Camera dei deputati
Servizio Studi
XVII Legislatura

Documentazione per l'esame di
Progetti di legge

Norme in materia di difesa dello spazio cibernetico e istituzione del sistema nazionale di sicurezza cibernetica A.C. 3677

Dossier n° 615 - Schede di lettura
2 agosto 2017

Informazioni sugli atti di riferimento

A.C.	3677
Titolo:	Norme in materia di difesa dello spazio cibernetico e istituzione del sistema nazionale di sicurezza cibernetica
Iniziativa:	Parlamentare
Primo firmatario:	Artini
Iter al Senato:	No
Numero di articoli:	23
Date:	
presentazione:	15 marzo 2016
Commissione competente :	IV Difesa
Sede:	referente
Pareri previsti:	II Giustizia (ex articolo 73, comma 1-bis, del regolamento, per le disposizioni in materia di sanzioni), III Affari Esteri, V Bilancio, VII Cultura, IX Trasporti, X Attività Produttive e XIV Politiche dell'Unione Europea

Quadro normativo

L'architettura istituzionale italiana per la sicurezza cibernetica è attualmente delineata nel DPCM del 17 febbraio 2017, recante i nuovi indirizzi per la protezione cibernetica e la sicurezza informatica nazionali.

Il richiamato provvedimento sostituisce integralmente, pur riprendendone l'impostazione generale, il precedente DPCM del 24 gennaio 2013, adottato dal Governo Monti in linea con analoghe iniziative intraprese a livello europeo nel campo della protezione cibernetica.

Per un approfondimento dei due provvedimenti si rinvia al *dossier* n. 305 "Direttiva recante gli indirizzi per la protezione cibernetica, Testo a fronte tra il DPCM 24 gennaio 2013 e DPCM 17 febbraio 2017".

Quadro strategico nazionale per la sicurezza dello spazio cibernetico

Contribuiscono a definire la cornice complessiva dell'attuale sistema di sicurezza cibernetica il *Quadro strategico nazionale per la sicurezza dello spazio cibernetico* del dicembre 2013 ed il *Piano nazionale per la protezione cibernetica e la sicurezza informatica* del 2017.

Il primo di questi due documenti, adottato dal Presidente del Consiglio dei ministri **su proposta** del Comitato Interministeriale per la Sicurezza della Repubblica (Cisr), rappresenta il Documento di lungo periodo contenente l'indicazione dei profili e delle tendenze evolutive delle minacce e delle vulnerabilità dei sistemi e delle reti di interesse nazionale, la definizione dei ruoli e dei compiti dei diversi soggetti, pubblici e privati, e di quelli nazionali operanti al di fuori del territorio del Paese, l'individuazione degli strumenti e delle procedure con cui perseguire l'accrescimento della capacità del Paese di prevenzione e risposta rispetto ad eventi nello spazio cibernetico, anche in un'ottica di diffusione della cultura della sicurezza.

Piano nazionale per la protezione cibernetica e la sicurezza informatica

A sua volta il *Piano nazionale per la protezione cibernetica e la sicurezza informatica* del 2017, adottato, dal Presidente del Consiglio dei ministri **su deliberazione** del Cisr, rappresenta il documento di breve periodo attraverso il quale sono definiti gli obiettivi da conseguire e le linee di azione da porre in essere per realizzare il quadro strategico nazionale.

Il *Piano nazionale per la protezione cibernetica e la sicurezza informatica* del 2017 sostituisce integralmente il precedente *Piano nazionale per la protezione cibernetica e la sicurezza informatica* del 2013.

Relazioni sulla politica dell'informazione per la sicurezza predisposte dal Governo

Di estrema rilevanza per la valutazione dell'architettura nazionale per la sicurezza dello spazio cibernetico sono infine le **Relazioni annuali sulla politica dell'informazione per la sicurezza predisposte dal Governo** (Presidenza del Consiglio dei ministri) e trasmesse al Parlamento ai sensi dell'articolo 38 della legge n. 124 del 2007.

Tale norma prevede, infatti, che entro il mese di febbraio di ogni anno il Governo trasmetta al Parlamento una relazione scritta, riferita all'anno precedente, sulla politica dell'informazione per la sicurezza e sui risultati ottenuti. Alla relazione è allegato il documento di sicurezza nazionale, concernente le attività relative alla protezione delle infrastrutture critiche materiali e immateriali nonché alla protezione cibernetica e alla sicurezza informatica (comma 1-bis).

La legge n. 124 del 2007 reca disposizioni concernenti il *sistema di informazione per la sicurezza della Repubblica e nuova disciplina del segreto.* L'elenco delle relazioni trasmessa al parlamento ai sensi della richiamata legge è consultabile al sito https://www.sicurezzanazionale.gov.it/sisr.nsf/.../relazione-annuale.html.

Il DPCM 17 febbraio 2017

Ciò premesso in via generale, nel nuovo assetto strategico delineato nel **DPCM del 17 febbraio 2017 c**.d. decreto Gentiloni) al **Presidente del Consiglio dei ministri** è affidata l'alta direzione e la responsabilità generale della politica dell'informazione per la sicurezza (articolo 1 del DPCM 17 gennaio 2017). In tale funzione emana le disposizioni necessarie per l'organizzazione e il funzionamento del Sistema di sicurezza cibernetica e, in particolare, sentito il Comitato interministeriale per la sicurezza della Repubblica, impartisce al Dipartimento delle informazioni per la sicurezza e ai servizi di informazione per la sicurezza direttive per rafforzare le attività di informazione per la protezione delle infrastrutture critiche materiali e immateriali, con particolare riguardo alla protezione cibernetica e alla sicurezza informatica nazionale.

Il Comitato interministeriale per la sicurezza della Repubblica

In presenza di situazioni di crisi che coinvolgono aspetti di sicurezza nazionale il **Comitato Interministeriale per la Sicurezza della Repubblica** (Cisr), presieduto dal Presidente del Consiglio e composto dall' l'Autorità delegata e dai ministri degli Affari Esteri e della Cooperazione internazionale (Maeci), dell'Interno, della Difesa, della Giustizia, dell'Economia e delle Finanze (Mef) e dello Sviluppo economico (Mise), partecipa alle determinazioni del Presidente del consiglio con funzioni di consulenza e di proposta, nonché di deliberazione.

In CISR, inoltre, esprime parere sulle direttive del Presidente, sorveglia l'attuazione del Piano Nazionale, approva le linee di indirizzo per favorire la collaborazione fra gli attori istituzionali e stabilisce gli obbiettivi in materia di protezione cibernetica nazionale.

A supporto del CISR opera il cosiddetto "**CISR tecnico** "presieduto dal Direttore Generale del DIS".

Il Direttore generale del Dipartimento delle informazioni per la sicurezza

A sua volta spetta al **Direttore generale del Dipartimento delle informazioni per la sicurezza** (DIS) il compito di definire linee di azione che dovranno portare ad assicurare i necessari livelli di sicurezza dei sistemi e delle reti di interesse strategico, sia pubblici che privati, verificandone ed eliminandone le vulnerabilità. Per la realizzazione di tali iniziative, il direttore generale del DIS predisporrà gli opportuni moduli organizzativi anche attraverso il coinvolgimento del mondo accademico e della ricerca ed avvalendosi di risorse di eccellenza e della collaborazione di imprese del settore.

In relazione agli specifici compiti del Direttore del DIS nel campo della protezione cibernetica, si rinvia al resoconto stenografico della seduta delle Commissione riunite I (Affari Costituzionali) e IV (Difesa) della Camera dei deputati del 14 giugno 2017 nel corso della quale ha avuto luogo l'audizione del Direttore generale del Dipartimento delle informazioni per la sicurezza, Alessandro Pansa, sulle problematiche legate alla difesa e alla sicurezza nello spazio cibernetico. Il resoconto è consultabile al seguente link: http://www.camera.it/leg17/1102?id_commissione=04&shadow_organo_parlamentare=2078&sezione=commissioni&tipoDoc=elencoResoconti&idLegisla

Poteri del DIS nel campo della sicurezza cibernetica

Spetta, invece, al DIS nel suo complesso, coadiuvato dalle Agenzie (AISE e AISI), raccogliere le informazioni finalizzate alla protezione dello spazio cibernetico nazionale e formulare analisi, valutazioni e previsioni della minaccia cibernetica. Inoltre, è consentito al DIS e alle agenzie l'accesso agli archivi informatici delle pubbliche amministrazioni e dei soggetti erogatori di servizi pubblici secondo le modalità previste dal Dpcm n.4/2009.

Il Nucleo per la sicurezza cibernetica

A supporto del Presidente del Consiglio per gli aspetti relativi alla prevenzione e all'approntamento rispetto a situazioni di crisi, opera il **Nucleo per la sicurezza cibernetica (Nsc)**, originariamente istituito presso l'Ufficio del Consigliere militare del Presidente del Consiglio dei Ministri ed ora collocato all'interno del DIS.

Il Nucleo organismo è chiamato a svolgere una serie di attività nella fase di gestione delle crisi di natura cibernetica, con particolare riferimento agli aspetti relativi alla prevenzione di situazioni di crisi cibernetica e all'attivazione delle procedure di allertamento.

Il Nucleo è presieduto da un vice direttore generale del DIS, designato dal direttore generale ed è composto dal Consigliere militare del Presidente del Consiglio e da un rappresentante rispettivamente del DIS, dell'AISE, dell'AISI, del Ministero degli affari esteri, del Ministero dell'interno, del Ministero della difesa, del Ministero della giustizia, del Ministero dello sviluppo economico, del Ministero dell'economia e delle finanze, del Dipartimento della protezione civile e dell'Agenzia per l'Italia digitale.

Con particolare riferimento al campo della prevenzione e della preparazione ad eventuali situazioni di crisi cibernetica, spetta **al Nucleo per la Sicurezza Cibernetica:**

1. promuovere la programmazione e la pianificazione operativa della risposta a situazioni di crisi cibernetica da parte delle amministrazioni e degli operatori privati interessati e l'elaborazione delle necessarie procedure di coordinamento interministeriale;
2. mantenere attiva, 24 ore su 24, 7 giorni su 7, l'unità per l'allertamento e la risposta a situazioni di crisi cibernetica;
3. valutare e promuovere procedure di condivisione delle informazioni, anche con gli operatori privati interessati, al fine di diffondere gli allarmi relativi ad eventi cibernetici e per la gestione delle crisi;
4. acquisire le comunicazioni circa i casi di violazione o dei tentativi di violazione della sicurezza o di perdita dell'integrità dal Ministero dello sviluppo economico, dagli organismi di informazione per la sicurezza, dalle Forze di polizia e, in particolare, dal CNAIPIC, nonché dalle strutture del Ministero della difesa e dai CERT;
5. promuovere e coordinare, in raccordo con il Ministero dello sviluppo economico e con l'Agenzia per l'Italia digitale per i profili di rispettiva competenza, lo svolgimento di esercitazioni interministeriali, ovvero la partecipazione nazionale in esercitazioni internazionali che riguardano la simulazione di eventi di natura cibernetica;
6. costituire punto di riferimento nazionale per i rapporti con l'ONU, la NATO, l'UE e le altre organizzazioni internazionali e gli altri Stati, ferme restando le specifiche competenze del Ministero dello sviluppo economico, del Ministero degli affari esteri e della cooperazione internazionale, del Ministero dell'interno, del Ministero della difesa e di altre amministrazioni previste dalla normativa vigente, assicurando comunque in materia ogni necessario raccordo.

Peraltro, nel campo dell'attivazione delle azioni di risposta e ripristino rispetto a situazioni di crisi cibernetica, il Nucleo per la Sicurezza Cibernetica:

1. riceve, anche dall'estero, le segnalazioni di eventi cibernetici e dirama gli allarmi alle amministrazioni e agli operatori privati;
2. valuta se l'evento assume dimensioni, intensità o natura tali da non poter essere fronteggiato dalle singole amministrazioni competenti in via ordinaria, ma richiede l'assunzione di decisioni coordinate in sede interministeriale;
3. informa tempestivamente il Presidente del Consiglio, per il tramite del Direttore Generale del DIS, sulla situazione in atto.

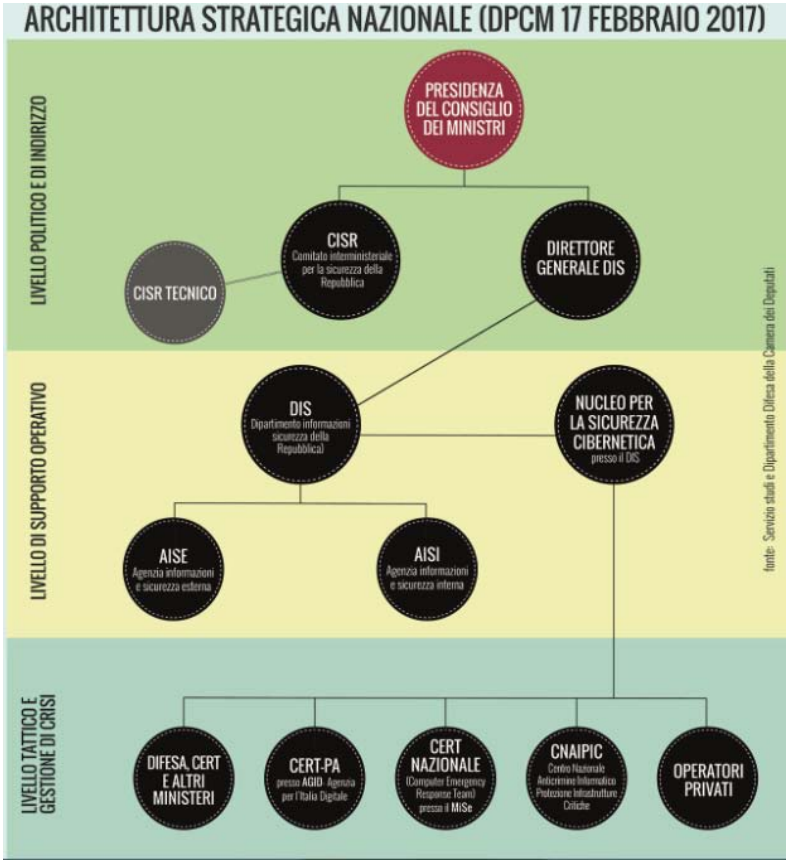
Il ruolo degli operatori privati

Tra gli attori dell'architettura nazionale preposta a garantire la sicurezza cibernetica e la sicurezza informatica nazionale, Il DPCM 17 febbraio 2017 include, oltre ai soggetti pubblici, anche gli **operatori privati** che forniscono reti pubbliche di comunicazione o servizi di comunicazione elettronica accessibili al pubblico, gli operatori di servizi essenziali e i fornitori di servizi digitali e quelli che gestiscono infrastrutture critiche di rilievo nazionale ed europeo, il cui funzionamento è condizionato dall'operatività di sistemi informatici e telematici.

Tali soggetti sono tenuti a:

1. comunicare al Nucleo per la sicurezza cibernetica, ogni significativa violazione della sicurezza o dell'integrità dei propri sistemi informatici, utilizzando canali di trasmissione protetti;
2. adottare le best practices e le misure finalizzate all'obiettivo della sicurezza cibernetica;
3. fornire iinformazioni agli organismi di informazione per la sicurezza che consentono ad essi l'accesso ai Security Operations Center aziendali e ad altri eventuali archivi informatici di specifico interesse ai fini della sicurezza cibernetica;
4. collaborare alla gestione delle crisi cibernetiche contribuendo al ripristino della funzionalità dei sistemi e delle reti da essi gestiti.

Infine, un elemento di novità del nuovo DPCM del 2017 è la previsione normativa che impegna il Ministro dello sviluppo economico a promuovere l'istituzione di un centro di valutazione e certificazione nazionale per la verifica delle condizioni di sicurezza e dell'assenza di vulnerabilità su prodotti, apparati e sistemi destinati ad essere utilizzati per il funzionamento di reti, servizi e infrastrutture critiche.



Difesa cibernetica

Per quanto riguarda più specificatamente il tema della **difesa cibernetica,** il Libro bianco per la sicurezza internazionale e la difesa 2015, nell'individuare gli **obiettivi per la sicurezza internazionale e la difesa** che orienteranno in modo innovativo l'azione del Dicastero e favoriranno l'integrazione delle risorse potenzialmente esprimibili da tutti gli attori istituzionali, assegna un ruolo prioritario alla difesa dello spazio cibernetico.

"La particolare dipendenza dell'Occidente da un sistema di reti informatiche ", si legge nel Libro Bianco "comporta l'affermazione di un nuovo dominio operativo, quello cibernetico, che dovrà essere presidiato e difeso. Gli effetti di attacchi cibernetici alle reti o ai servizi informatici possono essere particolarmente distruttivi per i Paesi occidentali e, se di successo, comportare effetti sulla società paragonabili a quelli di un conflitto combattuto con armi convenzionali". Ed ancora nel richiamato Documento si osserva come la Difesa svilupperà, in piena armonia con la strategia nazionale sulla protezione informatica, le possibilità di difesa contro attacchi di natura cibernetica che dovessero eccedere le capacità predisposte dalle agenzie civili.

Le Forze armate dovranno quindi avere adeguate capacità operative a livello Interforze, *integrate nel complesso delle forze NATO*, per respingere eventuali aggressioni militari che si dovessero manifestare contro l'Italia e i suoi interessi vitali, operando nelle tre dimensioni fisiche, in quella dei fattori umani e in quella cibernetica.

Piano nazionale per la protezione cibernetica e la sicurezza informatica

A sua volta nel *Piano nazionale per la protezione cibernetica e la sicurezza informatica* del 2017 prevede il supporto alle iniziative del Ministero della Difesa volte a istituire un Comando Interforze Operazioni Cibernetiche (CIOC), deputato alla protezione dei sistemi e delle reti di quel Dicastero nonché all'effettuazione delle operazioni in campo cibernetico.

Si ricorda, inoltre come nel corso del **vertice NATO di Varsavia** del luglio 2016 gli alleati hanno riconosciuto il cyberspazio come dominio di operazioni in cui la NATO deve difendersi nel modo più efficace come fa nei tradizionali domini operativi .

Sul tema della sicurezza e la difesa nello spazio cibernetico. È attualmente in corso di

svolgimento un'indagine conoscitiva presso la IV Commissione difesa della Camera.

La direttiva NIS

A livello europeo si ricorda che la **direttiva 2016/1148**, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione (c.d. "Direttiva NIS"), rappresenta il primo provvedimento di carattere generale adottato in ambito europeo sul tema della sicurezza informatica.

Attraverso l'adozione da parte dei singoli Stati membri di una di una serie di misure strategiche e organizzative comuni in materia di sicurezza cibernetica, la direttiva mira a raggiungere un **livello elevato di sicurezza** dei sistemi, delle reti e delle informazioni in ambito europeo, nella convinzione che il rafforzamento del dominio digitale rappresenti un importante volano di crescita del sistema economico dell'Unione, incidendo, positivamente sulla propensione ad investire degli operatori economici, con particolare riferimento al commercio internazionale.

Nello specifico, la direttiva in esame prevede l'adozione di una serie di iniziative da parte degli stati membri volte a **migliorare le capacità** di sicurezza cibernetica dei singoli Paesi, **aumentare il livello di collaborazione in ambito europeo** nella prevenzione delle minacce cibernetiche e nelle eventuali misure di risposta ad attacchi *cyber*, **sviluppare** una cultura della sicurezza con particolare riferimento a quei settori vitali per l'economia e la società e che si basano sulle tecnologie dell'informazione e della comunicazione.

Relativamente al miglioramento delle capacità dei singoli Stati dell'Unione, la direttiva "fa obbligo a tutti gli Stati membri di adottare una **strategia nazionale** in materia di sicurezza della rete e dei sistemi informativi" (articoli 1 e 7), definendo, in particolare:

1. gli **obiettivi** strategici;
2. le opportune **misure strategiche** e regolamentari al fine di conseguire e mantenere un livello elevato di sicurezza delle reti e dei sistemi informativi;
3. **gli operatori di servizi essenziali** nei settori reputati essenziali dal punto di vista della sicurezza cibernetica. In relazione all'individuazione degli operatori essenziali la direttiva fornisce alcuni criteri per la loro individuazione.

In particolare, è **qualificato come operatore di servizio essenziale** il soggetto pubblico o privato che appartiene alle categorie elencate nell'allegato 2 della medesima direttiva (energia, trasporti, settore bancario, settore sanitario, fornitura e distribuzione di acqua potabile, infrastrutture digitali, infrastrutture dei mercati finanziari), il quale fornisce un servizio reputato essenziale per il mantenimento di attività sociali e/o economiche fondamentali. Si prevede, inoltre, che la fornitura di tale servizio dipenda dalla rete e dai sistemi informativi e che un eventuale incidente avrebbe effetti negativi rilevanti sulla fornitura di tale servizio.

In relazione all'adempimento di cui al precedente n. 3 la direttiva fissa il termine del il 9 novembre 2018.

Sempre con riferimento al miglioramento delle capacità di sicurezza cibernetica e alla cooperazione a livello europeo ed internazionale in materia di sicurezza delle reti e dei sistemi informativi la direttiva (artt.8 e 9) stabilisce l'obbligo per gli Stati membri di:

1. individuare una o più autorità nazionali in materia di sicurezza delle reti e dei sistemi informativi, con funzioni, tra le altre, di controllo circa l'applicazione della direttiva;
2. designare un **punto di contatto unico nazionale** in materia di sicurezza delle reti e dei sistemi informativi ("punto di contatto unico");
3. istituire uno o più Gruppi di intervento per la sicurezza informatica in caso di incidente (*Computer Security Incident Response Team* **CSIRT**) responsabili del monitoraggio degli incidenti a livello nazionale, fornendo allarmi tempestivi, avvisi ed annunci con lo scopo di diffondere informazioni su rischi ed incidenti.

In particolare, il **punto di contatto** dovrà garantire la cooperazione transfrontaliera tra le autorità nazionali competenti in materia di sicurezza cibernetica e il gruppo di cooperazione di cui all'articolo 11 della direttiva, composto da rappresentati degli Stati membri, dalla Commissione e dall'ENISA (*European Union for Network and Information Security Agency*).

Il punto di contatto dovrà, altresì, svolgere un ruolo di coordinamento tra i richiamati organismi nazionali e la rete di *Computer Security Incident Response Team* formata da rappresentanti dei CSIRT degli Stati membri e del CERT-UE.

Spetterà, invece, ai Gruppi di intervento per la sicurezza informatica (**CSIRT),** gestire gli incidenti e i rischi cibernetici secondo una procedura ben definita dai singoli ordinamenti. A tal fine gli Stati membri dovranno garantire le necessarie risorse finanziarie.

Contenuto

La proposta di legge in esame, composta da 24 articoli, è strutturata in due diversi titoli: il primo, recante norme volte a individuare le finalità dell'intervento legislativo e definire il

significato di talune espressioni tecniche ricorrenti nel testo della proposta di legge e l'individuazione degli organismi istituzionali con competenze nel campo della sicurezza cibernetica (artt. da 1 a 3); il secondo, concernente sia disposizioni specifiche in materia di difesa cibernetica (artt. da 4 a 8), sia norme che incidono sull'attuale sistema nazionale di sicurezza cibernetica (artt. da 9 a 23).

Ambito di applicazione dell'intervento legislativo e definizioni (articoli da 1 a 3)

L'**articolo 1** della proposta di legge, pur non intervenendo direttamente sull'articolo 117 della Costituzione stabilisce il principio generale in forza del quale "**le competenze** relative alla disciplina e all'organizzazione della difesa dello **spazio cibernetico** spettano allo Stato ai sensi del secondo comma, lettere *d*) ed *h*) del richiamato articolo" (comma 1).

Come noto tali lettere attribuiscono tra l'altro allo Stato la potestà legislativa esclusiva in materia di difesa e Forze armate (lettera *d*)) e ordine pubblico e sicurezza (lettera *h*)).

Il medesimo articolo 1 delimita, inoltre, l'ambito di operatività della Difesa nel campo cibernetico precisando che costituisce oggetto di interesse militare ogni attacco volto a minacciare il funzionamento e l'integrità della rete informatica e delle infrastrutture informatizzate critiche di interesse nazionale (comma 2).

In relazione alla formulazione del comma 2 andrebbe valutata l'opportunità di costruire la disposizione sotto forma di novella al Codice dell'ordinamento militare (d.lgs. n. 66 del 2010) che attualmente ricomprende in un unico testo normativo le disposizioni di rango legislativo concernenti l'organizzazione, le funzioni e l'attività della difesa e della sicurezza militare e delle Forze armate. Tale considerazione vale altresì per le altre disposizioni della proposta di legge che attengono ai richiamati profili trattati nel decreto legislativo n. 66 del 2010.

Per quanto concerne le **definizioni** di taluni termini tecnici impiegati nella proposta in esame, l'articolo 2, da un lato, conferma il significato delle espressioni "spazio cibernetico", "sicurezza cibernetica", "evento cibernetico", "minaccia cibernetica" e "situazione di crisi cibernetica" attualmente contenuto nell'articolo 2 del DPCM 17 febbraio 2017, dall'altro, prevede nuove terminologie non presenti nel richiamato decreto e riguardanti le nozioni di "sovranità cibernetica", "contromisure cibernetiche" ed *info sharing.*

Nello specifico, la sovranità cibernetica è intesa come la capacità dello Stato di essere autosufficiente nella costruzione, nel controllo e nella certificazione in ambito sia di *software*, sia di *hardware*. A loro volta le contromisure cibernetiche sono rappresentate da quelle azioni mirate alla risposta a una minaccia cibernetica, che possono produrre effetti anche al di fuori del territorio nazionale. Per "*info sharing"* si intende il sistema costituito da una piattaforma informatica per la condivisione delle informazioni sugli allarmi e sugli eventi cibernetici, contenente altresì le soluzioni relative agli allarmi e agli eventi cibernetici.

Disposizioni in materia di Difesa cibernetica (articoli da 4 a 8)

Gli articoli da 3 a 8 della proposta di legge recano una serie di disposizioni eterogenee nel campo della difesa cibernetica e concernenti la formazione specialistica del personale militare nel campo della *cyber defence*, la previsione della difesa cibernetica tra i compiti delle Forze armate, la ricerca militare nel campo cibernetico.

Per quanto riguarda quest'ultimo profilo, l'articolo 4 della proposta di legge assegna al **Segretario generale della Difesa**, direttore nazionale degli armamenti, il compito di:

Competenze del Segretario generale della Difesa nel campo della

1. promuovere lo sviluppo della ricerca tecnologica nel campo della sicurezza

cibernetica, considerata di interesse militare, secondo gli indirizzi impartiti dal Ministro della difesa;

sicurezza cibernetica

2. assicurare la piena integrazione delle attività di ricerca militare nel settore cibernetico con quelle previste dal Programma nazionale per la ricerca;
3. predisporre e attuare, nell'ambito della propria competenza, le misure necessarie per agevolare e incrementare lo scambio delle informazioni tra i soggetti utilizzatori delle tecnologie e i soggetti operanti nelle attività di sviluppo o di produzione delle medesime;
4. promuovere iniziative di cooperazione sinergica tra centri di ricerca, università, imprese industriali e operatori finanziari nazionali, con l'eventuale partecipazione di analoghe istituzioni, imprese e operatori esteri, allo scopo di favorire il raggiungimento della piena sovranità cibernetica nazionale e una maggiore integrazione nell'ambito dell'Unione europea.

Spetta al Ministro della Difesa impartire gli indirizzi per l'attuazione delle richiamate disposizioni.

In relazione alla disposizione in esame si osserva che, allo stato, il DPCM del 17 febbraio 2017, nel delineare l'architettura strategica nazionale in materia di sicurezza cibernetica non assegna una specifica competenza in ambito cibernetico al Segretario Generale della Difesa, ferme restando le attribuzioni nel campo della *cyber defence* in capo al Ministero della difesa esplicitate sia nel Quadro strategico nazionale per la sicurezza dello spazio cibernetico, sia nel Piano nazionale per la sicurezza dello spazio cibernetico.
In base al DPCM del 17 febbraio 2017 spetta attualmente al NSR valutare e promuovere procedure di condivisione delle informazioni, anche con gli operatori privati interessati, al fine di diffondere gli allarmi relativi ad eventi cibernetici e per la gestione delle crisi. Il Nucleo costituisce punto di riferimento nazionale per i rapporti con l'ONU, la NATO, l'UE.
Si ricorda, altresì, che in base all'articolo 41 del d. lgs. n. 66 del 2010, il Segretario generale della Difesa predispone, d'intesa con il Capo di stato maggiore della difesa, le proposte di pianificazione generale finanziaria annuale e pluriennale relative all'area industriale, pubblica e privata, di interesse della Difesa ed è responsabile, nel quadro della pianificazione generale dello strumento militare, dell'organizzazione e del funzionamento dell'area tecnico-industriale e tecnico-amministrativa della Difesa.

Il successivo **articolo 5** interviene, a sua volta, sul tema della **formazione del personale militare nel settore della sicurezza cibernetica** autorizzando il Governo ad adottare, entro sessanta giorni dalla data di entrata in vigore della legge, un apposito Regolamento che, intervenendo sul Testo unico delle disposizioni regolamentari in materia di ordinamento militare, assicuri la crescita professionale, la formazione permanente e la specializzazione del personale militare a ogni livello nel settore della sicurezza cibernetica.

Iniziative in favore della formazione del personale militare nel settore della sicurezza cibernetica

Al riguardo, l'articolo 5 individua una serie di criteri direttivi che dovranno essere tenuti in considerazione dal Governo in sede di attuazione della norma e riguardanti i diversi livelli di conoscenza nel campo cibernetico che devono essere garantiti negli ordinamenti delle scuole militari, delle Accademie, nelle scuole di applicazione e di guerra e nelle scuole per gli allievi sottufficiali.

Le Scuole Militari (o Collegi militari) sono scuole superiori ad ordinamento militare, comprendenti percorsi formativi di Liceo Classico, Scientifico e Scientifico Europeo, cui possono accedere i ragazzi a partire dai 15 anni (ovvero dal I° Liceo per il Classico e dal III° per lo Scientifico), con lo scopo di prepararli per l'accesso alle Accademie Militari. La tradizione delle Scuole Militari è nata con la Scuola Militare *Nunziatella* di Napoli (Esercito e Arma dei carabinieri) e la Scuola Navale Militare Francesco *Morosini* di Venezia; in anni recenti, è stata riaperta la Scuola Militare *Teuliè* di Milano e la Scuola Militare Aeronautica *Douhet* di Firenze.
Le Accademie Militari sono le istituzioni formative degli Ufficiali di carriera delle diverse Forze Armate; istituzioni in cui, oltre a conseguire un diploma di Laurea (che, in base all'Accademia ed al percorso di inquadramento scelto può essere in Scienze Strategiche, Ingegneria, Medicina e Chirurgia, etc.), si riceve una formazione militare approfondita. I percorsi formativi d'Accademia, compreso il proseguimento dei corsi che si segue presso le Scuole d'Applicazione d'Arma post-Accademia, durano 4 o 5 anni.
Le Accademie Militari sono l'Accademia dell'Esercito e dell'Arma dei Carabinieri, a Modena, l'Accademia dell'Aeronautica, a Pozzuoli, l'Accademia Navale, a Livorno, l'Accademia della Guardia di Finanza, a Bergamo.
Le Scuole di Guerra sono invece istituti formativi avanzati, riservati agli Ufficiali di carriera delle Forze Armate con diversi anni di esperienza, che vi devono frequentare i corsi di perfezionamento e preparazione alle responsabilità di comando superiore nel momento di passaggio dai ranghi degli Ufficiali "inferiori" a quelli degli Ufficiali "superiori". Esistono poi le cosiddette Scuole di Formazione che sono centri o istituti interni alle diverse Forze Armate, e che forniscono l'inquadramento iniziale per Sottufficiali o Truppa addetta a particolari ruoli/specialità. Erogano inoltre corsi di formazione, di breve o media durata, al personale già inquadrato (Truppa, Sottufficiali, Ufficiali), per il conseguimento di particolari competenze operative e specialistiche.

A sua volta l'**articolo 6** della proposta di legge novella l'articolo 10 del Codice dell'ordinamento militare al fine di attribuire al Ministro della Difesa la specifica

Direttive del Ministro della

competenza in merito all'emanazione di direttive in materia di sicurezza cibernetica.

Difesa in ambito cibernetico

In relazione alla disposizione in esame, si ricorda che la sicurezza cibernetica rappresenta una categoria generale che interessa una pluralità di ambiti di interesse. Pertanto, al fine di evitare possibili dubbi interpretativi andrebbe valutata l'opportunità di limitare l'ambito di applicazione della disposizione al campo specifico della sicurezza cibernetica militare.

Ulteriori modifiche al Codice dell'ordinamento militare sono previste dai successivi articolo **7 e 8**.

La prima di queste disposizioni, dopo aver enunciato il principio generale in forza del quale le Forze armate concorrono alla protezione dello spazio cibernetico nel rispetto delle competenze già previste in capo ad altri soggetti istituzionali modifica l'articolo 89 del Codice dell'ordinamento militare, concernente i **compiti delle Forze armate,** al fine di prevedere tra le varie attribuzioni anche quella relativa al concorso nella protezione dello spazio cibernetico. La medesima disposizione prevede, inoltre, l'inserimento nel Codice del nuovo articolo 89-*bis* in materia di **contromisure cibernetiche**, intese come quelle azioni mirate di risposta a una minaccia cibernetica, che possono produrre effetti anche al di fuori del territorio nazionale.

Procedimento decisionale relativo all'avvio di contromisure cibernetice

Al riguardo, il nuovo articolo 89-*bis* definisce il procedimento decisionale concernente l'avvio di "contromisure cibernetiche" e le **garanzie funzionali** previste per il personale che vi è preposto. Il successivo articolo 16 della proposta di legge disciplina, invece, l'organizzazione del Comando interforze operativo cibernetico al quale spetta l'otganizzazione e la direzione operativa delle attività relative alla difesa cibernetica.

Per quanto concerne l'autorizzazione all'avvio di contromisure ciibernetiche il primo passaggio procedurale previsto dal comma 2 del nuovo articolo 89-*bis* è rappresentato dalla delibera del Consiglio dei ministri in ordine all'utilizzo delle contromisure cibernetiche. Tale deliberazione dovrà essere adottata previa comunicazione al Presidente della Repubblica anche eventualmente convocando il Consiglio supremo di difesa, ove se ne ravvisi la necessità. Successivamente Il Governo dovrà comunicare al Comitato parlamentare per la sicurezza della Repubblica " le misure deliberate".

Garanzie funzionali per il personale impiegato in contromisure cibernetiche

In relazione alle garanzie funzionali il comma 3 del nuovo articolo 89-*bis* richiama quanto previsto dall'articolo 17 della legge 3 agosto 2007, n. 124 che attualmente reca la particolare scriminante prevista per il personale dei servizi di informazione per la sicurezza. Ai sensi di tale norma non è punibile il personale dei Servizi di informazione per la sicurezza "che ponga in essere condotte previste dalla legge come reato, legittimamente autorizzate di volta in volta in quanto indispensabili alle finalità istituzionali di tali servizio".

In relazione alla formulazione del nuovo articolo 89-*bis* si osserva che tale disposizione non specifica la categoria di personale, militare e/o civile, che potrà prendere parte ad operazioni cibernetiche aventi carattere di "contromisure" facendo genericamente riferimento "agli operatori che attuano le deliberazioni".

Al contempo, nel definire il quadro delle garanzie funzionali loro applicabili la disposizione in esame richiama la normativa prevista per il personale che opera nei Servizi di informazione per la sicurezza. Tale normativa, allo stato (comma 7, art. 17 della legge n. 124 del 2007) può essere estesa a personale non addetto ai servizi di informazione per la sicurezza qualora abbia operato in concorso con uno o più dipendenti dei servizi di informazione per la sicurezza e risulti che il ricorso alla loro opera da parte dei servizi di informazione per la sicurezza è stato indispensabile ed autorizzato secondo apposite procedure.

Ai sensi del comma 5 del nuovo articolo 89-*bis* la scriminante non opera per i crimini di genocidio, crimini contro l'umanità, crimini di guerra, e crimini di aggressione, previsti dagli articoli 5 e seguenti dello Statuto della Corte penale internazionale.

Relazioni al Parlamento nel campo della sicurezza cibernetica

Interviene, invece sugli articoli 12 e 536 del Codice dell'ordinamento militare il successivo articolo 8.

Nello specifico la novella all'articolo 12 è volta ad integrare il contenuto della relazione che Il Ministro della difesa è tenuto a presentare al Parlamento in sede di presentazione annuale dello stato di previsione del Ministero al fine di inserirvi anche una parte dedicata **all'evoluzione e alle prospettive della minaccia cibernetica alla sicurezza nazionale.**

In relazione alla disposizione in esame si ricorda che allo stato (cfr.quadro normativo), ai sensi dell'articolo 38 della legge n. 124 del 2007 entro il mese di febbraio di ogni anno il Governo trasmette al Parlamento una relazione scritta, riferita all'anno precedente, sulla politica dell'informazione per la sicurezza e sui risultati ottenuti. Alla relazione di cui al comma 1 è allegato il documento di sicurezza nazionale, concernente le attività relative alla protezione delle infrastrutture critiche materiali e immateriali nonché alla protezione cibernetica e alla sicurezza informatica.

Per quanto concerne, invece, la novella all'articolo 536 del Codice che attualmente disciplina la pianificazione dei programmi di ammodernamento e rinnovamento dei sistemi d'arma, delle opere, dei mezzi e dei beni direttamente destinati alla difesa nazionale, la modifica proposta è volta ad integrare il contenuto del documento programmatico che annualmente, entro la data del 30 aprile, il Ministro della Difesa è tenuto a trasmettere al Parlamento con **l'indicazione dei programmi concernenti la sicurezza cibernetica.**

Disposizioni concernenti l'organizzazione del Sistema nazionale di sicurezza cibernetica (articoli da 9 a 16)

Gli articoli da 9 a 16 della proposta di legge delineano il nuovo assetto istituzionale in materia di protezione cibernetica individuando i diversi soggetti con competenze in tale ambito ed i relativi compiti.

Al riguardo gli organi richiamati dall'articolo 9 della proposta di legge sono il Presidente del Consiglio dei ministri, il Comitato interministeriale per la sicurezza della Repubblica (CISR), il Dipartimento delle informazioni per la sicurezza (DIS), il Nucleo per la sicurezza cibernetica (NSC), il Comando interforze operativo cibernetico (CIOC), il CERT nazionale, il CERT-PA, il CERT-Difesa, il Centro nazionale anticrimine informatico per la protezione delle infrastrutture strategiche (CNAIPIC) e l'Istituto superiore delle comunicazioni e delle tecnologie dell'informazione ('ISCOM).

Si tratta di organismi pertanto di organismi già operativi nell'ambito della protezione cibernetica e regolamentati da precise disposizioni normative, con la sola eccezione del Comando interforze operativo cibernetico (CIOC) in via di implementazione le cui caratteristiche fondamentali sono state illustrate dal Capo di Stato maggiore della Difesa, Generale Claudio Graziano, nel corso di una sua audizione presso la Commissione difesa della Camera lo scorso 25 gennaio.

Il resoconto stenografico della seduta della Commissione difesa della Camera dei deputati del 25 gennaio 2017, è consultabile al seguente link : http://www.camera.it/leg17/1079?idLegislatura=17&tipologia=indag&sottotipologia=c04_cibernetico&anno=2017&mese=01&giorno=25&idCommissione=04&numero=0009&fil
L'istituzione di un Comando interforze per le Operazioni cibernetiche (CIOC), (CIOC) è previsto anche dal Libro Bianco per la sicurezza internazionale e la difesa (punto 173) e dal *Piano nazionale per la sicurezza dello spazio cibernetico 2017.*

Attribuzioni del

In particolare, nel nuovo assetto delineato dalla proposta di legge in esame al

Presidente del Consiglio dei ministri

Presidente del Consiglio dei ministri spetta il compito di coordinare le politiche dell'informazione per la sicurezza e di impartire le direttive e, sentito il CISR, emanare ogni disposizione necessaria per l'organizzazione e per il funzionamento del sistema nazionale di sicurezza cibernetica.

Al Presidente del Consiglio dei ministri viene, inoltre, conferito il potere di nominare e revocare il direttore del NSC, sentito il CISR. Ai sensi del successivo articolo 13 l'incarico ha durata biennale e deve essere conferito ad a un soggetto dotato di adeguata qualificazione, appartenente al DIS, al Ministero della difesa, al Ministero dell'interno o al Ministero dello sviluppo economico.

Spetta sempre al Presidente del Consiglio dei ministri il compito di determinare, di concerto con i Ministri dell'economia e delle finanze, dell'interno e della difesa, l'ammontare annuo delle risorse finanziarie destinate all'attività del sistema nazionale di sicurezza cibernetica a valere sul Fondo di cui all'articolo 20 della proposta di legge.

Come precedentemente rilevato (cfr. quadro normativo) ai sensi del DPCM del 17 febbraio 2017 il Presidente del Consiglio dei ministri è il soggetto responsabile della politica generale del Governo e vertice del Sistema di informazione per la sicurezza della Repubblica. Assume le decisioni in caso di situazioni di crisi che coinvolgano aspetti di sicurezza nazionale, provvedendo, nelle situazioni di crisi che coinvolgono aspetti di sicurezza nazionale, a convocare il CISR. Adotta, curandone l'aggiornamento, su proposta del CISR, il *Quadro strategico nazionale per la sicurezza dello spazio cibernetico* e il *Piano nazionale per la sicurezza dello spazio cibernetico, e*mana le direttive ed ogni atto d'indirizzo necessari per l'attuazione del Piano ed impartisce, sentito il CISR, le direttive al DIS e alle Agenzie.
Per quanto concerne la nomina del direttore del NISC attualmente il Nucleo è presieduto da un vice direttore generale del DIS, designato dal direttore generale (comma 2 dell'articolo 8 del DPCM del 17 febbraio 2017).

Delega di funzioni all'Autorità delegata

Ai sensi dell'articolo 11 della proposta di legge il Presidente del Consiglio dei ministri, ove lo ritenga opportuno, può delegare le funzioni che non sono ad esso attribuite in via esclusiva a un Ministro senza portafoglio o a un Sottosegretario di Stato.

Nomina del direttore del DACI

Spetta, invece al Ministro degli affari esteri e della cooperazione internazionale il compito di nominare, sentita l'AISE, il **Direttore per l'analisi cibernetica internazionale** (DACI), con il compito di fornire ai competenti organi politici un'analisi geopolitica complessiva rispetto agli eventi cibernetici. L'AISE collabora con il DACI per l'analisi degli eventi cibernetici pertinenti agli interessi italiani all'estero (Art. 12)

Istituzione di un sistema di sistema InfoSharing unico

Per quanto concerne, invece, le competenze del il CERT nazionale ai sensi dell'articolo 14 della proposta di legge tale organismo è tenuto ad attivare un **sistema di** *InfoSharing* unico che consenta di memorizzare dati con distinte autorizzazioni all'accesso in relazione al livello di segretezza del dato inserito, nel rispetto delle disposizioni della legge 3 agosto 2007, n. 124.

Classifiche di sicurezza di documenti

Al riguardo, si ricorda che le **classifiche di sicurezza** vengono attribuite per circoscrivere la conoscenza di informazioni e di qualsiasi altro dato ai soli soggetti che vi possono accedere in ragione delle proprie funzioni istituzionali.
La **tutela amministrativa del segreto** (che è fattispecie distinta dalla tutela processuale del segreto di Stato), consiste nella apposizione del segreto e nella conferma dell'opposizione ed è disciplinata principalmente dalla legge di riforma dei servizi di informazione, L. 124/2007, sul punto modificata dal D.L. 78/2009 (art. 24, co. 73), e dal DPCM 12 giugno 2009.
In sintesi, per tutela amministrativa del segreto si intende l'insieme delle attività volte a garantire in via ordinaria la segretezza delle informazioni e dei documenti la cui conoscenza potrebbe nuocere alla sicurezza della Repubblica. Tra questi strumenti ha un ruolo rilevante il **nulla osta di sicurezza o NOS**. Si tratta di una speciale abilitazione che autorizza il ministero, l'ente o l'impresa richiedente ad avvalersi di una persona in attività che comportano la trattazione di informazioni classificate (art. 9, L. 124/2007).
Competente al rilascio del NOS è l'**Ufficio centrale per la segretezza (UCSe)** istituito nell'ambito del **Dipartimento delle informazioni per la sicurezza (DIS)**. L'UCSe procede all'accertamento dell'idoneità di ciascun soggetto all'attribuzione del NOS.
La competenza relativa all'attribuzione a ciascun documento o informazione della corrispondente **classifica di sicurezza** spetta all'autorità che forma o che acquisisce il documento o che ne ha la disponibilità (art. 42, comma 2, L. 124/2007). Le classifiche sono quattro: segretissimo, segreto, riservatissimo e riservato (art. 42, comma 3, L. 124/2007).
A ciascuna classifica di segretezza corrisponde un distinto livello di NOS, ad eccezione della classifica più bassa, quella di riservato, per la quale è non necessario il nulla osta per il rilascio.
Chi appone la classifica di segretezza individua, all'interno di ogni atto o documento, le parti che devono essere classificate e fissa specificamente il grado di classifica corrispondente ad ogni singola parte.
La classifica di segretezza è automaticamente declassificata a livello inferiore quando sono trascorsi cinque anni dalla data di apposizione; decorso un ulteriore periodo di cinque anni, cessa comunque ogni vincolo di classifica. La **declassificazione automatica** non si applica quando, con provvedimento motivato, i termini di efficacia del vincolo

sono prorogati dal soggetto che ha proceduto alla classifica o, nel caso di proroga oltre il termine di quindici anni, dal Presidente del Consiglio dei ministri (art. 42, commi 5 e 6 L. 124/2007)..
Il Presidente del Consiglio verifica il rispetto delle norme in materia di classifiche di segretezza (art. 42, comma 7, L. 124/2007).
Con il DPCM 12 giugno 2009 sono stati determinati l'ambito dei singoli livelli di segretezza, i soggetti cui è conferito il potere di classifica e gli uffici che, nell'ambito della pubblica amministrazione, sono collegati all'esercizio delle funzioni di informazione per la sicurezza della Repubblica, nonché i criteri per l'individuazione delle materie oggetto di classifica e i modi di accesso nei luoghi militari o in quelli definiti di interesse per la sicurezza della Repubblica.
Al DIS spetta il compito di attuare tali disposizioni, oltre che a vigilare sulla loro applicazione (art. 4, comma 3, lett. *l)*, L. 124/2007).

Secondo quanto previsto sempre dall'articolo 14 della proposta di legge spetta sempre al CERT nazionale definire il sistema di accesso e il mantenimento del sistema di *InfoSharing* unico. La definizione delle caratteristiche tecniche relative alla conservazione e all'accesso alle informazioni classificate è a sua volta effettuata d'intesa con il CNAIPIC, il CERT-Difesa e il DIS.

Il ***CERT nazionale*** è una struttura individuata dall'articolo 16 - bis del D.Lgs. n. 259 del 2003, recante il Codice delle Comunicazioni elettroniche. Si tratta di una struttura destinata a potenziare i meccanismi di risposta agli incidenti informatici e gli strumenti di rilevazione e contrasto alle minacce. Il CERT nazionale ha avviato le sue attività a partire dal 5 giugno 2014. Il CERT nazionale opera a supporto di cittadini ed imprese con l'obiettivo di incrementare la consapevolezza e la cultura della sicurezza nell'utilizzo di servizi on line, fornendo informazioni tempestive su potenziali minacce informatiche, raccomandazioni e consigli utili per la prevenzione, contromisure per la risoluzione di incidenti informatici con impatto significativo (www.certnazionale.it). Il CERT opera sulla base di un modello cooperativo pubblico-privato. Il CERT nazionale ha avviato, infatti, la collaborazione con imprese che gestiscono infrastrutture informatizzate. Sulla base di tale collaborazione è stato istituito un Tavolo tecnico permanente per garantire un confronto costante tra i principali attori coinvolti e quindi migliorare e velocizzare le azioni di risposta ad eventuali incidenti informatici. il CERT nazionale ha, altresì, avviato una stretta collaborazione con il **CERT-PA** (CERT delle Pubbliche Amministrazioni che opera all'interno dell'Agenzia per l'Italia Digitale), ***CERT Difesa e CNAIPIC*** (Centro nazionale anticrimine informatico per la protezione delle infrastrutture critiche che opera nell'ambito del Servizio di polizia postale e delle comunicazioni). In ambito internazionale, il CERT nazionale ha già avviato forme di dialogo con CERT europei, extra-europei e con il CERT EU (CERT dell'Unione Europea sostenuto dall'Agenzia europea per la sicurezza ENISA).

Compiti del CNAIPC

Per quanto concerne, invece, l'esercizio delle funzioni di pubblica sicurezza nell'ambito del nuovo sistema nazionale di sicurezza cibernetico, tale potere viene riconosciuto dall'articolo 15 della proposta di legge in capo al **Centro nazionale anticrimine informatico per la protezione delle infrastrutture strategiche** (CNAIPC), in coordinamento con il con il Cert nazionale.

In particolare spetta al CNAIPC, entro sei mesi dalla data di entrata in vigore della legge, definire l'elenco delle infrastrutture strategiche e fornire le Linee guida per l'eventuale integrazione del medesimo. In via permanente il CNAIPC provvede, in presenza di un evento cibernetico di gravità tale da poter evolvere in una crisi cibernetica nazionale, a disporre, su richiesta del Presidente del Consiglio dei ministri o dell'Autorità delegata l 'interruzione dei pubblici servizi. Provvede, inoltre, alla condivisione con gli altri soggetti del sistema nazionale di sicurezza cibernetica delle notizie necessarie alla risoluzione della crisi cibernetica o dell'evento cibernetico potendo a tal fine provvedere nel più breve tempo possibile alla rimozione dei dati e degli elementi classificati.

In relazione alla possibilità per il CNAIPC di procedere "nel più breve nel più breve tempo possibile alla rimozione dei dati e degli elementi classificati allo scopo di condividere con gli altri soggetti del sistema nazionale di sicurezza cibernetica le notizie necessarie alla risoluzione della crisi cibernetica o dell'evento cibernetico" andrebbe valutata l'opportunità di specificare meglio il contenuto di tale attività anche in relazione alla sopra richiamata normativa riguardante la gestione di dati classificati espressamente richiamata anche dal successivo articolo 17 della proposta di legge.

Sempre con riferimento al nuovo assetto strategico in materia di sicurezza cibernetica l'articolo 16 della proposta di legge delinea le caratteristiche essenziali del nuovo Comando operativo cibernetico (CIOC), istituito nell'ambito dello Stato maggiore della difesa e posto alle dipendenze del Ministro della difesa che, con proprio decreto, da adottare entro quattro mesi dalla data di entrata in vigore della legge, ne definirà le attribuzioni, la struttura e l'organizzazione.

Il CIOC viene identificato dalla proposta di legge in esame quale organismo

istituzionalmente deputato ad operare nel settore della sicurezza militare, in coordinamento con il DIS e il RIS. Al CIOC spetta la direzione delle soprarichiamate operazioni relative alle contromisure cibernetiche previste dall'articolo 89-*bis* (cfr. sopra, articolo 7).

Collocazione del CERT

Spetta, a sua volta al **CERT difesa** organizzare il sistema di protezione dei sistemi cibernetici delle Forze armate ed esercitare le funzioni di punto di riferimento nazionale per i rapporti con le organizzazioni internazionali e con altri Stati, nell'ambito della sicurezza cibernetica nel settore militare.

Da un punto di vista organizzativo il Il CERT-Difesa viene collocato alle dipendenze del CIOC con la finalità di fornire informazioni sugli eventi cibernetici nel settore cibernetico militare. A tal fine con decreto del Ministro della difesa, da adottare entro sei mesi dalla data di entrata in vigore della presente legge, è definita l'organizzazione del CERT-Difesa nell'ambito del CIOC.

Disposizioni in materia trattamento e gestione di dati classificati (articoli da 17 e 18)

Trattamento dei dati classificati

L'articolo 17 individua i soggetti istituzionalmente competenti a **trattare dati classificat**i.

Al riguardo, fermo restando il principio generale in forza del quale Il DIS esercita la gestione e il trattamento dei dati classificati nel settore della sicurezza cibernetica con gli strumenti e secondo le modalità e le procedure stabiliti dalla legge 3 agosto 2007, n. 124, si prevede altresì che il CERT-Difesa e il CNAIPIC collaborino con il DIS per il trattamento dei dati classificati nel campo della sicurezza cibernetica.

Come precedentemente rilevato in base all'articolo 4 della legge 124 del 2007 il DIS assicura l'attuazione delle disposizioni impartite dal Presidente del Consiglio dei Ministri con apposito regolamento ai fini della tutela amministrativa del segreto di Stato e delle classifiche di segretezza, vigilando altresì sulla loro corretta applicazione.

In particolare, il CNAIPIC , entro sei mesi dalla data di entrata in vigore della legge, d'intesa con il DIS e con il CERT nazionale, dovrà definire le linee guida per la presa in carico e la gestione degli eventi cibernetici classificati e per la pubblicazione, mediante la piattaforma *InfoSharing*, delle informazioni utili a ridurre l'eventuale crisi cibernetica o la sua propagazione. Le linee guida dovranno prevedere la presa in carico delle informazioni da parte del CNAIPIC per la valutazione della necessità di pubblicazione delle stesse, previa rimozione dei dati e degli elementi classificati, Tale operazione dovrà essere effettuata nel termine di tre ore dall'acquisizione dell'informazione. Qualora il CNAIPIC non abbia proceduto alla pubblicazione delle informazioni, il NSC, il CERT nazionale e il CERT-PA potranno reiterare la richiesta ai fini della presa in carico e della gestione dell'evento cibernetico, qualora ritengano che ne perduri la necessità.

Controllo parlamentare, disposizioni finanziarie e finali (articoli da 19 e 23)

Controllo parlamentare sugli schemi di decreto previsti dalla proposta di legge in esame

L'articolo 19 fissa il principio generale in forza del quale tutti gli schemi di decreto da adottarsi ai sensi della proposta di legge in esame (cfr, articoli 16, 20 e 22) devono essere sottoposti al **previo parere** delle Commissioni parlamentari competenti per materia, con le modalità e nelle forme stabilite dai rispettivi Regolamenti. Il termine per l'espressione del parere è di trenta giorni dalla richiesta. Ove tale termine decorra senza che le Commissioni si siano pronunciate, i decreti potranno essere comunque emanati. Analoga procedura è prevista per l'esame parlamentare delle Linee guida comuni.

Istituzione del Fondo per la

A sua volta l'articolo 20 prevede l'istituzione nello stato di previsione del Ministero dell'economia e delle finanze, per il successivo trasferimento al bilancio autonomo della Presidenza del Consiglio dei ministri, del **Fondo per la sicurezza cibernetica**. Spetta al Presidente del Consiglio dei ministri, con decreto da emanare entro

sicurezza cibernetica

sessanta giorni dalla data di entrata in vigore della presente legge, adottato di concerto con il Ministro della difesa, dello sviluppo economico, dell'interno e dell'economia e delle finanze, definire le modalità di impiego delle somme del fondo. Per quanto concerne la copertura finanziaria, il successivo articolo 21 prevede la riduzione del fondo di cui all'articolo 1, comma 965, della legge 28 dicembre 2015, n. 208.

Al riguardo, si ricorda che la legge di stabilità per l'anno 2016 ha istituito nello stato di previsione del Ministero dell'economia e delle finanze un fondo con una dotazione finanziaria di 150 milioni di euro per l'anno 2016 per il potenziamento degli interventi e delle dotazioni strumentali in materia di protezione cibernetica e di sicurezza informatica nazionali nonché per le spese correnti connesse ai suddetti interventi. Si è previsto che un decimo della dotazione finanziaria del fondo è destinato al rafforzamento della formazione del personale del servizio polizia postale e delle comunicazioni, nonché all'aggiornamento della tecnologia dei macchinari e delle postazioni informatiche.

Da ultimo l'articolo 22 autorizza il governo a modificare il DPCM del 24 gennaio del 2013 che, com'è noto è stato integralmente abrogato dal recente DPCM del 17 febbraio 2017, mentre l'articolo 23 concerne l'entrata in vigore del provvedimento prevista per il sessantesimi giorno successivo a quello della pubblicazione della legge nella Gazzetta Ufficiale.

Relazioni allegate o richieste

Trattandosi di una proposta di legge di iniziativa parlamentare alla medesima è allegata unicamente la relazione illustrativa.

Necessità dell'intervento con legge

La proposta di legge in esame reca disposizioni concernenti la difesa e la sicurezza dello spazio cibernetico. A tal fine, nel prevedere l'istituzione di un apposito "Sistema nazinale di sicurezza cibernetica", la proposta di legge interviene sia sulle competenze attualmente previste dal d.lgs. n. 60 del 2010 in capo alle forze armate, sia sulle attribuzioni del Presidente del Consiglio e degli organismi di informazione e sicurezza.
Si comprende, pertanto, l'intervento normativo con una fornte di rango primario.

Rispetto delle competenze legislative costituzionalmente definite

Le disposizioni contenute nella proposta di legge possono essere ricondotte alle materie «difesa», «sicurezza dello Stato», «ordine pubblico e sicurezza», ai sensi dell'articolo 117, secondo comma, lettera d) e h), della Costituzione.

Per costante giurisprudenza della Corte costituzionale, la materia «ordine pubblico e sicurezza», di competenza legislativa statale esclusiva (art. 117, secondo comma, lettera h, Cost.) si riferisce «all'adozione delle misure relative alla prevenzione dei reati ed al mantenimento dell'ordine pubblico, inteso quest'ultimo quale complesso dei beni giuridici fondamentali e degli interessi pubblici primari sui quali si regge l'ordinata e civile convivenza nella comunità nazionale» (*ex plurimis*, **sentenza n. 35 del 2011, n. 118 del 2013, n. 33 del 2015**).