle arrivare al Ministero della difesa ma soprattutto porle al servizio del Paese.

Infine, l'ultimo quesito è sulla diffusione della cultura della sicurezza cibernetica: ho assistito anche alle sue iniziative, che sono sicuramente molto interessanti, perché diffondere la cultura della sicurezza cibernetica nel nostro Paese è l'elemento fondamentale per cercare di innescare nella società quel principio per il quale è necessario essere preparati ad essere attenti anche quando si utilizza un normale *smartphone*. Quindi, chiedo se è prevista qualche iniziativa in merito alla diffusione della cultura e se il Ministero sta lavorando già su questo, soprattutto sulla formazione.

PRESIDENTE. Do la parola al Sottosegretario Tofalo per la replica.

ANGELO TOFALO, *Sottosegretario di Stato per la Difesa*. Grazie, Presidente. Parto dall'onorevole Cattoi: il provvedimento non va a incidere sul cambio di competenze. Ho capito la domanda, tutto resta com'è. Aggiungo un ulteriore elemento, ovviamente parlo esclusivamente per quanto riguarda la Difesa, e quindi l'Arma dei carabinieri: noi, accanto a questo percorso legislativo, a questo decreto e a tutto quello che deciderà il Parlamento, abbiamo iniziato nell'ultimo anno un forte potenziamento della parte *cyber* del Dicastero. Si tratta di un lavoro che ha già visto concludere un primo *step*, e in questo secondo *step*, che sarà molto breve, lo Stato Maggiore Difesa andrà a formare, proprio a costituire, un nuovo comando di vertice accanto agli altri: accanto a quelli esistenti, quali ad esempio il COI e il COFS, ci sarà un ulteriore comando di vertice che metterà insieme tutti gli uffici che trattano la materia cibernetica. Ovviamente noi parliamo di Dicastero della difesa, quindi parliamo delle quattro Forze armate, compresa l'Arma dei carabinieri, e all'interno della rete della Difesa (di cui parlavo in precedenza, staccata da tutto il resto), della rete strategica, si sta valutando, ma non le posso dare una risposta già adesso, ma sicuramente credo che si valuterà, e questa sarà una considerazione tecnica più che politica, di affidare all'Arma, all'interno del dominio cibernetico della Difesa, anche il compito di polizia militare. Se vogliamo riconoscere effettivamente il quinto dominio, come Amministrazione della difesa, così come nel resto delle reti il CNAIPIC della Polizia postale svolge il proprio compito, così all'interno del Dicastero della difesa abbiamo le nostre Forze armate, abbiamo l'Arma dei carabinieri, che può sicuramente svolgere egregiamente questo compito. Spero ci rivedremo, soprattutto in Commissione difesa, al termine di questo lavoro, e in quella sede potremo essere più dettagliati.

Per quanto riguarda l'onorevole Bruno Bossio, la ringrazio per le domande, e spero che i tempi siano brevissimi, nel senso che ha posto un problema che è importante: le aziende – siamo in un mercato libero – si sono già mosse, e credo sia importante arrivare – altri Paesi l'hanno fatto: la Spagna, la Slovenia, la Francia, la Germania ne

sta discutendo – a istituzionalizzare i processi di sicurezza, laddove per sicurezza intendo sia *security* sia *safety*. Altri Paesi lo stanno facendo, io un po' in giro lo sto dicendo, mi auguro che il Parlamento sovrano trovi in sede di conversione del decreto-legge in esame la possibilità di intervenire, perché andare a istituzionalizzare i processi di sicurezza significa mettere realmente insieme tutte le aziende. Semplificando, mi riferisco al *security manager*, al datore di lavoro quale responsabile della sicurezza, anche fisica, non solo cibernetica, dell'azienda, a un luogo istituzionale, magari presso la Presidenza del Consiglio, avendo come punto di snodo finale il DIS (Dipartimento informazioni per la sicurezza), a un tavolo istituzionalizzato dove si gestiscono tutti i rapporti relativi alla sicurezza cibernetica, così come avviene, ad esempio, per i rapimenti di ostaggi italiani, con grandi aziende che aiutano e collaborano. Ritengo pertanto che sia importante istituzionalizzare i processi di sicurezza, per agevolare la reale collaborazione tra aziende e istituzioni. Noi come Difesa, l'ho già ricordato, abbiamo il Ce.Va., quindi siamo un passo un po' in avanti rispetto agli altri, per fortuna, e mi riferisco anche al CVCN. Ci sono già laboratori che fanno questo, però questa fase sarà molto delicata. Anche nel privato c'è chi è più avanti di noi. Dunque, noi abbiamo il Ce.Va., ora verrà creato il CVCN al MISE: ho già posto il problema che già andare a sovraccaricare il nostro Ce.Va. sarà qualcosa per noi molto complicato da gestire, immagino l'importante lavoro che dovrà fare il MISE, ritengo che sicuramente dovrà rivolgersi anche ad attori esterni che siano in grado, almeno nella fase di *start up*, di svolgere questo lavoro.

Per quanto riguarda l'onorevole Zanella, io parlo per la Difesa, che sono onorato di rappresentare, e all'interno della Difesa vi sono eccellenze, non so all'interno di altre pubbliche amministrazioni, ma ritengo che la Difesa sia molto più avanti su questa materia rispetto ad altri dicasteri. Vado subito al nodo: noi abbiamo un problema, come Difesa, che i più bravi vengono chiamati dalla Presidenza del Consiglio, dove percepiscono un'indennità aggiuntiva. La Presidenza del Consiglio, quindi l'*intelligence*, vale a dire i servizi di sicurezza, hanno un ulteriore problema, che poi arrivano Amazon, Google e Facebook, i quali offrono una retribuzione ancora maggiore, e quindi le migliori risorse vanno fuori. Questo problema l'ho posto anche alla sensibilità del Presidente del Consiglio, che è molto attento alla questione, e si sta pensando – ovviamente servono risorse finanziarie – ad indennità aggiuntive non solo per la Difesa, ma per tutta la pubblica amministrazione che si occupa di questo tema.

Per quanto riguarda la Difesa, il lavoro che stiamo svolgendo – poi mi collego anche alla domanda dell'onorevole Iovino – relativamente alla formazione, il lavoro che stiamo svolgendo con questo nuovo comando che verrà formato, è creare una verticale *cyber* all'interno della Difesa che determinerà nuove tabelle di progressione nel percorso di carriera dei militari e civili della Difesa, per cui andremo a creare proprio una verticale *cyber* tabellare dove, per semplificare, il marinaio o il comandante dell'Esercito non farà una rotazione di tre anni e poi andrà magari in Afghanistan oppure il marinaio si imbarcherà: se vogliamo crescere delle risorse della Difesa specifiche nel settore *cyber* dobbiamo creare un percorso in cui il ragazzo che comincia a 20-25 anni poi resta per tutto il percorso, crescendo con i relativi, per così dire, gradi. Ci inventeremo qualcosa, ma questo è il futuro, se non lo facciamo noi lo farà prossimamente chi arriverà dopo di noi, ma noi abbiamo avviato questo importante lavoro, ed è un problema che va risolto.

Sul Ce.Va. magari le metterò a disposizione una scheda dettagliata. Lei parlava di militari e civili, la Difesa è costituita sia da civili sia da militari che lavorano in tutti i nostri uffici. In questi ultimi giorni ho approfondito il lavoro del Ce.Va., è un lavoro importante che impiega anche un po' di tempo, e devo dire alcune volte si va già in affanno per il lavoro corrente sulla certificazione delle reti strategiche più riservate della Difesa; andare, poi, a certifi-

care tutto sarà un lavoro ancora più cospicuo che, a mio giudizio, allungherà ulteriormente i tempi. Non si tratta di chiedere, per così dire, soldi per la Difesa, però sicuramente quell'ufficio andrà rafforzato, perché già oggi spesso si va in affanno e con questo decreto-legge ci sarà un sovraccarico di lavoro, per cui bisogna investire altre risorse per gestire l'ufficio.

Per quanto riguarda la formazione, ragionare come sistema-Paese, quindi singolo cittadino, azienda e Stato, credo che sia la chiave di tutto. Oggi, purtroppo, siamo un Paese di analfabeti, vale a dire l'italiano medio è digitalmente analfabeta (questo lo dicono i dati, non lo dico io), e purtroppo questo è un danno per il Paese. I giovani, i giovanissimi, sono nativi digitali e hanno ampie conoscenze dell'utilizzo dello strumento, ma manca, purtroppo, l'esperienza per riconoscere le minacce. Quindi il problema è che va creata velocemente una classe dirigente formativa per le nuove generazioni, ma questa stessa classe dirigente, che dovrebbe formare i giovani, ha meno pratica nell'uso dello strumento, però magari ha più coscienza delle minacce che esistono nel dominio cibernetico.

All'interno della Difesa, proprio con il CIOC, abbiamo fatto un importante lavoro di formazione interna. Molte aziende utilizzano modelli di *phishing* per i propri dipendenti. Questo è il dato un po' raccapricciante anche per le aziende, noi come Difesa, lo ripeto, siamo abbastanza fortunati, perché il livello è medio-alto, più alto che medio, però ho visto anche i dati di importanti aziende in cui si riscontra che quando arriva un'*e-mail* di *phishing*, quindi quando c'è un'*e-mail* malevola di un attaccante che vuole rubare le informazioni al soggetto, quando l'*e-mail* arriva sulla casella istituzionale c'è un livello di attenzione più basso, quando invece l'*e-mail* arriva sulla casella privata c'è un livello di attenzione più alto. Nella formazione, a mio avviso, occorre far capire proprio il concetto di sistema-Paese: chi ricopre un ruolo pubblico, all'interno di tutta la pubblica amministrazione, deve capire che la sua casella di *e-mail* personale istituzionale è dell'istituzione ma anche la sua, quindi deve avere lo stesso livello di attenzione che ha per la propria casella privata, perché, purtroppo, i dati parlano chiaro: per la casella privata il livello di attenzione è pari a 9/10, per la casella privata ma istituzionale del docente, del parlamentare, del dipendente dell'azienda partecipata il livello d'attenzione è pari a 4-5. Questo deve cambiare, dobbiamo alzare il livello di attenzione e capire che siamo tutti sistema-Paese, facciamo tutti parte del Paese. È la nostra bandiera, il nostro tricolore che va difeso, e quindi dobbiamo essere tutti più responsabili, anche curare le nostre piccole cose.

Quanto a Leonardo, con Leonardo c'è una *partnership* strategica, è inutile dire che è il nostro campione della *cyber*, tra l'altro negli ultimi mesi ha ridisegnato il quadro strategico della classe dirigenziale di prima fascia, concentrandosi ancora di più sulla materia cibernetica. Quindi, c'è una *partnership* consolidata, e sicuramente va ulteriormente potenziata, però è qualcosa che già esiste.

Vi ringrazio, e scusate se mi sono dilungato.

PRESIDENTE. Ringrazio il Sottosegretario Tofalo e dichiaro conclusa l'audizione.

La seduta termina alle 11.15.

Licenziato per la stampa
il 10 dicembre 2019

STABILIMENTI TIPOGRAFICI CARLO COLOMBO

18STC0081010