COMMISSIONI RIUNITE
AFFARI COSTITUZIONALI DELLA PRESIDENZA DEL CONSIGLIO E INTERNI (I)
DIFESA (IV)

RESOCONTO STENOGRAFICO

AUDIZIONE

2.

SEDUTA DI MERCOLEDÌ 14 GIUGNO 2017

PRESIDENZA DELLA VICEPRESIDENTE DELLA IV COMMISSIONE
ROSA MARIA VILLECCO CALIPARI

INDICE

N. B. Sigle dei gruppi parlamentari: Partito Democratico: PD; MoVimento 5 Stelle: M5S; Forza Italia - Il Popolo della Libertà - Berlusconi Presidente: (FI-PdL); Articolo 1 - Movimento Democratico e Progressista: MDP; Alternativa Popolare-Centristi per l'Europa-NCD: AP-CpE-NCD; Lega Nord e Autonomie - Lega dei Popoli - Noi con Salvini: (LNA); Sinistra Italiana-Sinistra Ecologia Libertà-Possibile: SI-SEL-POS; Civici e Innovatori: (CI); Scelta Civica-ALA per la Costituente Liberale e Popolare-MAIE: SC-ALA CLP-MAIE; Democrazia Solidale-Centro Democratico: (DeS-CD); Fratelli d'Italia-Alleanza Nazionale: (FdI-AN); Misto: Misto; Misto-Conservatori e Riformisti: Misto-CR; Misto-Minoranze Linguistiche: Misto-Min.Ling.; Misto-UDC-IDEA: Misto-UDC-IDEA; Misto-Alternativa Libera-Tutti Insieme per l'Italia: Misto-AL-TIpI; Misto-FARE !-PRI: Misto-FARE !-PRI; Misto-Partito Socialista Italiano (PSI) - Liberali per l'Italia (PLI): Misto-PSI-PLI.

PRESIDENZA DELLA VICEPRESIDENTE DELLA IV COMMISSIONE ROSA MARIA VILLECCO CALIPARI

La seduta comincia alle 15.

Sulla pubblicità dei lavori.

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

Audizione del Direttore generale del Dipartimento delle informazioni per la sicurezza (DIS), Alessandro Pansa, sulle problematiche legate alla difesa e alla sicurezza nello spazio cibernetico.

PRESIDENTE. L'ordine del giorno reca l'audizione del Direttore generale del Dipartimento delle informazioni per la sicurezza (DIS) Alessandro Pansa.

Ricordo che l'audizione del prefetto Pansa è stata programmata per permettere alle Commissioni affari costituzionali e difesa di approfondire la conoscenza, per i rispettivi profili di competenza, delle problematiche legate alla difesa e alla sicurezza nello spazio cibernetico. Sullo stesso tema le Commissioni hanno già audito il presidente dell'Autorità garante per la protezione dei dati personali, Antonello Soro.

Si tratta di un tema di stretta attualità, come è noto a tutti. Dal punto di vista normativo una novità di rilievo è rappresentata dalla revisione dell'architettura istituzionale in materia di protezione cibernetica e sicurezza informatica nazionale, disposta con il decreto del Presidente del Consiglio dei ministri del 17 febbraio ultimo scorso, che ha riformato il precedente assetto definito per la prima volta dal decreto del Presidente del Consiglio dei ministri del 24 gennaio 2013, il cosiddetto « decreto Monti ».

Ricordo che, come di consueto, i colleghi potranno intervenire per formulare osservazioni e porre quesiti dopo che il prefetto Pansa avrà svolto la sua relazione.

Do, quindi, subito la parola al direttore Pansa.

ALESSANDRO PANSA, *Direttore generale del Dipartimento delle informazioni per la sicurezza (DIS).* Grazie presidente e buonasera a tutti. Io, se ritenete, farei una breve presentazione della minaccia cibernetica e poi descriverei sinteticamente qual è l'attuale impianto ordinamentale realizzato sulla base del decreto del 17 febbraio scorso e del conseguente Piano nazionale per la protezione cibernetica e la sicurezza informatica.

Nell'ultimo anno la minaccia cibernetica a livello nazionale ha manifestato un *trend* di crescita imputabile all'aumentata sofisticazione degli strumenti utilizzati, alla loro pervasività e alla loro persistenza nell'azione. Tale crescita è dovuta quasi esclusivamente all'aumentata potenzialità degli strumenti che vengono utilizzati per portare avanti queste attività ostili.

Le principali minacce che sono rilevate contro i sistemi nazionali, sia pubblici che privati, possono ricondursi prevalentemente a tre matrici: al cosiddetto « cyber-spionaggio », all'hacktivismo e al cyber-terrorismo.

Evidentemente abbiamo di fronte una minaccia che richiede una grande consapevolezza e una grande conoscenza del fenomeno e di cosa significa utilizzare gli strumenti informatici e le reti per poterci

difendere, perché maggiore è la consapevolezza e minore è lo spazio che viene lasciato all'attività.

C'è un dato essenziale da tener presente: entrare nella rete, utilizzare la rete e usufruire della rete presenta costi bassissimi e procedure semplicissime; difendersi, invece, richiede costi elevatissimi e strutture molto complicate.

Questa diversità, questa opposta valenza dell'utilizzo e della difesa, rende i sistemi in generale tutti molto vulnerabili. Ai fini di questa esigenza di consapevolezza si può vedere quasi positivamente il risultato dell'ultimo attacco informatico – quello del famoso WannaCry – perché, in qualche modo, ha fatto comprendere e scoprire a tanti quanto si sia indifesi e quanta esigenza ci sia di difendersi.

Di fronte all'attività che noi abbiamo evidenziato, gli attacchi esaminati, come ho detto, sono riconducibili a tre aree. Una è quella del cyber-spionaggio, dove rivestono un ruolo centrale attori globali strutturati che hanno avuto essenzialmente come bersaglio le amministrazioni pubbliche, titolari di funzioni importanti e critiche.

Normalmente gli strumenti che sono stati utilizzati sono particolarmente sofisticati: *malware* articolati, infrastrutture tecnologiche di comando e controllo, tecniche di offuscamento, ingegneria sociale molto sofisticata.

I destinatari spesso non si rendono neanche conto di aver subìto l'attacco, perché molte volte si tratta di cosiddetti « attacchi silenti », che entrano all'interno dei sistemi e non hanno esigenza di far sapere né alla vittima né a terzi di aver ottenuto il risultato della loro azione.

La compromissione di questi sistemi avviene generalmente per due finalità. La prima è una finalità che potremmo definire di carattere strategico, tesa a conoscere e a comprendere il posizionamento politico, strategico ed economico dell'attaccato. Se sono sistemi pubblici, probabilmente è tesa a conoscere il posizionamento del Paese in ordine ai diversi obiettivi che quest'ultimo persegue sul piano geopolitico.

Sul piano tattico queste attività sono finalizzate a profilare il personale obiettivo dell'azione, cioè a conoscere chi c'è dall'altra parte ovvero le persone i cui dati sono contenuti nei sistemi attaccati. Si tratta di una descrizione di soggetti, il cui fine può essere il più vario: dal tentativo di reclutamento allo scoprire segreti che queste persone possono avere, dal ricatto a individuare debolezze di vario genere.

Il tipo di attacchi che viene fatto in questo ambito mostra un'elevatissima capacità offensiva, ampia disponibilità di risorse umane, tecnologiche e economiche. Questa circostanza conferma che vengono utilizzati per svolgere queste attività dei *team* di *hacker* che operano in stretto raccordo anche con analisti che selezionano i *target*, gli obiettivi e i contenuti che devono essere filtrati dai sistemi che vengono occupati. Sono operazioni complesse e congiunte, che mettono insieme professionalità di diversa origine.

Per quanto riguarda gli attacchi cosiddetti « dell'hacktivismo » di tutto il mondo della contestazione, quasi sempre questi sono di tipo dimostrativo e vengono portati avanti con armi digitali non particolarmente sofisticate. Per lo più sono strumenti reperibili già di per sé sulla rete e hanno successo perché vengono utilizzati contro strutture, installazioni e infrastrutture che sono facilmente vulnerabili dai sistemi di ordinaria utilizzazione.

Lo dimostra il fatto che gli obiettivi che vengono raggiunti non sempre sono consoni alla matrice dell'attacco, perché chi attacca lo fa dove trova una bassa difesa e va alla ricerca dei buchi nei quali poter entrare. Se entra nel buco del sistema a cui lui è interessato, ha un doppio vantaggio, altrimenti entra lo stesso, fa il danno che intende fare, divulga la sua abilità, ma non ottiene alcun risultato, perché la selezione dell'obiettivo è fatta sulla base della vulnerabilità dell'obiettivo stesso, non sulla finalizzazione dell'azione che l'*hacker* vuole raggiungere.

Si tratta essenzialmente di portare avanti istanze di contestazione sociale, politica eccetera, che vengono semplicemente basate sulla divulgazione di quello che è stato fatto, indicando spesso e volentieri la sola

debolezza del sistema come risultato della loro azione.

Negli ultimi tempi l'operatività digitale hacktivista che era in gran parte riferibile al movimento Anonymous Italia, sta molto diminuendo perché vi è un declino delle capacità tecniche di fronte alla crescita dei sistemi di sicurezza e, quindi, anche la presenza di Anonymous è molto più marginale sulla rete.

La scelta degli obiettivi, come dicevo prima, è basata sulla capacità di sfruttamento delle risorse ICT di cui l'attaccante dispone, che non sono particolarmente sofisticate e, quindi, gli obiettivi e i risultati non sono particolarmente rilevanti.

L'altra area è quella del cosiddetto « cyber-terrorismo », cioè gruppi estremisti che connotano la loro attività sui *social* principalmente per finalità di radicalizzazione, di proselitismo, di addestramento, di comunicazione, di finanziamento e di rivendicazione degli attacchi terroristici.

Vi sono gruppi particolarmente attivi e noti. Forse tra i più attivi vi è il Tunisian Fallaga team, che ha condotto migliaia di attacchi che hanno portato al *defacement* – cioè alla distruzione – del sito *web* attaccato e che agisce a livello globale.

Anche questi attacchi sono connotati, però, da un basso livello di sofisticazione. Si tratta comunque di attività che vengono portate avanti contro sistemi ICT anche di rilevanza strategica, che vengono attaccati con strumenti non particolarmente sofisticati. Riescono a ottenere risultati a causa delle carenze di difesa del sistema e non a causa dell'abilità degli attaccanti o della sofisticazione degli strumenti che questi ultimi utilizzano.

È evidente che il terrorismo in generale ha una grande capacità di evoluzione e di diffusione e, quindi, l'evoluzione delle sue tecniche e metodologie è un qualcosa che ci preoccupa particolarmente. Anche se allo stato gli episodi registrati non sono particolarmente sofisticati, riteniamo che la loro capacità di evoluzione e di crescita sia ampia e, quindi, dobbiamo essere sicuramente pronti a gestire azioni più complesse e più difficili, perché è molto semplice che gruppi terroristici organizzati e dotati di sufficienti fondi possano assoldare dei *team* di *hacker* qualificati e condurre azioni molto più devastanti di quelle che hanno fatto fino adesso.

Per quel che riguarda gli attacchi che sono stati condotti nel 2016 nei confronti di assetti ICT sia pubblici che privati a livello nazionale, la maggior parte sono stati fatti da gruppi hacktivisti. Il numero degli attacchi da noi censiti fa risalire all'hacktivismo il 52 per cento dell'attività, con un basso impatto della loro azione, soprattutto se lo compariamo all'alto impatto che hanno avuto gli attacchi del cyber-spionaggio di cui parlavamo prima, che invece riteniamo essere intorno al 19 per cento. I gruppi *hacker*, particolarmente quelli di matrice islamica, che hanno portato avanti azioni ostili sono intorno al 6 per cento del totale. Il resto, invece, è una galassia di attività riconducibili a soggetti singoli e a motivazioni che trascendono da una classificazione di carattere generale.

Per quanto riguarda gli obiettivi, quelli pubblici sono di gran lunga superiori a quelli privati: il 72 per cento degli obiettivi delle attività svolte da questo mondo degli attacchi è riferibile all'amministrazione pubblica.

La diffusione della qualità dell'attacco e l'utilizzo di *software* malevoli particolarmente sofisticati ha riguardato l'11 per cento degli attacchi registrati. La capacità di compromissione delle strutture e dei dati danneggiati, invece, riguarda il 28 per cento dei casi. L'impedimento di erogare i servizi a cui i sistemi erano rivolti è avvenuto nel 19 per cento dei casi. Il *defacement*, cioè la distruzione del sito, riguarda il 13 per cento dei casi avvenuti.

Questo è un panorama molto generale e sommario della minaccia *cyber* e soprattutto della sua evoluzione negli ultimi tempi.

A fronte di questa minaccia, con un gruppo di esperti, coinvolgendo tutti i ministeri che fanno parte del CISR (Comitato interministeriale per la sicurezza della Repubblica), oltre al Ministero della funzione pubblica, con l'Agenda digitale e con l'AGID (Agenzia per l'Italia digitale), abbiamo esaminato i risultati che si erano ottenuti con il sistema di difesa *cyber* impiantato con il cosiddetto « decreto Monti ».

Quello che abbiamo rilevato è che tale decreto probabilmente ha fatto crescere molto le capacità e le conoscenze del fenomeno da parte degli utenti e anche da parte della pubblica amministrazione, ma non ha consentito di superare i diversi profili di criticità che i sistemi informativi strategici del nostro Paese continuano a denotare, subendo attacchi cibernetici particolarmente importanti.

A fronte dell'esigenza di una maggiore esperienza – soprattutto in ragione del fatto che l'Italia ha assunto un ruolo a livello internazionale sia in sede NATO, sia in sede OSCE – e considerato che la minaccia si è resa particolarmente sofisticata e vi è stata anche una modifica del quadro normativo, specialmente con la direttiva europea, il Governo ci ha dato incarico di studiare e di individuare i profili di criticità manifestati e di trovare delle soluzioni.

I principali profili di criticità che abbiamo rilevato riguardavano, da un lato, la difficoltà a dare una risposta ai casi di attacchi gravi. In effetti, vi è stata soltanto la capacità di alcuni *team* che occasionalmente venivano messi insieme dai ministeri più sofisticati in materia. Il comparto, il Ministero dell'interno e il Ministero della difesa, mettendo insieme dei gruppi di esperti, ogni volta corrono e si rincorrono per trovare delle soluzioni, ma non abbiamo una struttura ben costituita.

Anche le competenze sono sparse un po' dappertutto e non sono concentrate intorno a un sistema di difesa unitario. Inoltre, in molte delle strutture costituite nei diversi tavoli e presso i diversi uffici ci sono sempre le stesse persone, che una volta stanno in un organismo con una veste e un'altra volta cambiano cappello e stanno in un altro organismo. Non avevamo una precisa divisione dei compiti e un preciso potenziamento.

Per fare questo, abbiamo analizzato il sistema e, sulla base di queste rilevanze, è stato emanato il decreto del Presidente del Consiglio del 17 febbraio 2017, anche alla luce delle modifiche normative che c'erano state.

Infatti, noi abbiamo avuto due importanti modifiche normative. Una, nel 2015, è stata la modifica della legge istitutiva del comparto. L'articolo 7-*bis* del decreto-legge n. 174 del 2015, infatti, individua nel CISR l'organo deputato alla gestione delle emergenze di sicurezza nazionale. Se l'attacco cibernetico determina un'emergenza per la sicurezza nazionale, normativamente l'organo che deve prendere in mano la situazione è il CISR, perché è previsto oggi dalla normativa vigente.

Il secondo intervento normativo, che pure ha spronato l'iniziativa di modifica che è stata fatta a febbraio scorso, è stata la direttiva NIS (*Network and information security*). La ratifica della direttiva NIS, che deve avvenire nel maggio 2018, richiede un nuovo sistema e un aumento fortissimo dei livelli di sicurezza delle reti e di sistemi informativi dei Paesi dell'Unione, a cui noi entro quella data ci dovremo adeguare.

Per questo motivo, c'è già stato un primo stanziamento di fondi di 150 milioni che nell'agosto dell'anno scorso è stato attribuito al DIS per essere destinato al rafforzamento del sistema di sicurezza.

A febbraio, con un provvedimento emesso dal Presidente del Consiglio, sono state affrontate e risolte alcune delle principali carenze presenti nell'architettura della sicurezza *cyber* del nostro Paese. In primo luogo, sono state semplificate le procedure ordinarie e straordinarie di gestione delle attività di implementazione dell'architettura nazionale.

Sono poi stati rimodulati gli organi, semplificandoli. C'era una duplicazione, come dicevo prima. Organi diversi in cui erano presenti le stesse persone sono stati unificati in un unico organismo ed è stato definito in maniera più chiara l'ambito delle competenze delle diverse amministrazioni, con una capacità di coordinamento, superando le forme di sovrapposizione o di non coordinamento.

Questo obiettivo è stato fissato attribuendo una responsabilità e una funzione alla Presidenza del Consiglio dei ministri e al CISR nel campo della sicurezza informatica e attribuendo al direttore centrale del DIS un ruolo più attivo, soprattutto per quel che riguarda la gestione ordinaria e straordinaria delle emergenze della sicurezza cibernetica nazionale.

È stata rimodulata l'architettura, semplificando alcuni organismi, tipo il NISP (Nucleo interministeriale situazione e pianificazione) cyber, che era completamente diverso dal cosiddetto NSC (Nucleo per la sicurezza cibernetica). Uno dei due è stato eliminato e l'NSC è stato riposizionato all'interno del DIS.

In questo modo, si è creata una filiera unica e precisa di responsabilità: Presidente del Consiglio, CISR, CISR tecnico, DIS, che è l'organismo che già oggi funziona in tutte le altre circostanze per la sicurezza nazionale. In questa modalità funzionerà anche per la sicurezza nazionale cibernetica.

Inoltre, è stato conferito al DIS un ruolo di coordinamento delle iniziative di altre amministrazioni che a vario titolo fanno capo al CISR, perché riferiscono a ministeri o a dipartimenti che rientrano all'interno delle competenze dei ministri CISR.

È stato attribuito al Ministero dello sviluppo economico il compito di istituire un centro di valutazione e certificazione nazionale per la verifica dell'affidabilità della componentistica delle apparecchiature ICT che vengono utilizzate da parte della pubblica amministrazione nelle strutture critiche e nelle strutture strategiche.

È stato inoltre previsto l'accesso alle banche dati dei soggetti privati e ai cosiddetti SOC (*Security Operation Center*) dal parte del DIS, in modo tale da poter avere una visione unitaria del sistema.

Subito dopo l'emanazione di questo provvedimento, sulla base delle valutazioni fatte, è stato ridisegnato il nuovo Piano nazionale per la protezione cibernetica, pubblicato sulla Gazzetta ufficiale il 31 maggio scorso. Oggi abbiamo un piano rinnovato rispetto al passato, che non è un mero aggiornamento del passato, ma è una nuova idea, una nuova formulazione del piano nazionale.

Il documento mira a sviluppare indirizzi strategici. I principali sono: il potenziamento della capacità di difesa delle infrastrutture, il miglioramento delle capacità tecnologiche operative delle istituzioni interessate, l'incentivazione della cooperazione tra le istituzioni, la promozione e la diffusione della cultura della sicurezza, il rafforzamento della cooperazione internazionale, il rafforzamento della capacità di contrasto delle attività, soprattutto quelle illegali a livello *on line*.

La nuova architettura nazionale *cyber* coinvolge il comparto, i ministeri CISR – cioè gli affari esteri, l'interno, la difesa, la giustizia, l'economia e le finanze e lo sviluppo economico – oltre all'AGID e all'ufficio del consigliere militare.

Questo piano ha redatto una *road map* attraverso la quale bisognerà portare avanti un processo che coinvolgerà tutti gli attori per il potenziamento di tutti gli obiettivi e le iniziative che sono state portate avanti.

Non voglio dilungarmi, ma due sono i momenti salienti. Il primo riguarda la capacità di reazione. Stiamo unificando i due CERT (*Computer Emergency Response Team*), quello della pubblica amministrazione e il CERT nazionale, che risiedevano uno presso l'AGID e l'altro presso il Ministero dello sviluppo economico. Fino a oggi erano delle entità abbastanza deboli. Li abbiamo riprogettati e li stiamo realizzando, perché siano un'unica struttura, come richiede peraltro la direttiva NIS, particolarmente sofisticata e particolarmente potente, in diretto collegamento con l'NSC, quindi con l'organismo che gestisce le emergenze nazionali.

L'altro elemento di particolare rilevanza è la costituzione presso il Ministero dello sviluppo economico del centro di valutazione e certificazione, che consentirà preventivamente la valutazione dell'utilizzo presso infrastrutture critiche del Paese di strumenti che siano certificati per la loro qualità e per la loro affidabilità e che non siano già *ab origine* utilizzabili da parte di terzi.

L'importanza di questa iniziativa è stata presa in considerazione anche nel Documento di economia e finanza, che alla pagina 64, in un paragrafo intitolato « Azioni a supporto di una maggiore *cyber security* nella pubblica amministrazione », prevede che il Governo, consapevole di questa esigenza, implementerà il Piano nazionale per la protezione cibernetica e la sicurezza.

In questo faranno rientrare tutte le iniziative che sono legate alla revisione del

piano stesso, con i seguenti obiettivi: l'accelerazione del progetto di un *data center* unificato di tutte le pubbliche amministrazioni, una prima definizione di un *cloud* governativo aperto a tutta la pubblica amministrazione e lo sviluppo di elementi che consentano di recuperare il *gap* strutturale nella *cyber security*, incluso il rapido recepimento della direttiva NIS.

Da ultimo, il piano prevede anche, come lo stesso « decreto Gentiloni », un ruolo forte di coordinamento e di promozione del DIS nel rapporto col mondo della ricerca, sia accademica sia del settore privato.

In tal modo, il DIS promuoverà tutte le iniziative a supporto della crescita dei sistemi di sicurezza, perché i sistemi di sicurezza non mantengono per tempi lunghi livelli particolarmente elevati e devono essere continuamente implementati, quindi abbiamo bisogno della scienza e della conoscenza che il mondo accademico e della ricerca e alcune aziende nazionali hanno. Fungerà anche da acceleratore per quel che riguarda iniziative nel settore produttivo dei sistemi di sicurezza.

In questo esercizio che abbiamo svolto, abbiamo anche accelerato un meccanismo di soluzione e di coordinamento dei rapporti con il Ministero della difesa – mi sembra doveroso dirlo in questa sede – e un inquadramento preciso di tutte le attività nel settore della *cyber security* che fanno capo alla difesa e di quelle che fanno capo al comparto.

Infatti, è evidente che ci sono difficoltà enormi nel definire quando la minaccia *cyber* è una minaccia che attiene alla difesa del Paese. Se l'azione di risposta è un'azione da difesa, è un'azione di tipo militare, che ha dei percorsi, il primo dei quali è il passaggio parlamentare; mentre quando è un'azione non convenzionale, spetta evidentemente agli organismi che si muovono attraverso altre competenze e altre facoltà autorizzate dalla legge.

Questo è il motivo per il quale noi abbiamo steso una matrice su cosa si fa a ogni azione e su chi la fa. Pertanto, tutto questo è stabilito in un protocollo che abbiamo formulato con la difesa, che ci consente di muoverci congiuntamente e coralmente senza sovrapposizioni e soprattutto senza mancanza di coordinamento.

Io credo di avere esaurito l'informazione e sono pronto per le vostre domande.

PRESIDENTE. Io ringrazio molto il prefetto, che è stato chiarissimo. Do ora la parola ai colleghi che intendano intervenire per porre quesiti o formulare osservazioni.

MASSIMO ARTINI. Innanzitutto ringrazio i colleghi della Commissione affari costituzionali per questa possibilità, perché l'audizione odierna offre un contributo indubbiamente fondamentale e strutturale anche relativamente all'indagine conoscitiva che stiamo svolgendo in Commissione difesa.

Ringrazio, poi, anche il prefetto, perché, non solo nella parte più meramente descrittiva, ma anche nella discussione sulla ristrutturazione fatta con il decreto del Presidente del Consiglio dei ministri, effettivamente ha messo a fuoco quali erano i problemi del precedente decreto Monti che la nuova disciplina in parte risolve.

A questo proposito e anche relativamente alla ricezione e all'adozione della direttiva NIS, che io spero avvenga molto prima del 9 maggio 2018, vorrei fare alcune considerazioni e poi alcune domande.

In particolare il decreto del Presidente del Consiglio dei ministri, soprattutto per quanto riguarda la parte relativa alle coperture funzionali, estendendo l'articolo 7-*bis* del decreto-legge n. 174 del 2015 anche alle operazioni cibernetiche, a mio avviso fa una forzatura che – questa è la domanda – dovrebbe essere sanata con un provvedimento normativo di rango primario.

Mi spiego: io considero questo un passaggio che spero porti a normare in maniera unitaria tutta la situazione cibernetica.

Perché dico questo ? Forse i colleghi ricordano che l'articolo 7-*bis* fu introdotto nel decreto missioni internazionali per estendere alle sole forze speciali la possibilità di adottare misure di *intelligence* di contrasto al terrorismo e, per quanto ci era stato descritto durante la fase di approvazione – ricordo che questo articolo fu approvato senza l'opposizione di nessuna delle forze

presenti in Parlamento – l'emendamento andava a coprire esclusivamente le operazioni che il Presidente del Consiglio autorizzava per operazioni in teatro.

Io ritengo che sia corretto dare coperture funzionali a chi opera nel mondo della *cyber*, siano militari oppure membri di altre componenti ministeriali. Penso, però, che estendere quella copertura con una norma che non ha lo stesso rango della legge che ha convertito il decreto possa creare delle preoccupazioni.

Per questo, la prima domanda che mi sorge è la seguente: è opportuno, secondo lei, introdurre una norma che definisca, come chiede la direttiva NIS, un'agenzia che abbia quel ruolo, che abbia un suo direttore e un suo percorso ben mirato ?

Come ripeto spesso, la *cyber* non è esclusivamente sicurezza, né esclusivamente difesa, ma è formazione, cultura, *business*; è un mondo a sé stante (si potrebbe definire un quinto dominio) e credo che non si possa approcciare il problema solamente da un punto di vista di sicurezza e di difesa.

Per esempio – e nel decreto del Presidente del Consiglio dei ministri non è possibile introdurle – non ci sono normative specifiche che riguardano i casi in cui un ente privato o una società subisca un attacco e non lo segnali. A differenza di ciò che avviene in altri Paesi, in Italia a oggi non c'è una sorta di reato che lo preveda.

Vado a concludere, per non tediare troppo i miei colleghi. Il punto fondamentale è: c'è bisogno o meno di una norma che faccia questo ?

Lei ha parlato dello stanziamento di 150 milioni di euro. In realtà, è un fondo generico assegnato, non c'è un fondo mirato al comparto *cyber* che riesca a definire un percorso anche pluriennale di investimenti. I 150 milioni nascono nel bilancio del 2015 per l'esercizio 2016. Nel bilancio del 2016 per l'esercizio 2017 non c'è stato nessun tipo di investimento. Voglio vedere cosa succede sul 2017 per il 2018.

Infine, la definizione del presidente-vicedirettore generale del DIS è un qualcosa che io ritengo possa essere urgente in quanto effettivamente tale figura risponde alle problematiche che in questi anni tutti avevamo valutato e rappresenta un elemento che potrebbe accelerare il percorso. Per esempio, credo che la fusione dei CERT sia da strutturare sulla base di un direttore che fa questo. La fusione dei CERT non è scritta nel decreto del Presidente del Consiglio dei ministri, ma credo sia corretto, anzi necessario e ineludibile, farlo.

ALESSANDRO PANSA, *Direttore generale del Dipartimento delle informazioni per la sicurezza (DIS)*. Io forse non l'ho detto, ma abbiamo condotto un'analisi prima dell'emanazione del decreto Gentiloni e abbiamo deciso di affrontare con questo tutti i temi che potevano essere affrontati con una normativa secondaria e non con una normativa primaria che avrebbe richiesto tempi più lunghi.

Di conseguenza, siamo entrati nel sistema quanto più profondamente potevamo, col decreto, col piano nazionale e col documento di economia e finanze, articolando tutte le mosse prima dell'arrivo di una normativa primaria, che deve passare per il Parlamento e richiede tempi più lunghi.

Sicuramente c'è bisogno di una normativa primaria, perché alcune cose non sono state previste. Ad esempio, l'unificazione dei CERT per noi è indispensabile e deve essere fatta. Noi, però, ci siamo già mossi. Stiamo mettendo i due CERT nello stesso luogo e daremo la responsabilità dei due CERT alla stessa persona.

Quando arriverà la norma, ufficialmente il CERT sarà uno solo, ma noi di fatto ci stiamo già materialmente portando avanti perché ce lo chiede l'Europa. La modalità cambierà, ma l'unificazione, a meno che non vogliamo andare in violazione della direttiva europea, va fatta.

Per quanto riguarda, invece, l'estensione delle garanzie funzionali per le attività *cyber*, esse erano previste dalla legislazione già prima della modifica introdotta nel 2015 dall'articolo 7-*bis*.

Infatti, l'articolo 7-*bis* per quel che riguarda il *cyber* ha definito il ruolo del CISR come organo unico competente per le crisi di sicurezza nazionale. Noi abbiamo detto che l'attacco informatico che mette in crisi la sicurezza nazionale è competenza del

CISR, per cui abbiamo riportato tutti gli organismi al di sotto di questa campana.

Per quanto riguarda le garanzie funzionali, queste sono già in atto, e venivano utilizzate già prima, perché le attività non convenzionali erano già definite.

Per quel che concerne la parte militare – lo ripeto – è un meccanismo che non attiene alle garanzie funzionali, perché, se l'azione è militare, è un'azione di guerra, quindi richiede un percorso diverso.

Noi lavoriamo insieme, noi siamo l'*intelligence* della difesa e, come tale, noi, lavorando nell'*intelligence* per la difesa, svolgiamo tutte le attività non convenzionali che servono alla difesa. Il perimetro è questo. Non vado più a fondo, se mi consentite.

Sono d'accordo con lei, onorevole Artini: l'obbligatorietà della denunzia che in qualche modo è prevista anche dalla direttiva NIS richiederà un intervento normativo. Infine, credo che la nomina del vicedirettore per il DIS sia una cosa in atto che non dovrebbe tardare.

ANTONINO MOSCATT. Grazie, prefetto, per la sua relazione e per le informazioni che ha portato qui in Commissione oggi.

Noi abbiamo chiesto la sua audizione – mi associo ai ringraziamenti del collega Artini alla Commissione affari costituzionali nella persona del presidente per tutti – proprio perché stiamo conducendo un'indagine conoscitiva che ci ha permesso di conoscere i vari assi che regolano, gestiscono e operano nell'ambito della *cyber security*.

Quella che le pongo è quasi una domanda retorica. Ritengo che, vista l'accelerazione che ci è stata attraverso l'emanazione dei vari decreti, ma anche le competenze del nostro patrimonio italiano, siamo un po' più avanti rispetto agli altri Stati.

Lei poneva una questione legata alla sicurezza verso gli attacchi terroristici. Penso sia una domanda che noi ci facciamo spesso anche quando parliamo di difesa europea comune. A che punto siamo sulla prevenzione nella *cyber security* nei rapporti internazionali ? Riusciamo a trovare dei momenti di collegamento con gli altri Stati per condividere alcune peculiarità, alcune competenze, ma soprattutto alcune informazioni che consentono di poter meglio interfacciarsi in un sistema internazionale ? Questa è la prima domanda.

La seconda è legata a quanto lei ha affermato nella sua relazione. Riprendo anche quello che affermava il collega Artini. *Cyber security* significa tutelare la sicurezza nazionale, ma anche gli interessi di chi opera nel nostro territorio, dalle banche – i principali soggetti che ricevono gli attacchi – alle grandi aziende italiane, che sono la spina dorsale del nostro Paese.

Abbiamo un sistema di monitoraggio anche rispetto agli attacchi che arrivano ai privati ? Vorrei sapere, per prima cosa, se ci sono delle denunce e se ci sono delle richieste di intervento e, in secondo luogo, quante e quali sono le stime, se ci sono state.

Ipoteticamente che danni potrebbe provocare nelle grandi strutture un attacco di questo tipo ? Parliamo naturalmente, non della piccola azienda, ma delle grandi aziende italiane.

Infine, noi durante le visite che abbiamo fatto delle varie strutture che si occupano di *cyber security* abbiamo notato una cosa che ci veniva detta. L'infrastrutturazione dei sistemi viene fatta, come ovvio, con delle gare pubbliche a cui possono partecipare tutte le aziende, non solo quelle italiane. Ci è stato riferito che alcuni lotti di bandi venivano affidati ad alcune aziende che non erano italiane piuttosto che ad altre che avevano vinto anche il completamento dell'infrastrutturazione.

In questo caso non pensa che anche lì dovrebbero esserci delle restrizioni, al fine di mantenere la sicurezza del nostro Stato, facendo in modo che ci siano delle aziende specifiche che possono fare ciò ? Esse, infatti, entrano nella carne viva del nostro sistema e acquisiscono dei dati, delle informazioni e degli elementi che, se non sotto tutela dello Stato, possono essere gestiti in maniera non perfettamente consona.

DANIELA MATILDE MARIA GASPARINI. Io seguo più da vicino gli enti locali e mi stavo domandando, dopo la relazione del prefetto, che ringrazio, se sul tema sicurezza sia chiaro – credo proprio di sì – che gli enti locali siano ormai dei soggetti

dotati di banche dati molto articolate che riguardano anche temi che potrebbero essere legati all'ambito della difesa. Penso alle aziende pubbliche, che gestiscono tutto il ciclo delle acque, fognatura e quant'altro.

Siccome è noto che c'è un problema di sicurezza, perché tantissimi enti hanno banche dati spesso poco protette, vorrei chiedere – in questo rapporto con Italia digitale e in questo tentativo di riforme che abbiamo fatto per quanto riguarda in particolar modo la pubblica amministrazione (parlo di tentativi perché le leggi dichiarano già che occorre che alcuni livelli istituzionali, le ex province, per intenderci, abbiano il compito di coordinare le logiche e le architetture informatiche degli enti e provare a trovare un unico luogo, o comunque un luogo più semplice dell'area vasta, per quanto riguarda le banche dati) – se questo tema degli enti locali che hanno sicuramente dati sensibili (penso all'anagrafe e ad altri dati) è dentro al piano di sicurezza cibernetica.

Visto che Italia digitale investe, i comuni stanno investendo e la riforma della pubblica amministrazione fortunatamente obbliga all'utilizzo della rete in maniera più spinta rispetto al passato, mi chiedo se in questa fase di riordino dell'architettura siete voi il soggetto che indica come fare una nuova organizzazione anche per proteggere meglio i dati.

PRESIDENTE. Do la parola al prefetto per la replica.

ALESSANDRO PANSA, *Direttore generale del Dipartimento delle informazioni per la sicurezza (DIS)*. Parto dall'onorevole Gasparini e poi rispondo all'onorevole Moscatt. Ci stiamo anche occupando degli enti locali e sarà uno *step* immediatamente successivo all'organizzazione che stiamo realizzando.

Tenga presente che questo tema è affrontato, non in maniera chiarissima ma sintetica, anche dal documento di economia e finanze. Rientrano tra le iniziative legate alla revisione del piano: l'accelerazione della progettazione di un *data center* unificato di tutte le amministrazioni pubbliche, con una sostanziale riduzione dei costi, e una prima definizione di un *cloud* pubblico aperto a tutte le pubbliche amministrazioni. Noi riteniamo debba essere aperto a tutte le pubbliche amministrazioni che hanno attinenza con la sicurezza nazionale.

L'ambito nel quale opera il DIS è solo quello della sicurezza nazionale, però abbiamo tutti chiaro che i sistemi informatici, anche i più semplici e quelli che detengono dati non particolarmente importanti, sono un *asset* all'interno di un'architettura. Se l'intera architettura può essere compromessa attraverso un piccolo *asset*, anche quell'*asset* che da solo non è elemento della sicurezza nazionale automaticamente lo diventa.

Di conseguenza, noi riteniamo che una parte delle banche dati e delle infrastrutture che vengono gestite dagli enti locali dovrà essere ricondotta alla sicurezza nazionale, quindi anche in quell'ambito dovranno essere impartite delle regole e delle modalità.

Le regole e le modalità sono in embrione anche nel documento di economia e finanze, che afferma « detteremo le regole e non ci saranno spese consentite al di fuori di queste regole », quindi è un meccanismo economico che dovrà regolare il tutto.

Stiamo accelerando, anche con l'Agenda digitale e con l'AGID, tutti i processi che riguardano la definizione delle regole e le prescrizioni per i parametri minimi di sicurezza che tutti i sistemi devono avere.

Noi non abbiamo un ruolo di comando, ma un ruolo di promozione, accelerazione vigilanza e, quindi, siamo abbastanza pressanti anche in questo campo. Addirittura, con le risorse di cui noi disponiamo, daremo supporto a questi organismi esterni per quel che riguarda il potenziamento delle loro infrastrutture.

Passo alle domande poste dall'onorevole Moscatt. Noi, come già dicevo, siamo coinvolti nella definizione dei sistemi di prevenzione e nel chiarire che la prevenzione sarà basata su standard che consentono o non consentono l'accesso a determinate informazioni. Lo facciamo, non soltanto nella

parte di difesa, di investigazione, di mera *intelligence*, ma anche nella definizione delle procedure e dei sistemi.

Il primo e più importante di questi meccanismi è che noi per quanto riguarda le infrastrutture critiche certifichiamo sia le persone che le aziende.

La preservazione dei sistemi dalla possibilità che pezzi di sistema, attraverso il meccanismo delle gare pubbliche, vengano affidati a società di cui non si ha il controllo avviene attraverso la certificazione, se vengono individuati come sistemi sensibili che gestiscono infrastrutture critiche del Paese.

Questo è il meccanismo predisposto, che stiamo ampliando cercando di definire meglio il limite al quale la certificazione può arrivare. Questa è una materia classificata e onestamente non posso andare oltre.

Vi è poi quello che stiamo immaginando con la realizzazione del centro di valutazione presso il Ministero dello sviluppo economico, che dal lato suo deve certificare le tecnologie. Se ci sono tecnologie che non hanno una validazione da parte del Ministero dello sviluppo economico – attraverso un sistema che esiste già in altri Paesi, che abbiamo studiato e importato nel nostro Paese adattandolo e migliorandolo – chi vorrà fare offerte di prodotti che dovranno essere utilizzati per la sicurezza dovrà utilizzare prodotti che rientrano in quelli certificati, altrimenti non potrà partecipare al bando.

Il meccanismo non starà nel trovare una norma che esclude gli stranieri dalle gare pubbliche (perché altrimenti ci troveremmo in forte difficoltà), ma starà nel definire i parametri della sicurezza a cui chi partecipa alle gare dovrà attenersi.

Crediamo che questo ci consentirà di portare il livello della sicurezza molto più in alto. Noi siamo consapevoli che non raggiungeremo mai un livello della sicurezza del 100 per cento, perciò ci stiamo muovendo con un meccanismo che riguarda contemporaneamente tante mosse.

Mi permetto di dire che quella forse più importante, alla quale io credo più di tutte, è proprio il partenariato con il mondo della ricerca privato e accademico, perché lì noi potremo effettivamente mettere il meglio, tutto sotto la bandiera nazionale (non ci può essere altra bandiera) del contributo allo sviluppo.

Se avremo la capacità di sviluppare, ad esempio, l'algoritmo nazionale sicuro, noi utilizzeremo l'algoritmo nazionale sicuro. Sarà un algoritmo nazionale; chi lo può utilizzare lo utilizzerà e chi non lo può utilizzare non parteciperà alle gare. Diventa oggettivamente un meccanismo di difesa.

Avendo un laboratorio che lo studia costantemente e lo tiene sotto controllo, l'algoritmo nazionale verrà implementato continuamente per essere mantenuto a livelli di particolare sicurezza. L'algoritmo di criptazione di tutti i sistemi di comunicazione e di banche dati che hanno valore per la sicurezza nazionale dovrà essere garantito da un unico ente di certificazione. Nella sicurezza nazionale l'ente di certificazione siamo sempre noi. Noi mettiamo in campo le risorse che il mondo della ricerca può darci, le raccogliamo, prendiamo il meglio e poi lo certifichiamo.

Pertanto, c'è interesse anche a svilupparlo, perché chi lo sviluppa e ottiene il risultato conseguirà la possibilità di accedere al mercato attraverso una certificazione a cui chiaramente possono accedere anche tutti quelli che ce l'hanno.

PRESIDENTE. Ringrazio moltissimo il prefetto Pansa per le sue risposte molto chiare e dichiaro conclusa l'audizione.

La seduta termina alle 16.

Licenziato per la stampa
il 14 dicembre 2017

STABILIMENTI TIPOGRAFICI CARLO COLOMBO

17STC0027270