*Commissioni riunite*

*I "Affari Costituzionali" e IX "Trasporti, Poste e Telecomunicazioni"*

*della Camera dei Deputati*

# Audizione del Capo del III Reparto del Comando Generale dell'Arma dei Carabinieri, delegato dal Comandante Generale, Gen.B. Pierangelo Iannotti

Signori Presidenti, Onorevoli Deputati,

anche a nome del signor Comandante Generale, che mi ha chiesto di portarVi il suo saluto, ringrazio per l'attenzione rivolta all'Arma dei Carabinieri e per l'opportunità concessami, in qualità di Capo del III Reparto "Telematica" del Comando Generale, di fornire elementi di valutazione sui contenuti del disegno di legge all'esame, che prende in considerazione un settore nevralgico per il sistema Paese: il *cyber-space*, probabilmente la cosa più complessa che l'uomo abbia sinora mai costruito, composto da un numero elevatissimo di "attori in gioco", reti, nodi, sistemi informatici, protocolli di comunicazione e programmi

*software* che ne rendono estremamente difficile una "fotografia istantanea".

Complessità che, nel contempo, è generatrice di un numero altrettanto elevatissimo di vulnerabilità (errori di programmazione del codice, errate configurazioni, debolezze nella progettazione dei protocolli, ecc.) che possono essere sfruttate da un "agente" attaccante per arrecare danni, nell'accezione più generale del termine.

Su tali premesse, l'iniziativa legislativa di riconoscere e regolamentare il perimetro di sicurezza nazionale cibernetica non può che essere accolta con estremo favore, attesa l'esigenza di ridurre al minimo possibile le ipotesi di vulnerabilità, di prevenire i rischi e di reagire, prontamente, alle aggressioni, ripristinando le funzionalità dell'infrastruttura in caso di compromissione.

Gli obiettivi di protezione e resilienza, da un lato, e di reattività, dall'altro, possono essere raggiunti, dal punto di vista macroscopico, con misure tecniche che oscillano tra un minimo e un massimo in ragione della valutazione del rischio ovvero della criticità dell'infrastruttura da proteggere. Nel livello minimo di protezione e resilienza, tutti i *software* dei sistemi e degli apparati asserviti ad applicazioni critiche e/o

esposte su *Internet* devono essere: adeguatamente supportati dalla *software house* e aggiornati allo stato dell'arte; sottoposti a verifiche di sicurezza (possibilmente a cadenza periodica); privi di "vulnerabilità posturali" ovvero scevri da debolezze progettuali e/o comportamentali (es., invio delle credenziali di accesso su un canale di comunicazione non sicuro). Nel livello massimo di protezione e resilienza, le citate misure devono essere applicate a tutti i sistemi e apparati in uso.

Nel livello minimo di reattività è altresì necessario dotarsi di un'unità organizzativa, attivabile in caso di incidente informatico, che disponga di una mappatura dei sistemi di tutto l'*asset* tecnologico, al fine di individuare i servizi compromessi o in corso di compromissione da interrompere, anche solo in via cautelativa. Nel livello massimo di reattività, occorre implementare, per tutti gli *asset* tecnologici in uso, una struttura tecnologica e organizzativa capace di agire quotidianamente nell'ottica del potenziale incidente informatico.

Pertanto, indipendentemente dal livello di profondità che si intende dare al termine *cyber-security*, risulta evidente che le variabili da prendere in considerazione non possono prescindere da tecnologia, organizzazione, processi, vigilanza e, soprattutto, formazione.

In tale quadro, nell'Arma, i compiti di controllo e monitoraggio e di risposta a eventuali incidenti informatici nonché di analisi proattiva per garantire la sicurezza dell'infrastruttura tecnologica da minacce provenienti sia dall'interno sia dall'esterno sono affidati, rispettivamente, al SOC (*Security Operation Center*) e al CERT (*Computer Emergency Response Team*), unità costituite all'interno del Centro Sicurezza Telematica del Comando Generale.

Il CERT dell'Arma, in particolare, è in costante contatto con i CIRT (*Computer Incident Response Team*) di Forza Armata e, soprattutto, con il CIOC – Comando Interforze per le Operazioni Cibernetiche del Ministero della Difesa, al cui interno è inglobato il CERT Difesa, unico referente operativo del Dicastero per gli aspetti cyber nell'ambito del Nucleo Sicurezza Cibernetica attivato in seno al DIS. Il CIOC, nel garantire un tempestivo e aderente scambio informativo, assicura la necessaria attività di prevenzione e preparazione ad eventuali situazioni di crisi nonché l'attivazione delle procedure di allertamento. In tale ambito è all'attenzione la costituzione di un'unità di Polizia Militare info/investigativa, composta da personale dell'Arma specializzato, in grado di fronteggiare anche minacce, interne e/o esterne, riconducibili all'anello più debole della catena di sicurezza: l'uomo.

L'Arma, infatti, oltre ad esercitare in via esclusiva le funzioni di Polizia militare per tutta la Difesa, possiede anche le indispensabili capacità tecniche e le prescritte competenze giuridico-normative per fare pienamente fronte alle evenienze nel settore.

Invero, il Reparto Indagini Telematiche del ROS (Raggruppamento Operativo Speciale), oltre a provvedere alle attività di *digital forensics* e di *Internet investigation*, assicura il supporto tecnico alle attività di Polizia Militare nei settori della *cyber-security* del comparto Difesa. Quando il supporto richiede un'alta specializzazione interviene il Ra.C.I.S. (Raggruppamento Investigazioni Scientifiche) con il Reparto Tecnologie Informatiche.

Ritornando all'esame del testo, appare condivisibile la scelta di rinviare a regolamentazione successiva non solo l'individuazione dei soggetti da includere nel perimetro, ma anche la definizione dei criteri di predisposizione degli elenchi delle reti, dei sistemi informativi e dei servizi informatici nonché delle procedure di notifica degli incidenti e le misure volte a garantire elevati livelli di sicurezza degli assetti.

In tale contesto, particolare attenzione dovrà essere rivolta ai meccanismi di approvvigionamento di prodotti e servizi ICT, al fine di limitare gli eventuali effetti delle attività dell'organo di certificazione sui tempi contrattuali e sui relativi costi per l'adeguamento alle prescrizioni dettate e l'esecuzione dei test imposti.

Due ulteriori considerazioni attengono al sistema sanzionatorio e alle relative attività di vigilanza nonché, più in generale, al tema della formazione che, come sopra ho sottolineato, assume un ruolo centrale.

Il sistema sanzionatorio predisposto nei commi da 9 a 14 del decreto individua, quali uniche condotte penalmente rilevanti, circostanze omissive o di comunicazioni infedeli riguardanti l'individuazione delle reti critiche e talune predisposizioni organizzative di sicurezza.

Al riguardo appare opportuno attrarre alla sfera penale della punibilità anche talune condotte colpose di soggetti qualificati (amministratori di sicurezza, ecc.) riguardanti l'inosservanza delle misure di sicurezza, i cui effetti sui sistemi risulterebbero particolarmente gravi. Tali condotte potrebbero essere individuate con ulteriore provvedimento di legge e il loro accertamento essere affidato dall'Autorità giudiziaria alle unità specializzate che ciascuna Forza di Polizia ha costituito nel settore e che, per l'Arma dei

Carabinieri, sono individuate nelle già richiamate unità dedicate appartenenti all'organizzazione di Polizia Militare, al Raggruppamento Operativo Speciale e al Raggruppamento Investigazioni Scientifiche.

In stretta connessione con il sistema dei controlli, si pone l'esigenza di prevedere significativi investimenti di formazione a favore del personale impiegato in tutte le strutture dedicate alla prevenzione e all'analisi degli incidenti informatici.

È indubbio che la valorizzazione delle eccellenze emergenti nel settore sia essenzialmente rimessa al settore privato, in collaborazione con le università.

Un piano addestrativo nazionale, con finanziamenti pubblici strutturati, consentirebbe anche alle Forze di Polizia di corrispondere alle esigenze di supporto delle strutture di vigilanza, richiamate dallo stesso provvedimento. Infrastrutture di addestramento, con capacità di simulazione, consentirebbero di rafforzare complessivamente i livelli di sicurezza e di minimizzare i rischi.

Signori Presidenti, Onorevoli Deputati, a Voi rinnovo il mio ringraziamento per aver consentito di

rappresentare il punto di vista dell'Arma dei Carabinieri su un argomento di tale preminenza e attualità.

Le misure individuate certamente contribuiranno a innalzare i livelli di difesa cibernetica del Paese.