CAMERA DEI DEPUTATI N. 3544

PROPOSTA DI LEGGE

D'INIZIATIVA DEI DEPUTATI

ARTINI, BALDASSARRE, BECHIS, MATARRELLI, SEGONI, TURCO, BRIGNONE, CIVATI, ANDREA MAESTRI, PASTORINO

Istituzione del sistema nazionale di sicurezza cibernetica

Presentata il 19 gennaio 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 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 incrementare esponenzialmente gli attac-

chi 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 dell'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 *cybercrime* (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 *cyberwarfare*, 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 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 stato pubblicato 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.

Un ostacolo alla diffusione delle *cyber weapons* ha provato a metterlo l'Unione europea 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 *cyberdefence* 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 si 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 l'organizzazione della difesa cibernetica, il ripristino della sovranità nazionale sul mondo cibernetico, la formazione e la cultura della cibernetica. Uno degli obiettivi è la disciplina delle contromisure cibernetiche. Inoltre la proposta di legge ha lo scopo di ripristinare la sovranità nazionale nel settore industriale e accademico al fine di restituire il pieno controllo sulle infrastrutture strategiche cibernetiche del Paese. Un'ulteriore finalità consiste nel dettare una disciplina per rendere uniforme la preparazione degli operatori in tutti i settori dello Stato e per diffondere la cultura della sicurezza cibernetica, istituendo anche un'Alta scuola di formazione cibernetica.

Le minacce provenienti dal mondo cibernetico comportano per lo Stato la necessità di raggiungere la piena sovranità cibernetica nazionale. Tale sovranità dovrà estendersi agli ambiti *hardware, software* e *firmware*. In questi tre ambiti lo Stato deve progettare e costruire dei sistemi nazionali.

Tale riorganizzazione consentirà di: creare una più efficiente catena di comando e di controllo nazionale, che permetterà di gestire l'intero Sistema nazionale di sicurezza cibernetica nazionale da estendere anche agli enti privati di rilevanza strategica; eliminare le sovrapposizioni funzionali tra i vari enti; semplificare la collaborazione tra gli enti, anche consentendo un costante scambio di informazioni; garantire, anche tramite una maggiore uniformazione di sistemi e procedure, la capacità di rapida concentrazione delle risorse messe a disposizione da più enti per fare fronte efficacemente a minacce specifiche e particolarmente gravi; assicurare l'efficace formazione del personale dello Stato addetto alle attività di sicurezza cibernetica e la piena capacità di integrazione operativa dello stesso offrendo percorsi formativi differenziati ma accomunati da un percorso di base comune.

La presente proposta di legge, infatti, per dar seguito a quanto testé indicato, si articola nella definizione lineare delle necessità del nostro sistema, al fine di riorganizzare in una prospettiva almeno decennale il settore della sicurezza cibernetica.

In primo luogo vengono definiti gli ambiti e i soggetti che sono interessati dalla legge, indicando sia i princìpi ispi-

ratori, sia gli ambiti di azione dell'atto normativo, sia gli organi direttamente coinvolti nella gestione della sicurezza cibernetica (articoli 1, 2 e 3).

Si passa poi a definire il Sistema nazionale di sicurezza cibernetica: come per il sistema nazionale di sicurezza della Repubblica, definito dalla 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 4).

La legge conferisce in maniera prioritaria, alla stregua di altri sistemi nazionali di Stati europei e non europei, al Presidente del Consiglio dei ministri una serie di attribuzioni sulla sicurezza cibernetica, che gli riservano i poteri di decisione politica, su proposta del 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 5, 6 e 7). Un supporto specifico all'attività di *intelligence* viene definito per dare la giusta competenza agli organi disciplinati dalla legge n. 124 del 2007 (articolo 8).

Infine si definiscono nel dettaglio il ruolo e le funzioni del Nucleo cibernetico di sicurezza, presieduto da un direttore, non più identificato nel consigliere militare del Presidente del Consiglio dei ministri (come indicato nel citato decreto del Presidente del Consiglio dei ministri 24 gennaio 2013), che costituisce la cabina di regia in caso di crisi o evento cibernetico (articolo 9). 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.

Il capo II del titolo II introduce gli organi operativi: CERT-IT, CERT-Nazionale, CERT-PA, Centro nazionale anticrimine informatico per la protezione delle infrastrutture strategiche (CNAIPIC), Istituto superiore delle comunicazioni e delle tecnologie dell'informazione (ISCOM) e CERT-Difesa (articoli 10, 11, 12, 13, 14 e 15). Per ognuno 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 operativo cibernetico interforze (COCI), i cui compiti e organizzazione sono definiti dal Ministro della difesa (articolo 15, comma 2). Da esso dipende il CERT-Difesa.

Il CERT-IT ha la funzione di coordinamento tra i CERT-Nazionale, CERT-PA e CNAIPIC, con il supporto accademico dell'ISCOM, presso il quale è istituito il comitato scientifico (articolo 16). Tra i ruoli ricoperti dal CERT-IT vi è quello di definire un unico luogo dove ospitare gli organi operativi nel settore cibernetico, che provengono dai CERT indicati dalla legge. Lo spirito ispiratore di questa disposizione risiede nella volontà di creare una relazione di fiducia diretta tra i vari organismi e tra i loro operatori e nell'esigenza di garantire continuità di servizio ad ogni settore della società presidiato dalle disposizioni della presente proposta di legge.

Al fine di rendere omogenea e stabile la presenza di operatori e dirigenti nell'ambito della sicurezza cibernetica, sono introdotti particolari vincoli per l'acquisizione di personale (articolo 17, comma 1), con l'introduzione del vincolo dell'assunzione mediante contratti di lavoro a tempo indeterminato, per preservare le conoscenze e la professionalità acquisite dagli operatori.

Viene indicato come requisito prioritario il compimento di un percorso presso l'Alta scuola di formazione cibernetica (articolo 17, comma 2) per coloro che dovranno operare nell'ambito della difesa

cibernetica, ma si concede la possibilità ai cittadini italiani, la cui capacità nell'ambito cibernetico risulti comprovata, di essere impiegati con rapporti di consulenza esterna (articolo 17, comma 3). La programmazione e la disciplina delle assunzioni sono demandate a periodici decreti dei Ministri competenti (articolo 18).

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 19) ed è assistita dalla creazione di uno snodo telematico *(cyber-gateway)* che possa acquisire dati classificati e possa trattarli al fine di rendere disponibile l'informazione in merito all'evento cibernetico e alla sua soluzione (articolo 20). 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.

Il capo V contiene le disposizioni sulle contromisure cibernetiche, per il cui impiego è stabilita la competenza del Ministro della difesa e, sul piano operativo, delle Forze armate (articolo 21). Alle Forze armate è riconosciuta la possibilità di realizzare programmi informatici che consentano la verifica dei sistemi di difesa cibernetica nazionali (articolo 21, comma 2).

L'uso delle contromisure è deliberato al massimo livello politico dal Consiglio dei ministri (articolo 22) ed è comunicato al Presidente della Repubblica e al Comitato parlamentare per la sicurezza della Repubblica (le cui restanti attribuzioni di controllo in materia di sicurezza cibernetica sono definite dall'articolo 44). Agli operatori che attuano le contromisure deliberate sono riconosciute le garanzie funzionali previste dall'articolo 17 della legge n. 124 del 2007 (articolo 22, comma 4). 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 titolo III disciplina la formazione e la cultura cibernetica. Viene istituita l'Alta scuola di formazione cibernetica, inquadrata all'interno dell'ISCOM, e ne sono stabilite le competenze e i princìpi di organizzazione (articoli 23 e 24). La scuola cura la formazione per tutti gli operatori, mediante lo svolgimento di corsi che non comportano l'accesso a dati classificati. Per gli operatori che dovranno trattare dati classificati nell'ambito delle loro mansioni, la formazione impartita presso l'Alta scuola di formazione cibernetica dovrà essere integrata dalla frequenza della Scuola di formazione del DIS (articolo 25), con la previsione che nella programmazione dei corsi essa debba operare d'intesa con il reparto informazioni e sicurezza dello stato maggiore della Difesa.

Per la formazione del corpo docente e per l'integrazione e il coordinamento del programma formativo, l'Alta scuola attinge alle università, con l'obiettivo di integrare il lavoro formativo svolto da essa con i programmi di ricerca delle università (articolo 26).

Al fine di uniformare quanto più possibile i criteri di funzionamento del sistema di sicurezza nazionale cibernetico, si istituisce presso l'ISCOM l'Ente per la definizione degli *standard* in ambito cibernetico (EDSC) (articolo 27), che funge da punto di riferimento nazionale nella definizione di princìpi e parametri attinenti al dominio cibernetico, così da rendere univoca la trattazione dell'argomento da parte della pubblica amministrazione e degli enti privati.

Infine, per diffondere la cultura cibernetica, è attribuito al Governo l'incarico di predisporre e aggiornare annualmente un programma di corsi da svolgere nelle scuole primarie e secondarie e nelle università e una campagna di informazione su mezzi di comunicazione di massa e

internet (articolo 28). Tale punto è di fondamentale importanza se si vuole intervenire radicalmente per modificare, nei prossimi dieci anni, la capacità di sviluppo del Paese, orientando tutto il sistema nazionale verso lo sviluppo cibernetico.

Il titolo IV regolamenta l'interazione con il dominio cibernetico da parte degli enti privati. Tali soggetti sono classificati secondo il livello di rischio cibernetico o di importanza strategica per il Paese, nonché l'intensità dei rapporti che tali soggetti hanno non solo con la pubblica amministrazione ma anche con Stati esteri (articoli 29, 30 e 31). Particolare rilevanza hanno gli enti definiti all'articolo 29, che gestiscono o sono responsabili delle infrastrutture riconosciute come strategiche dal CNAIPIC ai sensi dell'articolo 13, comma 3, lettera *a)*.

Tutti questi enti, tranne quelli di cui all'articolo 31, sono sottoposti all'obbligo di comunicare al sistema di *InfoSharing* previsto dall'articolo 2, comma 1, lettera *l)*, gli eventi cibernetici che riguardino le proprie reti informatiche (articolo 32). Tale comunicazione è resa con le necessarie garanzie di riservatezza. Agli enti definiti all'articolo 31 si concede la possibilità di accedere gratuitamente al sistema di *InfoSharing*, con conseguente obbligo di comunicazione degli eventi cibernetici, come per gli enti gestori di infrastrutture strategiche (articolo 29) e per gli enti di rilevanza cibernetica (articolo 30).

Agli enti privati di cui all'articolo 31 viene garantita la possibilità di accesso a corsi di formazione gratuiti svolti dall'Alta scuola.

Ad ognuno di questi soggetti è applicato un particolare livello di sicurezza che prevede gradi diversificati di interazione con il Sistema nazionale di sicurezza cibernetica, dando agli enti gestori di infrastrutture strategiche la massima valorizzazione rispetto all'obbligo di comunicazione (articoli 32 e 36) e al livello di sicurezza richiesto, prevedendo proporzionati obblighi e livelli di sicurezza per gli enti privati di rilevanza cibernetica, con specifico rilievo per quelli che hanno 1000 *Host IP* e proventi derivanti da relazioni con l'estero superiori al 5 per cento dei proventi totali dell'ente stesso (articolo 35), nonché per gli altri enti che non ricadono in questa fattispecie (articolo 34).

Agli enti che ricadono nell'ambito dell'articolo 31 si applicano le sole prescrizioni del codice in materia di produzione dei dati personali, di cui al decreto legislativo n. 196 del 2003 (articolo 33).

Per facilitare anche la capacità di formazione del personale da parte degli enti privati si prevede un regolamento che disciplini l'organizzazione di corsi di formazione e la pubblicazione di materiali informativi sulla sicurezza cibernetica (articolo 37).

Una parte fondamentale della proposta di legge riguarda il raggiungimento della sovranità sulla costruzione di *software*, *hardware* e *firmware* che mediante la predisposizione di un sistema operativo sovrano e di un antivirus/anti-*malware* sovrano (articolo 39).

Per gli apparati *hardware* e *firmware* si prescrive di sviluppare un sistema di comunicazione IP (*router*) entro dieci anni dalla data di entrata in vigore della legge (articolo 40).

Per tutte le disposizioni per il raggiungimento della sovranità cibernetica viene istituito un elenco di imprese certificate, abilitate ad operare nell'ambito della difesa cibernetica (articolo 38). Tale elenco è utilizzato come supporto agli enti assegnati ai compiti di difesa cibernetica (articolo 21) o di gestione delle infrastrutture strategiche (articolo 39).

Per proiettare il mondo universitario ed industriale nell'ambito dello sviluppo e della ricerca, è anche prevista la definizione di un piano strategico, da predisporre in collaborazione con l'ISCOM e le università (articolo 41). Il piano non prevede la ricerca e lo sviluppo di contromisure cibernetiche, che sono predisposte da parte del Ministro della difesa (articolo 42, comma 2) in collaborazione con le imprese certificate comprese nel suddetto elenco.

Di fondamentale importanza, per il raggiungimento della sovranità cibernetica,

è l'agevolazione alle imprese innovative (*start-up*). Un caso di particolare interesse in tal senso è rappresentato dall'esperienza dello Stato di Israele, ove annualmente si avviano almeno 250 *start-up* nel settore della difesa cibernetica (articolo 42). Oltre alla possibilità di accedere al fondo previsto nella proposta di legge (articolo 48), viene concesso l'esonero dal pagamento delle spese per la registrazione dei brevetti.

La legge disciplina in maniera ampia, in una materia come la cibernetica, di estrema sensibilità (anche per il possibile controllo sui dati personali dei cittadini), il controllo parlamentare sulle informazioni classificate e no, il controllo da parte delle autorità di garanzia nonché le forme di pubblicità.

In particolare ogni schema di decreto o linea 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 verificare ciascun provvedimento di attuazione (articolo 43).

Al Comitato parlamentare per la sicurezza della Repubblica è attribuito pieno potere di controllo sul Sistema nazionale di sicurezza cibernetica per la parte che concerne le informazioni classificate (articolo 44). Il Comitato è informato in caso di uso di contromisure cibernetiche (articolo 22).

Al fine di dare ad un ente terzo un potere di controllo anche sulle modalità di trattamento dei dati, si garantisce all'Autorità per la protezione dei dati personali l'accesso a banche di dati e archivi nonché lo svolgimento di ispezioni e verifiche nei luoghi ove si svolge il trattamento di dati inerenti alla sicurezza cibernetica (articolo 45).

Entro il 31 dicembre di ogni anno il Presidente del Consiglio dei ministri dovrà presentare alle Camere una relazione, integrata dalle informazioni pertinenti fornite dai CERT, dall'ISCOM e dal CNAIPIC (articolo 46).

Le informazioni pubblicate dai CERT (articolo 10) nei rispettivi siti *internet* istituzionali devono essere rese disponibili in formato aperto, con aggiornamenti almeno giornalieri sugli eventi cibernetici trattati (articolo 47).

Nel titolo VI sono disciplinati i fondi finanziari necessari per sostenere l'attuazione della legge e le modalità di approvvigionamento rapido in caso di necessità da parte degli enti preposti alla difesa cibernetica.

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, dell'istruzione, dell'università e della ricerca 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 48). Tale fondo provvede il finanziamento di tutte le disposizioni della proposta di legge che comportano oneri finanziari a regime.

Il problema, da più parti rilevato, che nel settore cibernetico è di primaria importanza, ossia la necessità di reperire materiale informatico (da utilizzare per contrastare un evento cibernetico), viene risolto concedendo la possibilità di accedere in via prioritaria al fondo per la sicurezza cibernetica, con l'obbligo, per le amministrazioni che vi accedono per motivi di gravità ed urgenza (in particolare nelle situazioni di crisi), di ristorare i fondi entro il secondo esercizio finanziario successivo al prelevamento (articolo 49).

Infine, nello stesso titolo VI, vengono introdotte le sanzioni, sia penali sia amministrative, per violazioni in materia cibernetica e per l'inottemperanza delle disposizioni previste nella proposta di legge.

In particolare è introdotto il delitto di terrorismo cibernetico, punito con la pena della reclusione da cinque a dieci anni per coloro che cagionano un evento cibernetico di tale gravità da essere deliberato come crisi dal NSC (articolo 50).

Le sanzioni amministrative invece riguardano la mancata applicazione, da parte degli enti privati di cui al titolo IV, delle disposizioni circa i sistemi di sicu-

rezza da adottare nonché la violazione dell'obbligo di comunicazione degli eventi cibernetici da parte degli stessi enti privati (articolo 51.)

Infine, nel titolo VII sono contenute le disposizioni finali e, in particolare, la copertura finanziaria degli oneri derivanti dalla legge, per la quale è impiegato l'apposito fondo istituito dalla legge di stabilità 2016 (articolo 52).

Dalle nuove disposizioni introdotte discende l'abrogazione integrale 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.

PROPOSTA DI LEGGE

—

TITOLO I
FINALITÀ E DEFINIZIONI

ART. 1.
(Oggetto).

1. La presente legge disciplina:

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

b) l'attuazione delle contromisure cibernetiche;

c) i princìpi per il raggiungimento della piena sovranità nazionale nel settore scientifico e industriale relativo alla sicurezza cibernetica, al fine di garantire il completo controllo sulle infrastrutture strategiche cibernetiche del Paese;

d) l'istituzione e le funzioni dell'Alta scuola di formazione cibernetica, al fine di garantire l'uniformità della formazione in materia cibernetica nell'ambito della pubblica amministrazione;

e) il controllo parlamentare sul sistema nazionale di sicurezza cibernetica.

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

idonee misure di sicurezza fisica, logica e procedurale rispetto a eventi, di natura volontaria o accidentale, consistenti 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;

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*;

f) « 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;

g) « allarme »: la comunicazione di avviso di un evento cibernetico da valutare ai fini dell'attivazione di misure di risposta pianificate;

h) « situazione di crisi »: la situazione in cui l'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;

i) « contromisure cibernetiche »: le azioni mirate alla risposta a una minaccia cibernetica, che possono produrre effetti anche al di fuori del territorio nazionale, effettuate al fine di eliminare la situazione di crisi.

l) « *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;

m) « LGC »: le linee guida comuni;

n) « IS »: le infrastrutture strategiche.

ART. 3.

(Organi).

1. Ai fini della presente legge si intende per:

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

b) « SOC »: il *Security operations center*;

c) « 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;

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

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

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

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

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

i) « 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;

l) « CERT-IT »: il CERT di collegamento funzionale e di coordinamento tra il CERT-Nazionale, il CERT-PA e il CERT-Difesa;

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

n) « 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;

o) « 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;

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

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

r) « COCI »: il Comando operativo cibernetico interforze, di cui all'articolo 15, comma 2.

TITOLO II

ISTITUZIONE E ORGANIZZAZIONE DEL SISTEMA NAZIONALE DI SICUREZZA CIBERNETICA

CAPO I

ORGANI POLITICO-STRATEGICI E LORO ATTRIBUZIONI

ART. 4.

(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 CERT-IT, dal CERT-Nazionale, dal CERT-PA, dal CERT-Difesa, dal CNAIPIC e dall'ISCOM.

ART. 5.

(Attribuzioni del Presidente del Consiglio dei ministri).

1. Il Presidente del Consiglio dei ministri provvede al coordinamento delle politiche 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) l'alta direzione e la responsabilità generale della politica di sicurezza cibernetica nazionale, nell'interesse e per la difesa della Repubblica e delle istituzioni democratiche poste dalla Costituzione a suo fondamento;

b) l'adozione e l'aggiornamento almeno annuale, su proposta del CISR, del Quadro strategico nazionale per la sicurezza dello spazio cibernetico, contenente l'indicazione dei profili e delle tendenze evolutive delle minacce cibernetiche e dei fattori di vulnerabilità dei sistemi e delle reti di interesse nazionale, l'indicazione dei criteri per lo sviluppo degli strumenti e delle procedure con cui si provvede all'incremento delle capacità di prevenzione e di risposta rispetto ad eventi occorrenti nello spazio cibernetico, al fine di diffondere la cultura della sicurezza;

c) l'adozione, previa deliberazione del CISR, del Piano nazionale per la protezione cibernetica e la sicurezza informatica nazionali, contenente gli obiettivi da conseguire e le linee di azione da porre in essere per realizzare il Quadro strategico nazionale di cui alla lettera *b)*;

d) l'emanazione delle direttive e degli atti d'indirizzo necessari per l'attuazione del Piano di cui alla lettera *c)*;

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

f) la nomina e la revoca del direttore del CERT-IT;

g) 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 48.

ART. 6.

(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. 7.

(Attribuzioni del CISR).

1. Al CISR sono attribuiti, nell'ambito del sistema nazionale di sicurezza cibernetica, i seguenti compiti nella materia della sicurezza dello spazio cibernetico:

a) proporre al Presidente del Consiglio dei ministri l'adozione del Quadro strategico nazionale di cui all'articolo 5, comma 2, lettera *b)*;

b) deliberare il Piano nazionale di cui all'articolo 5, comma 2, lettera *c)*, ai fini della sua adozione da parte del Presidente del Consiglio dei ministri;

c) esprimere parere, ai sensi dell'articolo 5, comma 2, lettera *h)*, della legge 23 agosto, 1988, n. 400, sulle direttive e sugli atti d'indirizzo del Presidente del Consiglio dei ministri di cui all'articolo 5, comma 2, lettera *d)*, della presente legge;

d) esprimere parere, ai sensi dell'articolo 1, comma 3-*bis*, della legge 3 agosto 2007, n. 124, ai fini dell'adozione delle direttive del Presidente del Consiglio dei ministri destinate al DIS e ai servizi di informazione per la sicurezza in materia di sicurezza cibernetica;

e) esercitare l'alta sorveglianza sull'attuazione del Piano nazionale di cui all'articolo 5, comma 2, lettera *c)*;

f) approvare le LGC per favorire l'efficace collaborazione tra i soggetti istituzionali e gli operatori privati interessati alla sicurezza cibernetica, nonché per la condivisione delle informazioni e per l'adozione di buone pratiche e di misure rivolte all'obiettivo della sicurezza cibernetica;

g) elaborare, ai sensi dell'articolo 5 della legge 3 agosto 2007, n. 124, gli indirizzi generali e gli obiettivi fondamentali in materia di protezione cibernetica e di sicurezza informatica nazionali, da perseguire nel quadro della politica dell'informazione per la sicurezza da parte degli organismi di informazione per la sicurezza, ciascuno per i profili di rispettiva competenza;

h) promuovere, tramite il CERT-IT e il CERT-Difesa, l'adozione delle iniziative necessarie per assicurare, in forma coordinata, la piena partecipazione dell'Italia ai diversi consessi di cooperazione internazionale, sia in ambito bilaterale o multilaterale, sia negli ambiti dell'Unione europea e dell'Alleanza atlantica, al fine della definizione e dell'adozione di politiche e strategie comuni di prevenzione e di risposta alla minaccia cibernetica;

i) formulare le proposte di intervento normativo e organizzativo ritenute necessarie al fine del potenziamento delle misure di prevenzione e di risposta alla minaccia cibernetica e quelle per la gestione delle situazioni di crisi;

l) partecipare, con funzioni di consulenza e di proposta, alle decisioni del Presidente del Consiglio dei ministri in caso di situazioni di crisi. Alle riunioni del CISR aventi ad oggetto la materia della sicurezza cibernetica partecipa, con funzioni di consulenza, il direttore del NSC.

2. Si applicano, anche ai fini di cui al comma 1 del presente articolo, le disposizioni dell'articolo 5, comma 5, della legge 3 agosto 2007, n. 124.

ART. 8.

(Organi di coordinamento e di informazione per la sicurezza cibernetica).

1. Il DIS, l'AISE e l'AISI svolgono la propria attività nel campo della sicurezza cibernetica avvalendosi degli strumenti e secondo le modalità e le procedure previsti dalla legge 3 agosto 2007, n. 124.

2. Per le finalità di cui al comma 1 del presente articolo, il direttore generale del DIS, sulla base delle direttive adottate dal Presidente del Consiglio dei ministri ai sensi dell'articolo 1, comma 3-*bis*, della legge 3 agosto 2007, n. 124, nonché degli indirizzi generali e degli obiettivi fondamentali individuati dal CISR, cura, ai sensi dell'articolo 4, comma 3, lettera *d-bis),* della citata legge n. 124 del 2007, il coordinamento delle attività di ricerca informativa finalizzate a rafforzare la protezione cibernetica e la sicurezza informatica nazionali.

3. Il DIS, sulla base delle informazioni raccolte e delle acquisizioni provenienti dallo scambio informativo di cui all'articolo 4, comma 3, lettere *c)* ed *e)*, della legge 3 agosto 2007, n. 124, nonché degli elementi acquisiti ai sensi dell'articolo 13, commi 1 e 2, della medesima legge n. 124 del 2007, trasmette al CERT-IT informazioni e analisi su eventi cibernetici. Il DIS

e il CERT-IT provvedono a trattare tempestivamente le informazioni e a pubblicarle, con le garanzie necessarie in base alla loro classificazione di segretezza, nella piattaforma *InfoSharing*.

4. Per lo svolgimento delle attività di coordinamento di cui al comma 2, il direttore generale del DIS si avvale delle strutture del medesimo DIS nonché, ove necessario, della collaborazione del CERT-IT. Il DIS, sulla base delle informazioni raccolte e delle acquisizioni provenienti dallo scambio informativo di cui all'articolo 4, comma 3, lettere *c)* ed *e)*, della legge 3 agosto 2007, n. 124, nonché degli elementi acquisiti ai sensi dell'articolo 13, commi 1 e 2, della medesima legge n. 124 del 2007, cura altresì la formulazione di analisi, valutazioni e previsioni sulla minaccia cibernetica. Provvede inoltre, secondo le disposizioni della presente legge, alla trasmissione delle informazioni rilevanti ai fini della sicurezza cibernetica al NSC, alle pubbliche amministrazioni e agli altri soggetti, anche privati, interessati all'acquisizione di informazioni medesime, ai sensi dell'articolo 4, comma 3, lettera *f)*, della citata legge n. 124 del 2007.

5. L'AISE e l'AISI, nell'ambito delle rispettive attribuzioni, svolgono, secondo gli indirizzi definiti dalle direttive del Presidente del Consiglio dei ministri e le linee di coordinamento delle attività di ricerca informativa stabilite dal direttore generale del DIS ai sensi del comma 2, le attività di ricerca e di elaborazione informativa rivolte alla protezione cibernetica e alla sicurezza informatica nazionali.

6. Per lo svolgimento delle attività previste dal presente articolo, il DIS, l'AISE e l'AISI corrispondono con le pubbliche amministrazioni, i soggetti erogatori di servizi di pubblica utilità, le università e gli enti di ricerca; per il medesimo fine possono stipulare convenzioni con tali soggetti ai sensi dell'articolo 13, comma 1, della legge 3 agosto 2007, n. 124. Per le stesse finalità, le pubbliche amministrazioni e i soggetti erogatori di servizi di pubblica utilità consentono l'accesso del DIS, dell'AISE e dell'AISI ai propri archivi informatici secondo le modalità e con le procedure

previste dal regolamento di cui al decreto del Presidente del Consiglio dei ministri 12 giugno 2009, n. 2.

7. 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 una visione 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. 9.

(Nucleo per la sicurezza cibernetica – NSC).

1. Il NSC è composto da un rappresentante, rispettivamente, del DIS, dell'AISE, dell'AISI, del Ministero degli affari esteri e della cooperazione internazionale, del Ministero dell'interno, del Ministero della difesa, del Ministero dello sviluppo economico, del Ministero dell'economia e delle finanze, del Dipartimento della protezione civile della Presidenza del Consiglio dei ministri e dell'Agenzia per l'Italia digitale nonché dal direttore del CERT-IT. I rappresentanti degli organi ed enti di cui al primo periodo sono designati secondo quanto previsto dalle LGC approvate ai sensi dell'articolo 7, comma 1, lettera *f)*.

2. Per gli aspetti relativi alla trattazione di informazioni classificate, il NSC è integrato da un rappresentante dell'Ufficio centrale per la segretezza, di cui all'articolo 9 della legge 3 agosto 2007, n. 124.

3. 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.

4. I rappresentanti degli organi ed enti di cui al secondo periodo del comma 1 possono essere assistiti, nelle riunioni del NSC, da esperti appartenenti alle strutture operative del rispettivo organo o ente. Il

direttore del NSC può autorizzare la partecipazione di rappresentanti di altre amministrazioni, di università o di enti e istituti di ricerca, nonché di operatori privati interessati alla materia della sicurezza cibernetica.

5. Il NSC si riunisce almeno una volta al mese, su iniziativa del suo direttore o su richiesta di almeno uno dei suoi componenti.

CAPO II

ORGANI OPERATIVI E LORO ATTRIBUZIONI

ART. 10.

(CERT-IT).

1. Presso la Presidenza del Consiglio dei ministri è istituito il CERT-IT.

2. Al CERT-IT sono attribuiti i seguenti compiti:

a) coordinare l'attività svolta in collaborazione tra il CERT-PA, il CERT-Nazionale e il CNAIPIC;

b) valutare e promuovere, in raccordo con le amministrazioni competenti per specifici profili della sicurezza cibernetica e tenuto conto di quanto previsto dall'articolo 32, procedure di condivisione delle informazioni, anche con gli operatori privati interessati, ai fini della diffusione di allarmi relativi ad eventi cibernetici e per la gestione delle crisi;

c) acquisire e coordinare, tramite il Ministero dello sviluppo economico, gli organismi di informazione per la sicurezza, le Forze di polizia e le strutture del Ministero della difesa, le comunicazioni circa i casi di violazione o i tentativi di violazione della sicurezza cibernetica e i casi di perdita dell'integrità di dati significativi ai fini del corretto funzionamento delle reti e dei servizi;

d) esercitare le funzioni di punto di riferimento nazionale per i rapporti con le organizzazioni internazionali e con gli al-

tri Stati, nell'ambito della sicurezza cibernetica, 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 delle altre amministrazioni competenti, assicurando il necessario coordinamento;

e) mantenere un costante scambio di informazioni e coordinare le proprie attività con il CERT-Difesa, al fine di conseguire la massima efficacia delle rispettive azioni;

f) attivare un unico sito *internet* istituzionale per gli organi di cui agli articoli 11, 12, 13 e 14, nel quale sono pubblicate le informazioni sullo stato della sicurezza cibernetica, ai sensi dell'articolo 47.

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

a) individua una sede unica per gli operatori del CERT-PA, del CERT-Nazionale e del CNAIPIC;

b) redige un protocollo per l'integrazione delle funzioni degli organi interessati, al fine di rendere più efficace e temporalmente completo il controllo delle IS;

c) 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. L'accesso al sistema di *InfoSharing* unico nonché l'inserimento dei dati da parte di enti diversi dal CERT-PA sono gratuiti. Il sistema di *InfoSharing* unico è certificato dall'ISCOM.

ART. 11.

(CERT-Nazionale).

1. Il CERT-Nazionale è collocato organizzativamente nell'ambito della Presidenza del Consiglio dei ministri e dipende

funzionalmente da questa; il personale ad esso assegnato dipende organicamente dal Ministero dello sviluppo economico ed è disciplinato dal suo ordinamento.

2. Al CERT-Nazionale sono attribuiti i seguenti compiti:

a) promuovere e coordinare, d'intesa con il Ministero dello sviluppo economico e con l'Agenzia per l'Italia digitale per i profili di rispettiva competenza, lo svolgimento di esercitazioni che coinvolgono amministrazioni diverse nonché la partecipazione nazionale a esercitazioni internazionali con la simulazione di eventi cibernetici;

b) garantire al CERT-IT, in collaborazione con il CERT-PA e con il CNAIPIC, l'integrazione del personale necessario ad assicurare la piena e ininterrotta operatività dei servizi di difesa cibernetica.

3. Il CERT-Nazionale, entro sei mesi dalla data di entrata in vigore della presente legge, definisce le LGC per la gestione delle simulazioni di eventi cibernetici.

ART. 12.

(CERT-PA).

1. Il CERT-PA è collocato organizzativamente nell'ambito della Presidenza del Consiglio dei ministri e dipende funzionalmente da questa; il personale ad esso assegnato dipende organicamente dall'Agenzia per l'Italia digitale ed è disciplinato dal suo ordinamento.

2. Al CERT-PA sono attribuiti i seguenti compiti:

a) definire 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;

b) garantire al CERT-IT, in collaborazione con il CERT-Nazionale e con il

CNAIPIC, l'integrazione del personale necessario ad assicurare la piena e ininterrotta operatività dei servizi di difesa cibernetica.

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

a) redige protocolli per la comunicazione e lo scambio di dati con il CERT-Nazionale e con gli altri CERT delle pubbliche amministrazioni e degli enti privati tenuti a tale adempimento secondo le disposizioni della presente legge;

b) stabilisce i criteri in base ai quali gli organi della pubblica amministrazione sono tenuti a dotarsi di un CERT interno;

c) stabilisce i criteri in base ai quali un'amministrazione può usufruire dei CERT di altre amministrazioni;

d) adotta le regole per la gestione, l'inserimento dei dati e la consultazione del sistema di *InfoSharing* unico.

ART. 13.

(CNAIPIC).

1. Nell'ambito del sistema nazionale di sicurezza cibernetica, il CNAIPIC esercita le funzioni di autorità di pubblica sicurezza, in coordinamento con il CERT-IT.

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-IT, in collaborazione con il CERT-Nazionale e con il CERT-PA, 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 IS;

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

ART. 14.

(ISCOM).

1. All'ISCOM sono attribuiti i seguenti compiti:

a) elaborare, convalidare, controllare e certificare le caratteristiche dei sistemi *software* e *hardware* distribuiti nel territorio nazionale;

b) elaborare e proporre al Presidente del Consiglio dei ministri le soluzioni per raggiungimento della completa sovranità cibernetica.

2. L'ISCOM, entro sei mesi dalla data di entrata in vigore della presente legge:

a) definisce le LGC per la certificazione delle procedure operative dei CERT, adottando le regole comuni e i criteri da applicare;

b) definisce le LGC per la certificazione dei sistemi *hardware* e *software* per garantire la sovranità cibernetica;

c) coadiuva tecnicamente l'attività del CERT-PA nella realizzazione del sistema di *InfoSharing* unico.

ART. 15.

(CERT-Difesa e ambito cibernetico militare).

1. Nell'ambito del sistema nazionale di sicurezza cibernetica, il CERT-Difesa opera nel campo 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 operativo cibernetico interforze (COCI), al quale spettano l'organizzazione e la direzione operativa delle attività relative alla difesa cibernetica. Le attribuzioni, la struttura e l'organizzazione del COCI sono stabilite con decreto del Ministro della difesa, da adottare entro quattro mesi dalla data di entrata in vigore della presente legge.

3. Al COCI spetta la direzione delle operazioni relative alle contromisure cibernetiche di cui all'articolo 21.

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 COCI 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 COCI.

ART. 16.

(Comitato tecnico-scientifico).

1. Presso l'Alta scuola di formazione cibernetica di cui all'articolo 23 è istituito

un comitato scientifico composto da esperti nelle discipline inerenti alla sicurezza cibernetica provenienti dalle università, dagli enti di ricerca, dalle pubbliche amministrazioni e dal settore privato.

2. Il comitato di cui al comma 1 predispone programmi di intervento volti a migliorare i parametri e i livelli di sicurezza dei sistemi e delle reti, al fine di coadiuvare il sistema nazionale di sicurezza cibernetica.

CAPO III

DISPOSIZIONI IN MATERIA DI PERSONALE

ART. 17.

(Disposizioni in materia di personale).

1. Al fine di valorizzare le competenze del personale e di garantire la riservatezza delle informazioni raccolte dagli organi di cui agli articoli 10, 11, 12, 13 e 14, il personale civile impiegato per le funzioni svolte dai medesimi organi può essere assunto soltanto con contratto di lavoro a tempo indeterminato.

2. Il personale civile da destinare agli organi di cui al comma 1 è scelto in via prioritaria tra coloro che hanno conseguito l'attestato di qualificazione presso l'Alta scuola di formazione cibernetica di cui all'articolo 23.

3. Gli organi di cui agli articoli 10, 11, 12, 13, 14 e 15 possono avvalersi di consulenti esterni scelti tra cittadini italiani che, pur non essendo in possesso del requisito di cui al comma 2 del presente articolo, possiedono comprovate capacità nelle attività cibernetiche, anche in deroga a quanto previsto ai sensi dell'articolo 18, comma 3.

ART. 18.

(Disciplina e programmazione dell'assunzione di personale).

1. Con uno o più decreti adottati dai Ministri competenti, anche di concerto tra

loro, sono definite per ogni triennio le modalità di assunzione del personale civile da assegnare agli organi di cui agli articoli 10, 11, 12, 13 e 14.

2. Con uno o più decreti adottati dai Ministri competenti, anche di concerto tra loro, è programmato annualmente il fabbisogno del personale civile necessario per gli organi di cui al comma 1. Nei decreti sono indicati i requisiti necessari per ciascun ruolo individuato.

3. Con uno o più decreti adottati dai Ministri competenti, anche di concerto tra loro, sono definiti gli ambiti della difesa cibernetica per i quali gli organi di cui al comma 1 possono stipulare contratti di consulenza di durata non superiore a un anno con soggetti esterni alla pubblica amministrazione.

CAPO IV

TRATTAMENTO E GESTIONE DEI DATI CLASSIFICATI

ART. 19.

(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. 20.

(Gestione di eventi cibernetici classificati).

1. Il CNAIPIC, ai sensi dell'articolo 12, comma 2, lettera *b)*, entro sei mesi dalla data di entrata in vigore della presente legge, d'intesa con il DIS e con gli organi di cui agli articoli 9, 10, 11, 12 e 13, definisce le LGC per la presa in carico e la gestione degli eventi cibernetici classificati e per la pubblicazione, mediante la piattaforma *InfoSharing*, delle informa-

zioni 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 13, comma 2, lettera *b)*;

b) il termine decorso il quale, senza che il CNAIPIC abbia proceduto alla pubblicazione delle informazioni, gli organi di cui agli articoli 9, 10, 11, 12 e 13 possono reiterare la richiesta ai fini della presa in carico e della gestione dell'evento cibernetico, qualora ritengano che ne perduri la necessità.

CAPO V
CONTROMISURE CIBERNETICHE

ART. 21.
(Organi e funzioni degli operatori di contromisure cibernetiche).

1. Le Forze armate sono autorizzate all'uso e alla gestione delle contromisure cibernetiche.

2. Le Forze armate possono sviluppare programmi di contromisure cibernetiche finalizzati alla verifica della funzionalità dei sistemi di difesa cibernetica previsti ai sensi della presente legge.

3. Per le finalità di cui al comma 2, le Forze armate possono avvalersi delle imprese iscritte nell'elenco di cui all'articolo 38.

4. Le attività di cui ai commi 1 e 2 sono finanziate a valere sul Fondo di cui all'articolo 48.

ART. 22.
(Deliberazione di contromisure cibernetiche).

1. Fuori dei casi previsti dagli articoli 78 e 87, nono comma, della Costituzione, l'uso delle contromisure cibernetiche è

consentito, in conformità a quanto disposto dalla presente legge, 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, del codice dell'ordinamento militare, di cui al decreto legislativo 15 marzo 2010, n. 66.

3. Il Governo comunica al Comitato parlamentare per la sicurezza della Repubblica, ai sensi dell'articolo 44, le misure deliberate ai sensi del comma 2.

4. Agli operatori che attuano le deliberazioni di cui al comma 2 sono riconosciute le garanzie funzionali di cui all'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 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.

TITOLO III

FORMAZIONE E CULTURA CIBERNETICA

CAPO I

ORGANI DI FORMAZIONE E DI CERTIFICAZIONE, FUNZIONI E COMPETENZE

ART. 23.

(Alta scuola di formazione cibernetica).

1. È istituita presso l'ISCOM l'Alta scuola di formazione cibernetica, di se-

guito denominata « Alta scuola », con il compito di curare la formazione:

a) del personale della pubblica amministrazione da inquadrare presso gli organi di cui agli articoli 10, 11, 12, 13, 14 e 15;

b) del personale della pubblica amministrazione competente per l'ambito cibernetico.

2. Il funzionamento dell'Alta scuola è assicurato a valere sulle risorse del Fondo di cui all'articolo 48.

3. L'Alta scuola può istituire corsi destinati a personale della pubblica amministrazione, diverso dai soggetti indicati al comma 1, nonché a personale delle università, degli enti di ricerca e di enti e imprese privati, al fine di diffondere e incrementare la cultura e la formazione nel settore della sicurezza cibernetica.

4. Al termine dei corsi di formazione, l'Alta scuola rilascia il corrispondente attestato di qualificazione ai partecipanti che hanno superato l'esame finale.

5. L'Alta scuola si avvale del personale di cui all'articolo 17 nonché di docenti e ricercatori delle università, sulla base di contratti di consulenza, in conformità a quanto disposto dall'articolo 18.

ART. 24.

(Organizzazione dell'Alta scuola).

1. Con decreto del Ministro dell'istruzione, dell'università e della ricerca, da adottare entro sei mesi dalla data di entrata in vigore della presente legge, di concerto con il Ministro della difesa e con il Ministro dello sviluppo economico e sentito l'ISCOM, sono definite la struttura, l'organizzazione e la disciplina dei corsi dell'Alta scuola, nonché gli ambiti della formazione da essa impartita.

2. I percorsi di studio dell'Alta scuola, uniformi per il personale di tutte le pubbliche amministrazioni, sono distinti in base alle funzioni dirigenziali od operative

esercitate e al livello di qualificazione richiesto ai soggetti di cui ai commi 1 e 3 dell'articolo 23. Per il personale che esercita funzioni operative sono previste esercitazioni e verifiche pratiche secondo la specificità della materia cibernetica.

ART. 25.

(Scuola di formazione per la gestione dei dati classificati in materia cibernetica).

1. Alla formazione cibernetica del personale degli organi di cui agli articoli 13 e 15, nell'ambito riguardante dati classificati, provvede la Scuola di formazione del DIS, istituita ai sensi dell'articolo 11 della legge 3 agosto 2007, n. 124.

2. La Scuola di formazione del DIS provvede alla formazione del personale necessario a svolgere le funzioni relative alla gestione e all'uso delle contromisure cibernetiche di cui all'articolo 21 in collaborazione con il RIS.

ART. 26.

(Coordinamento e collegamento con le università).

1. L'Alta scuola assicura il coordinamento e il collegamento con le università, ai sensi dell'articolo 23, comma 3, ai fini di:

a) selezionare i docenti e i ricercatori universitari da impiegare per lo svolgimento dei corsi di formazione;

b) attivare corsi di formazione nell'ambito cibernetico per gli studenti universitari meritevoli;

c) attivare corsi di aggiornamento permanente per il personale docente e i ricercatori universitari nel settore della sicurezza cibernetica.

ART. 27.

(Ente di definizione degli standard *cibernetici).*

1. È istituito presso l'ISCOM l'Ente per la definizione degli *standard* in ambito cibernetico (EDSC), con il compito di:

a) definire gli *standard* relativi a *hardware, software* e *firmware* per garantire il corretto funzionamento dei sistemi nell'ambito della sicurezza cibernetica;

b) definire annualmente, in collaborazione con l'Alta scuola, le LGC per la formazione nella settore della difesa cibernetica.

2. In caso di definizione di nuovi *standard* ai sensi del comma 1 che comportino oneri di adeguamento per i soggetti privati, gli oneri conseguenti a carico di questi ultimi sono ristorati, anche parzialmente, a valere sul Fondo di cui all'articolo 48.

ART. 28.

(Programmi di diffusione della cultura cibernetica).

1. Entro un anno dalla data di entrata in vigore della presente legge, con decreto del Ministro dell'istruzione, dell'università e della ricerca, di concerto con i Ministri dell'interno, della difesa e dello sviluppo economico, sono disciplinati:

a) un programma di diffusione della cultura della sicurezza cibernetica, anche tramite appositi corsi da attivare nelle università e nelle scuole primarie e secondarie di primo e di secondo grado;

b) una campagna di informazione, tramite i mezzi di comunicazione di massa e la rete *internet*, finalizzata alla diffusione della cultura della sicurezza cibernetica.

2. Il programma e la campagna di cui al comma 1 sono aggiornati con cadenza almeno annuale.

TITOLO IV

DISPOSIZIONI PER GLI ENTI PRIVATI

CAPO I

LINEE GUIDA DI SICUREZZA PER GLI ENTI PRIVATI

ART. 29.

(Enti privati di interesse strategico).

1. Ai fini della presente legge, sono considerati enti privati di interesse strategico gli enti privati gestori o responsabili delle IS definite dal CNAIPIC ai sensi dell'articolo 13, comma 3, lettera *a)*. Ad essi si applicano le disposizioni dell'articolo 36.

2. Per il supporto e l'aggiornamento dei sistemi di difesa cibernetica è consentito agli enti privati di interesse strategico l'accesso alle risorse del Fondo di cui all'articolo 48.

3. Con decreto del Presidente del Consiglio dei ministri, da adottare entro sei mesi dalla data di entrata in vigore della presente legge, sono definite le modalità per l'accesso alle risorse del Fondo di cui all'articolo 48 ai sensi del comma 2 del presente articolo.

ART. 30.

(Enti privati di rilevanza cibernetica).

1. Sono considerati enti privati di rilevanza cibernetica per la pubblica amministrazione i soggetti privati che hanno rapporti con essa.

2. Con decreti dei Ministri competenti, da adottare entro sei mesi dalla data di entrata in vigore della presente legge, sono approvati gli elenchi degli enti di cui al comma 1, previa valutazione della rilevanza cibernetica, della natura e della frequenza dei rapporti tra gli enti privati interessati e la pubblica amministrazione. Gli elenchi sono aggiornati con le stesse

modalità ogni volta che il Ministro lo ritenga necessario e, comunque, annualmente.

3. Il CERT-Nazionale definisce le LGC per la fissazione dei livelli di sicurezza da applicare agli enti privati che hanno rapporti con la pubblica amministrazione. Le LGC sono rese pubbliche nel sito *internet* istituzionale del CERT-IT.

4. Ai soggetti di cui all'articolo 29 che hanno rapporti con la pubblica amministrazione non si applicano le disposizioni di cui al comma 3 del presente articolo. Ad essi si applicano le disposizioni dell'articolo 36.

ART. 31.

(Altri enti privati).

1. L'Alta scuola organizza corsi di formazione finalizzati a rafforzare la cultura della sicurezza cibernetica, ai quali può partecipare il personale degli enti privati diversi da quelli di cui agli articoli 29 e 30, selezionato in base ad appositi bandi pubblici. I corsi di formazione sono gratuiti. Restano a carico degli enti privati di appartenenza tutte le spese relative alla frequenza dei partecipanti, compreso il costo dell'eventuale materiale didattico necessario per il corso ceduto in proprietà al partecipante.

ART. 32.

(Obbligo di comunicazione e accesso alla piattaforma InfoSharing).

1. Agli enti privati di cui agli articoli 29 e 30 è consentito l'accesso gratuito alla piattaforma *InfoSharing*, in modalità di lettura e scrittura e con il supporto degli organi di cui agli articoli 10, 11, 12, 13 e 14, limitatamente alle informazioni non classificate.

2. Agli enti privati di cui all'articolo 31 è consentito l'accesso gratuito alla piattaforma *InfoSharing*, in modalità di lettura e scrittura, limitatamente alle informazioni non classificate.

3. Gli enti privati di cui agli articoli 29, 30 e 31 che accedono alla piattaforma *InfoSharing* devono comunicare, con le necessarie garanzie di tutela della riservatezza, tramite la medesima piattaforma *InfoSharing*, gli eventuali attacchi ai propri sistemi informatici entro ventiquattro ore dal momento in cui sono stati rilevati.

ART. 33.

(Livello di sicurezza di base per gli enti privati).

1. Gli enti privati di cui all'articolo 31 della presente legge devono adottare le misure minime definite dall'articolo 34 del codice in materia di protezione dei dati personali, di cui al decreto legislativo 30 giugno 2003, n. 196.

ART. 34.

(Livello di sicurezza medio per gli enti privati).

1. Gli enti privati individuati ai sensi dell'articolo 30, commi 1 e 2, devono adottare le seguenti misure per la sicurezza cibernetica:

a) definire un responsabile della sicurezza cibernetica, dipendente dell'ente privato stesso o di un ente fornitore. All'ente fornitore si applicano in tal caso le disposizioni dell'articolo 30, ove non si trovi nelle condizioni indicate dall'articolo 29;

b) qualora abbiano più di 100 dipendenti, computati indipendentemente dalla forma del rapporto di lavoro instaurato, dotarsi di un SOC, i cui componenti devono essere formati annualmente mediante appositi corsi organizzati dall'Alta scuola;

c) garantire ai dipendenti adibiti a mansioni che prevedono l'impiego di sistemi cibernetici un aggiornamento, almeno annuale, sulla sicurezza cibernetica.

2. Gli oneri di adeguamento derivanti dall'attuazione del comma 1 a carico degli enti privati sono ristorati, anche parzialmente, a valere sul Fondo di cui all'articolo 48.

ART. 35.

(Livello di sicurezza alto per enti privati).

1. Agli enti privati individuati ai sensi dell'articolo 30, commi 1 e 2, che hanno più di mille *host IP* nell'azienda e i cui proventi derivano almeno per il 5 per cento da soggetti aventi sede in uno Stato estero si applicano le disposizioni del medesimo articolo 30. Tali enti devono adottare le seguenti misure per la sicurezza cibernetica:

a) istituire un CERT interno all'ente, che opera secondo i protocolli definiti dal CERT-Nazionale ai sensi dell'articolo 12, comma 3, lettera *a)*;

b) realizzare un sistema di scambio dei dati prioritario e garantito dal CERT-IT tramite la piattaforma *InfoSharing*.

c) assicurare la formazione dei componenti del CERT interno di cui alla lettera *a)* mediante la partecipazione ad appositi corsi organizzati presso l'Alta scuola.

2. Gli oneri di adeguamento derivanti dall'attuazione del comma 1 a carico degli enti privati sono ristorati, anche parzialmente, a valere sul Fondo di cui all'articolo 48.

ART. 36.

(Livello di sicurezza per gli enti privati di interesse strategico).

1. Gli enti privati di cui all'articolo 29, oltre a quanto previsto ai sensi dell'articolo 39, devono:

a) individuare un responsabile per i rapporti con gli organi di cui agli articoli 10, 11, 12, 13 e 14 e, ove necessario, 15;

b) organizzare una squadra di tecnici, con il compito di garantire ininterrottamente l'operatività del CERT.

ART. 37.

(Formazione del personale degli enti privati).

1. Con regolamento emanato con decreto del Presidente della Repubblica, su proposta dei Ministri delle attività produttive e dell'istruzione, dell'università e della ricerca, entro un anno dalla data di entrata in vigore della presente legge, sono disciplinati:

a) l'organizzazione di corsi di formazione di base sulla sicurezza cibernetica presso le Camere di commercio, industria, artigianato e agricoltura sotto la supervisione formativa dell'Alta scuola;

b) la pubblicazione di materiali informativi e la predisposizione di corsi di formazione sulla sicurezza cibernetica fruibili tramite la rete *internet*.

CAPO II

SOVRANITÀ CIBERNETICA

ART. 38.

(Certificazione delle aziende cibernetiche).

1. Presso la Presidenza del Consiglio dei ministri è istituito l'elenco delle imprese certificate per lo sviluppo negli ambiti cibernetici ai fini del mantenimento della sovranità cibernetica. A tali imprese spetta, in via prioritaria, l'accesso alle risorse del Fondo di cui all'articolo 48. La certificazione delle aziende è effettuata dal CERT-Nazionale.

ART. 39.

(Sistemi operativi e software *antivirus per le infrastrutture strategiche).*

1. Entro cinque anni dalla data di entrata in vigore della presente legge, il

Ministero dello sviluppo economico provvede, anche mediante accordi con le imprese certificate di cui all'articolo 38, alla realizzazione di un sistema operativo sovrano, basato su codice libero e aperto, da utilizzare nelle IS informatiche. Il sistema operativo è mantenuto e aggiornato costantemente.

2. Entro tre anni dalla data di entrata in vigore della presente legge, il Ministero dello sviluppo economico provvede, anche mediante accordi con le imprese certificate di cui all'articolo 38, alla realizzazione di un *software* antivirus di protezione sovrano, da utilizzare nelle IS informatiche, distribuito in forma gratuita. Il *software* è mantenuto e aggiornato costantemente.

3. La certificazione della sicurezza cibernetica dei *software* prodotti in Italia è rilasciata dall'ISCOM, su richiesta del produttore. Il rilascio della certificazione è soggetto al pagamento di un contributo nella misura determinata e aggiornata con decreti del Presidente del Consiglio dei ministri, di concerto con il Ministro dello sviluppo economico.

ART. 40.

*(*Hardware *e* firmware*).*

1. Entro dieci anni dalla data di entrata in vigore della presente legge, il Ministero dello sviluppo economico provvede, anche mediante accordi con le imprese certificate di cui all'articolo 38, allo sviluppo di un sistema sovrano di comunicazione e re-indirizzamento dei dati *internet* (IP), costituito da componenti progettati e prodotti in Italia, da utilizzare nelle IS informatiche. Il sistema è mantenuto e aggiornato costantemente utilizzando componenti prodotti esclusivamente da imprese certificate di cui al citato articolo 38.

2. La certificazione relativa alla sicurezza cibernetica degli *hardware* e dei *firmware* prodotti in Italia è rilasciata dall'ISCOM, su richiesta del produttore. Il rilascio della certificazione è soggetto a un contributo nella misura determinata e ag-

giornata con decreti del Presidente del Consiglio dei ministri, di concerto con il Ministro dello sviluppo economico.

ART. 41.

(Ricerca e sviluppo nel settore cibernetico).

1. Il Governo predispone un piano per la ricerca e lo sviluppo nel settore cibernetico, la cui attuazione inizia entro un anno dalla data di entrata in vigore della presente legge, in collaborazione con l'ISCOM e con le università. All'attuazione del piano partecipano, ove possibile, le imprese certificate di cui all'articolo 38.

2. Il Ministro della difesa, anche in collaborazione con le imprese certificate di cui all'articolo 38, redige un piano per la ricerca e lo sviluppo di contromisure cibernetiche in ambito militare.

3. L'attuazione del piano di cui al comma 1 è finanziata a valere sul Fondo di cui all'articolo 48.

ART. 42.

*(*Start-up *e proprietà intellettuale).*

1. Al fine di incrementare la capacità di sviluppo industriale del settore cibernetico nazionale, le imprese *start-up* innovative, come definite dall'articolo 25 del decreto-legge 18 ottobre 2012, n. 179, convertito, con modificazioni, dalla legge 17 dicembre 2012, n. 221, e successive modificazioni, possono accedere alle risorse del Fondo di cui all'articolo 48, secondo le modalità stabilite dal decreto del Presidente del Consiglio dei ministri adottato ai sensi del medesimo articolo.

2. Le imprese di cui al comma 1 sono esonerate dal pagamento dei diritti e di ogni altro onere dovuto per la registrazione dei brevetti relativi ai progetti cibernetici da esse realizzati.

TITOLO V

CONTROLLO PARLAMENTARE, GARANZIA DELLA RISERVATEZZA DEI DATI E PUBBLICITÀ

CAPO I

CONTROLLO PARLAMENTARE

ART. 43.

(Parere delle Commissioni parlamentari).

1. Gli schemi dei decreti previsti dalla presente legge 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 sono 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.

ART. 44.

(Comitato parlamentare per la sicurezza della Repubblica).

1. Il Comitato parlamentare per la sicurezza della Repubblica, di cui all'articolo 30 della legge 3 agosto 2007, n. 124, esercita il controllo parlamentare sull'attività del sistema nazionale di sicurezza cibernetica, verificando che essa si svolga nel rispetto della Costituzione e delle leggi, nell'esclusivo interesse e per la difesa della Repubblica e delle sue istituzioni.

2. Oltre alle audizioni previste dall'articolo 31 della legge 3 agosto 2007, n. 124,

il Comitato parlamentare per la sicurezza della Repubblica ascolta periodicamente il direttore del NSC, il direttore del CERT-IT e il comandante del CERT-Difesa.

CAPO II

TUTELA DELLA RISERVATEZZA

ART. 45.

(Garante per la protezione dei dati personali).

1. Il Garante per la protezione dei dati personali può disporre, ai sensi dell'articolo 157 del codice di cui al decreto legislativo 30 giugno 2003, n. 196, accessi a banche di dati e archivi nonché ispezioni e verifiche nei luoghi ove si svolge il trattamento di dati inerenti alla sicurezza cibernetica.

CAPO III

DIVULGAZIONE E PUBBLICITÀ

ART. 46.

(Relazione alle Camere).

1. Entro il 31 dicembre di ogni anno il Presidente del Consiglio dei ministri presenta alle Camere una relazione sulla sicurezza cibernetica. La relazione è predisposta dal Presidente del Consiglio dei ministri, di concerto con il Ministro della difesa, ed è integrata con i pertinenti elementi di valutazione trasmessi dagli organi di cui agli articoli 10, 11, 12, 13, 14 e 15.

ART. 47.

(Trasparenza e accesso ai dati aggregati sugli eventi cibernetici).

1. Il CERT-IT pubblica nel proprio sito *internet* istituzionale, in formato aperto e

con aggiornamento almeno giornaliero, i dati relativi agli eventi cibernetici non classificati.

2. Agli oneri derivanti dall'attuazione del comma 1 si provvede a carico del Fondo di cui all'articolo 48.

TITOLO VI

DISPOSIZIONI FINANZIARIE, PROCEDURE DI APPROVVIGIONAMENTO E SANZIONI

CAPO I

DISPOSIZIONI FINANZIARIE E PROCEDURE DI APPROVVIGIONAMENTO

ART. 48.

(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, con il Ministro dell'istruzione, dell'università e della ricerca e con il Ministro dell'economia e delle finanze, sono definite le modalità di impiego del fondo di cui al comma 1.

ART. 49.

(Approvvigionamento di servizi, lavori, materiali e strumenti del sistema nazionale di sicurezza cibernetica).

1. Al fine di assicurare il funzionamento ottimale e ininterrotto del sistema nazionale di sicurezza cibernetica, gli organi che lo compongono procedono a un'attenta e puntuale programmazione a

medio e a lungo termine degli approvvigionamenti di servizi, lavori, materiali e strumenti necessari a tale fine.

2. In caso di situazioni di crisi che richiedano il rapido approvvigionamento di servizi, lavori, materiali e strumenti per evitare il rischio di interruzione del servizio o per provvedere all'integrazione della capacità operativa, gli organi che compongono il sistema nazionale di sicurezza cibernetica possono impiegare le procedure disciplinate dal decreto legislativo 15 novembre 2011, n. 208.

3. Per l'approvvigionamento dei servizi, lavori, materiali e strumenti, nei casi di cui al comma 2, gli organi che compongono il sistema nazionale di sicurezza cibernetica, possono accedere alle risorse del Fondo di cui all'articolo 48 per un importo complessivo, riferito a ciascun esercizio finanziario, non eccedente il 10 per cento dell'importo che l'organo stesso ha destinato all'approvvigionamento di servizi, lavori, materiali e strumenti nell'esercizio finanziario precedente e, comunque, non superiore a un milione di euro.

4. L'organo che utilizza risorse del Fondo di cui all'articolo 48 ai sensi del comma 3 del presente articolo deve reintegrare l'importo ricevuto mediante versamento al Fondo, da effettuare entro il secondo esercizio finanziario successivo a quello in corso alla data del prelevamento.

CAPO II

SANZIONI

ART. 50.

*(Introduzione dell'articolo 280-*bis *del codice penale, in materia di terrorismo cibernetico).*

1. Dopo l'articolo 280-*bis* del codice penale è inserito il seguente:

« ART. 280-*ter*. – *(Terrorismo cibernetico)*. – Salvo che il fatto costituisca più grave reato, chiunque, per finalità di ter-

rorismo, anche internazionale, di cui all'articolo 270-*sexies*, provoca un evento cibernetico rilevante, consistente nell'acquisizione e nel trasferimento indebiti di dati, nella loro modifica o distruzione illegittima ovvero nel danneggiamento, nella distruzione o nel blocco del regolare funzionamento delle reti e dei sistemi informativi o dei loro elementi costitutivi, è punito con la reclusione da cinque a dieci anni ».

ART. 51.

(Sanzioni amministrative).

1. Agli enti privati di cui all'articolo 29, in caso di mancato adeguamento alle disposizioni dell'articolo 36, si applica la sanzione amministrativa pecuniaria consistente nel pagamento di una somma non inferiore a 100 mila euro e non superiore a un milione di euro.

2. Agli enti privati individuati ai sensi dell'articolo 30, commi 1 e 2, in caso di mancato adeguamento alle disposizioni dell'articolo 34 e, ricorrendone le condizioni, dell'articolo 35, si applica la sanzione amministrativa pecuniaria consistente nel pagamento di una somma non inferiore a 10 mila euro e non superiore a 100.000 euro.

3. Agli enti di cui all'articolo 31, in caso di mancato adeguamento alle disposizioni dell'articolo 33, si applicano le sanzioni previste dal codice in materia di protezione dei dati personali, di cui al decreto legislativo 30 giugno 2003, n. 196.

4. In caso di violazione della disposizione dell'articolo 32, comma 3, si applica la sanzione amministrativa pecuniaria consistente nel pagamento di una somma non inferiore a 10 mila euro e non superiore a 100 mila euro per ciascuna segnalazione omessa o non inviata nel termine ivi previsto.

5. L'organo competente a ricevere il rapporto e ad irrogare le sanzioni di cui ai commi 1, 2 e 4 è il prefetto competente per territorio. L'organo competente a ricevere il rapporto e ad irrogare le sanzioni di cui al comma 3 è il Garante per la protezione dei dati personali. Si osser-

vano, in quanto applicabili, le disposizioni della legge 24 novembre 1981, n. 689. I proventi delle sanzioni irrogate ai sensi dei commi 1, 2 e 4 sono versati all'entrata del bilancio dello Stato per essere riassegnati al Fondo di cui all'articolo 48.

TITOLO VII

DISPOSIZIONI FINALI

ART. 52.

(Oneri finanziari).

1. Agli oneri derivanti dall'attuazione delle disposizioni della presente legge si provvede mediante corrispondente riduzione del fondo di cui all'articolo 1, comma 965, della legge 28 dicembre 2015, n. 208.

ART. 53.

(Abrogazione).

1. Il decreto del Presidente del Consiglio dei ministri 24 gennaio 2013, pubblicato nella *Gazzetta Ufficiale* n. 66 del 19 marzo 2013, è abrogato.

ART. 54.

(Entrata in vigore).

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

€ 4,00

Stampato su carta riciclata ecologica

17PDL0038430