CAMERA DEI DEPUTATI

N. **3677**

PROPOSTA DI LEGGE

d'iniziativa del deputato ARTINI

Norme in materia di difesa dello spazio cibernetico e istituzione del sistema nazionale di sicurezza cibernetica

Presentata il 15 marzo 2016

ONOREVOLI COLLEGHI ! — Che il cyberspazio sia ormai un dominio non meno reale di quelli terrestre, marittimo, aereo e spaziale è cosa risaputa. La breve storia della *cyber warfare* non manca di esempi eclatanti. Basti ricordare l'attacco ai siti governativi georgiani durante il conflitto con la Russia nel 2008; il virus Stuxnet impiegato per sabotare le centrifughe di arricchimento dell'uranio dell'impianto iraniano di Natanz nel 2010; la diffusione, nel 2012, del *malware Red October*, che avrebbe portato alla sottrazione di informazioni da ambasciate, centri di sviluppo, installazioni militari, società del settore energetico e infrastrutture strategiche di vario genere in Russia e in molti altri Paesi, soprattutto dell'ex Unione Sovietica. Nel 2014 la sola rete informatica del Governo degli Stati Uniti d'America (USA), certamente una delle più sicure, ha subìto ben 61.000 violazioni della sicurezza, tra cui l'attacco al sistema di posta elettronica del Dipartimento di Stato e della Casa Bianca, con migliaia di messaggi intercettati, compresi alcuni inviati dal Presidente Obama ai suoi collaboratori. Il 2015 si è rivelato ancora peggiore per gli USA: il 5 giugno e il 10 luglio, in due attacchi per i quali Washington ha puntato il dito verso la Cina, dai *database* dell'*Office of Personnel Management* sono stati trafugati i dati personali rispettivamente di 18 milioni di impiegati federali e di 22 milioni di cittadini che avevano presentato domanda di assunzione. In Europa sono i Paesi dell'est i più colpiti, oggetto di un'estesa campagna di *cyber warfare* della Russia focalizzata soprattutto contro l'Ucraina – che ha visto crescere esponenzialmente gli attacchi condotti dalla Russia alle proprie reti informatiche della Difesa e delle Forze di polizia – ma che ha già coinvolto anche Georgia, Estonia, Polonia, Romania e Germania.

A livello globale, secondo quanto riportato nell'edizione 2015 del rapporto del-

l'Associazione italiana per la sicurezza informatica (CLUSIT), lo scorso anno gli attacchi cibernetici di *information warfare* in supporto ad attività militari, paramilitari e terroristiche hanno visto un incremento del 68 per cento, attestandosi al 5 per cento del totale, mentre le violazioni classificate sotto la voce « spionaggio » sono aumentate del 2,99 per cento, raggiungendo la quota dell'8 per cento. Per contro, risulta in netto calo (-14,8 per cento) il cosiddetto *hacktivism*, ovvero gli attacchi, per lo più dimostrativi, condotti per attivismo politico, che si attestano al 27 per cento del totale. La quota più grande è ancora occupata dal crimine informatico (60 per cento), ma la minaccia maggiore, almeno per quanto riguarda la sicurezza nazionale, deriva sicuramente dalla sempre più ampia diffusione di capacità avanzate di *cyber warfare*, quella che nel rapporto della CLUSIT viene indicata come una « selvaggia corsa ai *cyber* armamenti » le cui possibili conseguenze non riguardano solo le cosiddette infrastrutture strategiche, ma anche una quantità crescente di servizi erogati da aziende private e da pubbliche amministrazioni che, se resi indisponibili a seguito di un attacco, creerebbero enormi disagi alla popolazione e, in certi scenari, anche perdite di vite umane.

All'esigenza di proteggere le reti informatiche nazionali si somma, dunque, quella di prevenire la proliferazione delle armi cibernetiche. A questo proposito appare emblematico il caso dell'attacco informatico subìto il 6 luglio 2015 dalla società italiana Hacking Team, che si è vista sottrarre 400 gigabyte di dati, tra cui documenti fiscali e amministrativi, comunicazioni interne e, soprattutto, il codice sorgente del *software* RCS (*remote control software*) Galileo, uno dei principali strumenti di *intelligence* a disposizione delle Forze di polizia e dei servizi segreti italiani. Il furto non solo ha costretto gli utenti del *software* spia a sospenderne immediatamente l'impiego, ma potrebbe anche aver portato nelle mani sbagliate un potente strumento di guerra cibernetica. Inoltre, poiché gran parte del materiale copiato è stata pubblicata nel *web*, si sono rapidamente diffusi degli antivirus in grado di individuare la presenza della versione di Galileo impiegata fino al 6 luglio, di fatto permettendo a chiunque, terroristi e criminali compresi, di sapere se era sorvegliato.

L'Unione europea ha provato a opporre un ostacolo alla diffusione delle armi cibernetiche con il regolamento delegato (UE) n. 1382/2014 della Commissione, del 22 ottobre 2014, entrato in vigore il 30 dicembre 2014, che aggiorna la lista dei materiali ad uso duale soggetti ad autorizzazione all'esportazione, includendovi i *software* di intrusione. Grazie a questa norma, le imprese europee devono ottenere un'autorizzazione governativa per vendere i propri prodotti fuori dell'Unione europea. Tuttavia, non bisogna aspettarsi che vi sia una volontà reale degli Stati di collaborare sul fronte cibernetico il quale, anzi, vede spesso azioni di spionaggio informatico condotte nei confronti di Paesi che formalmente sono alleati, ma di fatto sono rivali dal punto di vista economico o politico. In effetti, ogni Stato intende mantenere la completa sovranità sul proprio « territorio digitale ». Il fronte cibernetico, dunque, assomiglia sempre di più a una giungla dove solo i più forti sopravvivono.

Per un Paese come l'Italia, dove certamente non mancano bersagli d'interesse per attacchi cibernetici, è dunque fondamentale l'avvio di un programma di potenziamento quanto meno delle proprie capacità di difesa cibernetica. L'attivazione dei vari *computer emergency response team* (CERT), tra i quali il CERT-Difesa e il CERT nazionale, rappresenta un passo importante ma non sufficiente, soprattutto se paragonato a quanto stanno facendo altri Paesi. Nel 2014 il Governo britannico ha lanciato un programma del valore di 800 milioni di sterline (oltre un miliardo di euro) per il potenziamento delle capacità di difesa cibernetica delle Forze armate britanniche; la Francia ha stanziato circa un miliardo e mezzo di euro allo stesso scopo, senza contare gli investimenti degli USA, della Russia e della Cina, tutte potenze che si sono dotate di grandi strutture destinate espressamente a tale fine, comprendenti vari comandi e reparti specializzati in

guerra cibernetica. In Italia, con il decreto del Presidente del Consiglio dei ministri 24 gennaio 2013, pubblicato nella *Gazzetta Ufficiale* n. 66 del 19 marzo 2013, è stata emanata la direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionale, ma purtroppo il medesimo decreto prevede che dallo stesso « non derivano nuovi oneri a carico del bilancio dello Stato ». Restare indietro in questo settore significa esporre il Paese a rischi gravissimi.

Con la presente proposta di legge, che ripropone parzialmente il contenuto della proposta di legge n. 3544 allo scopo di concentrare l'attenzione su alcuni aspetti nodali, s'intende compiere un ulteriore fondamentale passo avanti rispetto al decreto del Presidente del Consiglio dei ministri 27 gennaio 2014, che ha adottato il Quadro strategico nazionale per la sicurezza dello spazio cibernetico e il Piano nazionale per la protezione cibernetica e la sicurezza informatica del dicembre 2013, quale strategia nazionale per la sicurezza cibernetica. Lo scopo è di istituire il sistema nazionale di sicurezza cibernetica tramite un'ottimale ripartizione delle responsabilità e delle competenze tra i vari enti interessati e una riarticolazione della struttura gerarchico-funzionale allo scopo di consentire, anche attraverso un sistematico scambio di informazioni e la piena sinergia tra gli enti, una maggiore e più capillare capacità di difesa cibernetica, pur garantendo la salvaguardia delle esigenze di riservatezza necessarie alla tutela della sicurezza nazionale.

La presente proposta di legge disciplina le competenze della difesa cibernetica e definisce come evento di interesse militare ogni attacco volto a minacciare il funzionamento e l'integrità della rete informatica e delle infrastrutture informatizzate critiche d'interesse nazionale. Essa tende inoltre al ripristino della sovranità nazionale sul mondo cibernetico, alla formazione degli operatori e alla diffusione della cultura della difesa cibernetica. Uno degli obiettivi è la disciplina delle contromisure cibernetiche.

In primo luogo vengono definiti gli ambiti e i soggetti che sono interessati dalla legge, indicando sia i princìpi ispiratori, sia gli ambiti di azione dell'atto normativo, sia gli organi direttamente coinvolti nella gestione della sicurezza cibernetica (articoli 1, 2 e 3).

Si definiscono poi le competenze del Segretario generale della difesa – Direttore nazionale degli armamenti (articolo 4) e si enunziano i princìpi relativi alla formazione del personale militare (articolo 5), volti ad assicurare la piena valorizzazione delle competenze e a favorire la crescita professionale, la formazione permanente e la specializzazione del personale militare a ogni livello nel settore della sicurezza cibernetica. A questo fine si prevede altresì che siano apportate le opportune modificazioni al codice dell'ordinamento militare, di cui al decreto legislativo 15 marzo 2010, n. 676, e al correlato testo unico delle disposizioni regolamentari in materia di ordinamento militare, di cui al decreto del Presidente della Repubblica 15 marzo 2010, n. 90.

Sono altresì indicate le attribuzioni spettanti nella materia al Ministro della difesa (articolo 6), tra cui in particolare l'emanazione delle direttive di sua competenza relativamente alla protezione dello spazio cibernetico e alla risposta ad attacchi cibernetici. Con opportune integrazioni della disciplina contenuta nel citato codice dell'ordinamento militare sono ampliate le competenze delle Forze armate ed è introdotta la possibilità di agire con contromisure cibernetiche (articoli 7 e 8), la cui attuazione spetta, sul piano operativo, alle Forze armate. Alle medesime è consentito di realizzare programmi informatici che permettano la verifica del funzionamento e dell'efficacia dei sistemi di difesa cibernetica nazionali.

L'uso delle contromisure è deliberato al massimo livello politico dal Consiglio dei ministri ed è comunicato al Presidente della Repubblica e al Comitato parlamentare per la sicurezza della Repubblica. Agli operatori che attuano le contromisure deliberate sono riconosciute le garanzie funzionali previste dall'articolo 17 della legge 3

agosto 2007, n. 124. Le garanzie funzionali non si applicano nei casi di violazioni che integrino le fattispecie previste dagli articoli 5 e seguenti del trattato istitutivo della Corte penale internazionale, come, ad esempio, il crimine di genocidio, crimini contro l'umanità, crimini di guerra o crimine di aggressione.

Il capo II del titolo II delinea il sistema nazionale di sicurezza cibernetica. Come per il sistema nazionale di sicurezza della Repubblica, definito dalla citata legge n. 124 del 2007, ci si pone l'obiettivo (anche tramite la definizione di una possibile autorità politica delegata nell'ambito della Presidenza del Consiglio dei ministri) di conferire autonomia di operatività e di gestione funzionale a tutto l'ambito della sicurezza cibernetica, definendo una serie di ruoli e di organi (strategici e tattici) che compongono il sistema nazionale di sicurezza cibernetica (articolo 9).

La proposta di legge – alla stregua di altri sistemi nazionali di Stati europei e non europei e in conformità a quanto già previsto nel decreto del Presidente del Consiglio dei ministri 24 gennaio 2013, pubblicato nella *Gazzetta Ufficiale* n. 66 del 19 marzo 2013 – conferisce in via prioritaria al Presidente del Consiglio dei ministri una serie di attribuzioni sulla sicurezza cibernetica, che gli riservano i poteri di decisione politica, su proposta del Comitato interministeriale per la sicurezza della Repubblica (CISR), relativamente agli organi e alle scelte strategiche in materia di cibernetica, in caso di crisi, ovvero gli consentono di nominare un'autorità delegata responsabile esclusivamente dell'ambito cibernetico (articoli 10 e 11).

Si interviene inoltre sulla disciplina del Nucleo per la sicurezza cibernetica (NSC), presieduto da un direttore, non più identificato nel consigliere militare del Presidente del Consiglio dei ministri (come previsto dal citato decreto del Presidente del Consiglio dei ministri 24 gennaio 2013), che costituisce la cabina di regìa in caso di crisi o evento cibernetico (articolo 13). Il direttore del NSC è nominato dal Presidente del Consiglio dei ministri con incarico di durata biennale da conferire, a scelta e secondo un implicito criterio di rotazione, tra personale qualificato appartenente al DIS, al Ministero dell'interno, al Ministero della difesa e al Ministero dello sviluppo economico.

Vengono rimodulate le competenze del CERT nazionale, del Centro nazionale anticrimine informatico per la protezione delle infrastrutture strategiche (CNAIPIC) e del CERT-Difesa (articoli 14, 15 e 16). Per ognuno di essi sono definiti la catena di comando, ossia la dipendenza funzionale, il compito istituzionale che deve svolgere e le disposizioni attuative di sua competenza, che devono essere adottate entro sei mesi dalla data di entrata in vigore della legge. Viene altresì istituito il Comando interforze operativo cibernetico (CIOC), i cui compiti e organizzazione sono definiti dal Ministro della difesa. Da esso dipende il CERT-Difesa.

La competenza per la trattazione di eventi cibernetici classificati e la gestione dei dati classificati è assegnata al Dipartimento delle informazioni per la sicurezza (DIS) in coordinamento con il CNAIPIC e il CERT-Difesa (articolo 17) ed è assistita dalla creazione di uno snodo telematico (*cyber-gateway*) che possa acquisire dati classificati e possa trattarli al fine di rendere disponibili le informazioni relative all'evento cibernetico e alla sua soluzione (articolo 18). Il gestore dello snodo disporrà di termini minimo e massimo per la presa in carico e la trattazione dei dati, che dovrà depurare degli elementi soggetti a classifiche di segretezza, così da garantire agli altri organi che non possono ricevere informazioni classificate una tempestiva possibilità di raccolta delle informazioni necessarie per proteggersi o debellare un attacco cibernetico.

Data l'estrema sensibilità della materia (anche per il possibile controllo sui dati personali dei cittadini), la proposta di legge prevede il controllo parlamentare sull'attuazione delle misure previste. In particolare ogni schema di decreto o linee guida indicato nella proposta di legge deve essere sottoposto al parere delle competenti Commissioni parlamentari. Il parere non è vincolante, ma consente al Parlamento di ve-

rificare ciascun provvedimento di attuazione (articolo 19). Il Comitato parlamentare per la sicurezza della Repubblica deve essere informato in caso di uso di contromisure cibernetiche (articolo 89-*bis*, comma 3, del codice dell'ordinamento militare, di cui al decreto legislativo 15 marzo 2010, n. 66, introdotto dall'articolo 7 della presente proposta di legge).

Oltre alle disposizioni sul controllo parlamentare, nel titolo III sono altresì contenute le disposizioni finanziarie volte ad apprestare i fondi necessari per sostenere l'attuazione della legge.

Il Fondo per la sicurezza cibernetica, regolato da un decreto del Presidente del Consiglio dei ministri, da adottare di concerto con i Ministri della difesa, dello sviluppo economico, dell'interno e dell'economia e delle finanze, è istituito nello stato di previsione del Ministero dell'economia e delle finanze per poi essere iscritto nel bilancio autonomo della Presidenza del Consiglio dei ministri (articolo 20). Tale fondo provvede il finanziamento di tutte le disposizioni della proposta di legge che comportano oneri finanziari a regime, nonché delle conseguenti attività.

L'articolo 21 indica la copertura finanziaria degli oneri derivanti dalla legge, per la quale è impiegato l'apposito fondo istituito dalla legge di stabilità 2016.

Dalle nuove disposizioni introdotte discende la necessità di adeguamento del decreto del Presidente del Consiglio dei ministri 24 gennaio 2013, così da evitare sovrapposizioni normative o eventuali conflitti in fase di applicazione delle norme. A questo fine, l'articolo 22 conferisce espressa autorizzazione al Governo. L'articolo 23 regola l'entrata in vigore della disciplina introdotta.

PROPOSTA DI LEGGE

—

TITOLO I

PRINCÌPI, FINALITÀ E DEFINIZIONI

ART. 1.

(Princìpi generali e finalità).

1. Le competenze relative alla disciplina e all'organizzazione della difesa dello spazio cibernetico spettano allo Stato ai sensi dell'articolo 117, secondo comma, lettere *d)* e *h)*, della Costituzione. Lo Stato esercita le funzioni ad esse relative e adotta le disposizioni che devono essere osservate dai soggetti pubblici e privati, stabilendo i livelli di protezione necessari per l'attuazione del compito prioritario della sicurezza delle infrastrutture e dei dati di interesse nazionale.

2. 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.

3. La presente legge disciplina altresì:

a) l'istituzione e l'organizzazione del sistema nazionale di sicurezza cibernetica;

b) la deliberazione e l'attuazione delle contromisure cibernetiche.

ART. 2.

(Definizioni).

1. Ai fini della presente legge si intende per:

a) « spazio cibernetico »: l'insieme delle infrastrutture informatiche interconnesse, comprendente *hardware, software*, dati e utenti, nonché delle relazioni logiche, comunque stabilite, tra essi;

b) « sicurezza cibernetica »: la condizione per la quale lo spazio cibernetico risulta protetto mediante l'adozione di ido-

nee misure di sicurezza fisica, logica e procedurale rispetto a eventi, di natura volontaria o accidentale, consistenti nell'acquisizione o nel trasferimento indebiti di dati, nella loro illegittima modifica o distruzione ovvero nel danneggiamento, nella distruzione o nel blocco del regolare funzionamento delle reti e dei sistemi informativi o dei loro elementi costitutivi;

c) « minaccia cibernetica »: il complesso delle condotte che possono essere realizzate nello spazio cibernetico o tramite esso, ovvero in danno dello stesso e dei suoi elementi costitutivi, che si sostanzia, in particolare, nelle azioni di singoli individui od organizzazioni, statali e no, pubbliche o private, finalizzate all'acquisizione e al trasferimento indebiti di dati, alla loro illegittima modifica o distruzione ovvero a danneggiare, distruggere od ostacolare il regolare funzionamento delle reti e dei sistemi informativi o dei loro elementi costitutivi;

d) « sovranità cibernetica »: la capacità dello Stato di essere autosufficiente nella costruzione, nel controllo e nella certificazione in ambito sia di *software*, sia di *hardware*;

e) « evento cibernetico »: l'avvenimento significativo, di natura volontaria o accidentale, consistente nell'acquisizione e nel trasferimento indebiti di dati, nella loro illegittima modifica o distruzione ovvero nel danneggiamento, nella distruzione o nel blocco del regolare funzionamento delle reti e dei sistemi informativi o dei loro elementi costitutivi;

f) « situazione di crisi »: la situazione in cui un evento cibernetico assume dimensioni, intensità o natura tali da incidere sulla sicurezza nazionale o da non poter essere fronteggiato dalle singole amministrazioni competenti in via ordinaria, bensì con l'assunzione di decisioni coordinate in sede interministeriale;

g) « contromisure cibernetiche »: le azioni mirate alla risposta a una minaccia cibernetica, che possono produrre effetti anche al di fuori del territorio nazionale,

attuate al fine di eliminare la situazione di crisi;

h) « *InfoSharing* »: 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;

i) « LGC »: le linee guida comuni.

ART. 3.

(Organi).

1. Ai fini della presente legge si intende per:

a) « CERT »: il *computer emergency response team*;

b) « NSC »: il Nucleo per la sicurezza cibernetica, di cui all'articolo 8 del decreto del Presidente del Consiglio dei ministri 24 gennaio 2013, pubblicato nella *Gazzetta Ufficiale* n. 66 del 19 marzo 2013;

c) « CISR »: il Comitato interministeriale per la sicurezza della Repubblica, di cui all'articolo 5 della legge 3 agosto 2007, n. 124;

d) « DIS »: il Dipartimento delle informazioni per la sicurezza, di cui all'articolo 4 della legge 3 agosto 2007, n. 124;

e) « AISE »: l'Agenzia informazioni e sicurezza esterna, di cui all'articolo 6 della legge 3 agosto 2007, n. 124;

f) « AISI »: l'Agenzia informazioni e sicurezza interna, di cui all'articolo 7 della legge 3 agosto 2007, n. 124;

g) « ISCOM »: l'Istituto superiore delle comunicazioni e delle tecnologie dell'informazione, istituito dalla legge 24 marzo 1907, n. 111;

h) « CNAIPIC »: il Centro nazionale anticrimine informatico per la protezione delle infrastrutture strategiche, istituito dal decreto del Capo della Polizia – Direttore generale della pubblica sicurezza 7 agosto 2008;

i) « CERT nazionale »: il CERT di cui all'articolo 16-*bis* del codice delle comunicazioni elettroniche, di cui al decreto legislativo 1º agosto 2003, n. 259;

l) « CERT-PA »: il CERT della pubblica amministrazione, istituito presso l'Agenzia per l'Italia digitale ai sensi del decreto del Presidente del Consiglio dei ministri 24 gennaio 2013, pubblicato nella *Gazzetta Ufficiale* n. 66 del 19 marzo 2013;

m) « CERT-Difesa »: il CERT istituito presso lo stato maggiore della Difesa, ai sensi della direttiva del Ministro per l'innovazione e le tecnologie 16 gennaio 2002, pubblicata nella *Gazzetta Ufficiale* n. 69 del 22 marzo 2002;

n) « DACI »: il Direttore per l'analisi cibernetica internazionale;

o) « RIS »: il reparto informazioni e sicurezza dello stato maggiore della Difesa;

p) « CIOC »: il Comando interforze operativo cibernetico, di cui all'articolo 16, comma 2.

TITOLO II

PROTEZIONE DELLO SPAZIO CIBERNETICO

CAPO I

DISPOSIZIONI DI INTERESSE DELLA DIFESA NEL SETTORE DELLA PROTEZIONE DELLO SPAZIO CIBERNETICO

ART. 4.

(Competenze del Segretario generale della difesa in materia di difesa cibernetica).

1. Il Segretario generale della difesa – Direttore nazionale degli armamenti promuove lo sviluppo della ricerca tecnologica nel campo della sicurezza cibernetica, considerata di interesse militare, secondo gli indirizzi impartiti dal Ministro della difesa.

2. Per i fini di cui al comma 1, il Segretario generale della difesa – Direttore nazionale degli armamenti assicura la piena integrazione delle attività di ricerca

militare nel settore cibernetico con quelle previste dal Programma nazionale per la ricerca, di cui all'articolo 1 del decreto legislativo 5 giugno 1998, n. 204; predispone e attua, 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; promuove 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.

3. Il Ministro della difesa impartisce gli indirizzi per l'attuazione delle disposizioni del presente articolo e per promuovere la cooperazione tra i centri di ricerca, sperimentazione e certificazione appartenenti all'Amministrazione della difesa e i soggetti pubblici e privati operanti nel sistema della ricerca e della produzione industriale nazionale nell'ambito della sicurezza cibernetica.

ART. 5.

(Formazione del personale militare nel settore della sicurezza cibernetica).

1. Il Governo è autorizzato ad apportare, entro sessanta giorni dalla data di entrata in vigore della presente legge, le modificazioni necessarie ad adeguare il testo unico delle disposizioni regolamentari in materia di ordinamento militare, di cui al decreto del Presidente della Repubblica 15 marzo 2010, n. 90, alle disposizioni della presente legge, allo scopo di assicurare la piena valorizzazione delle competenze e di favorire la crescita professionale, la formazione permanente e la specializzazione del personale militare a ogni livello nel settore della sicurezza cibernetica, secondo i seguenti criteri:

a) prevedere che l'ordinamento delle scuole militari garantisca una conoscenza

di base dei pericoli e delle minacce alla sicurezza globale connessi all'impiego delle nuove tecnologie, con particolare riferimento ai conflitti cibernetici;

b) prevedere che il ciclo di formazione degli ufficiali in servizio permanente delle Forze armate comprenda il conseguimento di una completa informazione sui pericoli e sulle minacce alla sicurezza globale connessi all'impiego delle nuove tecnologie, con particolare riferimento ai conflitti cibernetici;

c) prevedere che l'ordinamento delle scuole di applicazione e delle scuole di guerra per gli ufficiali in servizio assicuri il conseguimento di competenze operative e specialistiche nel settore della sicurezza cibernetica, comprese le strategie e gli strumenti operativi per il contrasto delle minacce e degli attacchi cibernetici;

d) prevedere che le scuole per gli allievi sottufficiali, le scuole per i volontari di truppa e gli altri istituti di formazione assicurino le necessarie conoscenze nel campo della sicurezza cibernetica secondo i ruoli e le specialità del personale.

ART. 6.

(Attribuzioni del Ministro della difesa).

1. Il Ministro della difesa emana le direttive di propria competenza in materia di protezione dello spazio cibernetico e di risposta ad attacchi cibernetici.

2. All'articolo 10, comma 1, del codice dell'ordinamento militare, di cui al decreto legislativo 15 marzo 2010, n. 66, dopo la lettera *b)* è inserita la seguente:

« *b-bis)* emana le direttive in materia di sicurezza cibernetica ».

ART. 7.

(Competenze delle Forze armate in materia di protezione dello spazio cibernetico).

1. Le Forze armate, nel rispetto delle competenze definite in materia di protezione delle infrastrutture informatiche cri-

tiche di interesse nazionale, concorrono alla protezione dello spazio cibernetico e alle operazioni di reazione ad attacchi di natura cibernetica.

2. All'articolo 89 del codice di cui al decreto legislativo 15 marzo 2010, n. 66, dopo il comma 1 è inserito il seguente:

« *1-bis*. Le Forze armate concorrono alla protezione dello spazio cibernetico nazionale ».

3. Dopo l'articolo 89 del codice di cui al decreto legislativo 15 marzo 2010, n. 66, è inserito il seguente:

« ART. 89-*bis*. – *(Contromisure cibernetiche)*. – *1*. Fuori dei casi previsti dagli articoli 78 e 87, nono comma, della Costituzione, l'uso delle contromisure cibernetiche è consentito a condizione che avvenga nel rispetto dei princìpi di cui all'articolo 11 della Costituzione, del diritto internazionale generale, del diritto internazionale dei diritti umani, del diritto internazionale umanitario e del diritto internazionale penale.

2. L'uso delle contromisure cibernetiche è deliberato dal Consiglio dei ministri, previa comunicazione al Presidente della Repubblica. Ove il Presidente della Repubblica o il Governo ne ravvisi la necessità, può essere convocato il Consiglio supremo di difesa, ai sensi dell'articolo 8, comma 2.

3. Il Governo comunica al Comitato parlamentare per la sicurezza della Repubblica, di cui all'articolo 30 della legge 3 agosto 2007, n. 124, le misure deliberate ai sensi del comma 2 del presente articolo.

4. Agli operatori che attuano le deliberazioni di cui al comma 2 del presente articolo sono riconosciute le garanzie funzionali previste dall'articolo 17 della legge 3 agosto 2007, n. 124, alle condizioni ivi previste. La deliberazione di cui al comma 2 del presente articolo tiene luogo dell'autorizzazione di cui all'articolo 18 della citata legge n. 124 del 2007.

5. Le garanzie di cui al comma 4 del presente articolo non si applicano in nessun caso ai crimini previsti dagli articoli da 5 a 8 dello Statuto della Corte penale internazionale, adottato a Roma il 17 luglio

1998, ratificato ai sensi della legge 12 luglio 1999, n. 232 ».

ART. 8.

(Ulteriori modifiche al codice di cui al decreto legislativo 15 marzo 2010, n. 66).

1. Al codice di cui al decreto legislativo 15 marzo 2010, n. 66, sono apportate le seguenti modificazioni:

a) all'articolo 12, comma 1, dopo la lettera *a)* è inserita la seguente:

« *a-bis)* l'evoluzione e le prospettive della minaccia cibernetica alla sicurezza nazionale »;

b) all'articolo 536, comma 1, la lettera *b)* è sostituita dalla seguente:

« *b)* l'elenco dei programmi d'armamento e di ricerca in corso e il relativo piano di programmazione finanziaria, indicante le risorse assegnate a ciascuno dei programmi per un periodo non inferiore a tre anni, compresi i programmi di ricerca o di sviluppo finanziati nello stato di previsione del Ministero dello sviluppo economico e quelli concernenti la sicurezza cibernetica. Nell'elenco sono altresì indicate le condizioni contrattuali, con particolare riguardo alle eventuali clausole penali ».

CAPO II

ORGANIZZAZIONE DEL SISTEMA NAZIONALE DI SICUREZZA CIBERNETICA

ART. 9.

(Sistema nazionale di sicurezza cibernetica).

1. Il sistema nazionale di sicurezza cibernetica è composto dal Presidente del Consiglio dei ministri, dal CISR, dal DIS, dal NSC, dal CIOC, dal CERT nazionale, dal CERT-PA, dal CERT-Difesa, dal CNAIPIC e dall'ISCOM.

ART. 10.

(Attribuzioni del Presidente del Consiglio dei ministri).

1. Il Presidente del Consiglio dei ministri provvede al coordinamento delle poli-

tiche dell'informazione per la sicurezza, impartisce le direttive e, sentito il CISR, emana ogni disposizione necessaria per l'organizzazione e per il funzionamento del sistema nazionale di sicurezza cibernetica.

2. Al Presidente del Consiglio dei ministri sono attribuite in via esclusiva:

a) la nomina e la revoca del direttore del NSC;

b) la determinazione, di concerto con i Ministri dell'economia e delle finanze, dell'interno e della difesa, dell'ammontare annuo delle risorse finanziarie destinate all'attività del sistema nazionale di sicurezza cibernetica a valere sul Fondo di cui all'articolo 20.

ART. 11.

(Autorità delegata e funzioni).

1. 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, di seguito denominato « Autorità delegata ».

2. Il Presidente del Consiglio dei ministri è costantemente informato dall'Autorità delegata sulle modalità di esercizio delle funzioni delegate e sui risultati conseguiti. Fermo restando il potere di direttiva, egli può comunque avocare a sé in qualsiasi momento l'esercizio di tutte le funzioni o di alcune di esse.

ART. 12.

(*Nomina del Direttore per l'analisi cibernetica internazionale*)

1. Il Ministro degli affari esteri e della cooperazione internazionale nomina, 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 ciber-

netici pertinenti agli interessi italiani all'estero.

ART. 13.

(Nomina del direttore del Nucleo per la sicurezza cibernetica).

1. Al NSC è preposto il direttore del NSC. L'incarico ha durata biennale ed è conferito con decreto del Presidente del Consiglio dei ministri, sentito il CISR, a un soggetto dotato di adeguata qualificazione, appartenente al DIS, al Ministero della difesa, al Ministero dell'interno o al Ministero dello sviluppo economico.

ART. 14.

(Conferimento di nuove attribuzioni al CERT nazionale).

1. In aggiunta ai compiti definiti dal decreto del Presidente del Consiglio dei ministri 24 gennaio 2013, pubblicato nella *Gazzetta Ufficiale* n. 66 del 19 marzo 2013, il CERT nazionale attiva 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.

2. Il CERT nazionale definisce la base di dati, 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 effettuata d'intesa con il CNAIPIC, il CERT-Difesa e il DIS. L'accesso al sistema di *InfoSharing* unico nonché l'inserimento dei dati da parte di enti diversi dal CERT nazionale sono gratuiti. Il sistema di *InfoSharing* unico è certificato dall'ISCOM.

ART. 15.

(CNAIPIC).

1. Nell'ambito del sistema nazionale di sicurezza cibernetica, il CNAIPIC esercita le funzioni di autorità di pubblica sicu-

rezza, in coordinamento con il CERT nazionale.

2. Al CNAIPIC sono attribuiti i seguenti compiti:

a) disporre l'interruzione dei pubblici servizi, su richiesta del Presidente del Consiglio dei ministri o dell'Autorità delegata, qualora sia necessario per contrastare un evento cibernetico di gravità tale da poter evolvere in una crisi cibernetica nazionale;

b) ricevere o produrre le informazioni classificate relative a eventi cibernetici e trattarle, provvedendo 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;

c) raccogliere e trasmettere ai soggetti interessati, in collaborazione con il DIS e nel rispetto delle disposizioni della legge 3 agosto 2007, n. 124, le informazioni classificate o riservate o la cui divulgazione potrebbe comunque costituire un pericolo per la sicurezza nazionale;

d) garantire al CERT nazionale l'integrazione del personale necessario ad assicurare la piena e ininterrotta operatività dei servizi di difesa cibernetica.

3. Il CNAIPIC, entro sei mesi dalla data di entrata in vigore della presente legge:

a) compila l'elenco delle infrastrutture strategiche;

b) definisce le LGC per l'integrazione dell'elenco di cui alla lettera *a)*.

ART. 16.

(CERT-Difesa e istituzione del CIOC).

1. Nell'ambito del sistema nazionale di sicurezza cibernetica, il CERT-Difesa opera nel settore della sicurezza militare, alle dipendenze del Ministro della difesa, in coordinamento con il DIS e con il RIS.

2. Nell'ambito dello Stato maggiore della difesa è istituito il Comando inter-

forze operativo cibernetico (CIOC), al quale spettano l'organizzazione e la direzione operativa delle attività relative alla difesa cibernetica. Le attribuzioni, la struttura e l'organizzazione del CIOC sono stabilite con decreto del Ministro della difesa, da adottare entro quattro mesi dalla data di entrata in vigore della presente legge.

3. Al CIOC spetta la direzione delle operazioni relative alle contromisure cibernetiche previste dall'articolo 89-*bis* del codice dell'ordinamento militare, di cui al decreto legislativo 15 marzo 2010, n. 66, introdotto dall'articolo 7 della presente legge.

4. Al CERT-Difesa sono attribuiti i seguenti compiti:

a) organizzare il sistema di protezione dei sistemi cibernetici delle Forze armate;

b) 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.

5. Il CERT-Difesa opera alle dipendenze del CIOC con la finalità di fornire informazioni sugli eventi cibernetici nel settore cibernetico militare.

6. 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.

CAPO III

TRATTAMENTO E GESTIONE DEI DATI CLASSIFICATI

ART. 17.

(Operatori di dati classificati).

1. 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.

2. Il CERT-Difesa e il CNAIPIC collaborano con il DIS per il trattamento dei dati

classificati nel campo della sicurezza cibernetica.

ART. 18.

(Gestione di eventi cibernetici classificati).

1. Il CNAIPIC, ai sensi dell'articolo 14, comma 2, entro sei mesi dalla data di entrata in vigore della presente legge, d'intesa con il DIS e con il CERT nazionale, definisce le LGC 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.

2. Nelle LGC predisposte ai sensi del comma 1 sono stabiliti:

a) il termine, non superiore a tre ore, per la presa in carico delle informazioni da parte del CNAIPIC e per la valutazione della necessità di pubblicazione delle stesse, previa rimozione dei dati e degli elementi classificati ai sensi dell'articolo 15, comma 2, lettera *b)*;

b) il termine decorso il quale, senza che il CNAIPIC abbia proceduto alla pubblicazione delle informazioni, il NSC, il CERT nazionale e il CERT-PA possono reiterare la richiesta ai fini della presa in carico e della gestione dell'evento cibernetico, qualora ritengano che ne perduri la necessità.

TITOLO III

CONTROLLO PARLAMENTARE, NORME FINANZIARIE E DISPOSIZIONI FINALI

CAPO I

CONTROLLO PARLAMENTARE

ART. 19.

(Parere delle Commissioni parlamentari).

1. Gli schemi dei decreti previsti dalla presente legge sono trasmessi alle Camere

per l'espressione del parere delle Commissioni parlamentari competenti per materia, con le modalità e nelle forme stabilite dai Regolamenti delle Camere. 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 possono essere comunque emanati.

2. Gli schemi delle LGC previste dalla presente legge sono trasmessi alle Camere per l'espressione del parere delle Commissioni parlamentari competenti per materia. Il termine per l'espressione del parere è di trenta giorni dalla trasmissione. Decorso tale termine, le LGC possono essere comunque adottate.

CAPO II

NORME FINANZIARIE

ART. 20.

(Fondo per la sicurezza cibernetica).

1. È istituito nello stato di previsione del Ministero dell'economia e delle finanze, per il successivo trasferimento al bilancio autonomo della Presidenza del Consiglio dei ministri, il Fondo per la sicurezza cibernetica.

2. Con decreto del Presidente del Consiglio dei ministri, da emanare entro sessanta giorni dalla data di entrata in vigore della presente legge, di concerto con il Ministro della difesa, con il Ministro dello sviluppo economico, con il Ministro dell'interno e con il Ministro dell'economia e delle finanze, sono definite le modalità di impiego del fondo di cui al comma 1.

ART. 21.

(Copertura finanziaria).

1. Agli oneri derivanti dall'attuazione delle disposizioni della presente legge si provvede mediante corrispondente ridu-

zione del fondo di cui all'articolo 1, comma 965, della legge 28 dicembre 2015, n. 208.

CAPO III

DISPOSIZIONI FINALI

ART. 22.

(Modifiche al decreto del Presidente del Consiglio dei ministri 24 gennaio 2013).

1. Il Governo è autorizzato ad apportare al decreto del Presidente del Consiglio dei ministri 24 gennaio 2013, pubblicato nella *Gazzetta Ufficiale* n. 66 del 19 marzo 2013, le modificazioni necessarie per adeguarlo e coordinarlo rispetto alle disposizioni della presente legge, con particolare riferimento alle norme contenute negli articoli 9, 10, 12, 13, 14 e 15 in materia di organizzazione del sistema nazionale di sicurezza cibernetica.

ART. 23.

(Entrata in vigore).

1. La presente legge entra in vigore il sessantesimo giorno successivo alla data della sua pubblicazione nella *Gazzetta Ufficiale*.