DECRETO DEL PRESIDENTE DEL CONSIGLIO DEI MINISTRI 24 gennaio 2013

Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionale. (13A02504)

(GU n.66 del 19-3-2013)

IL PRESIDENTE DEL CONSIGLIO DEI MINISTRI

Vista la legge 3 agosto 2007, n. 124, recante "Sistema di

informazione per la sicurezza della Repubblica e nuova disciplina del

segreto", come modificata e integrata dalla legge 7 agosto 2012, n.

133, e, in particolare, l'art. 1, comma 3-bis, che dispone che il

Presidente del Consiglio dei Ministri, sentito il Comitato

interministeriale per la sicurezza della Repubblica, adotti apposite

direttive per rafforzare le attivita' di informazione per la

protezione delle infrastrutture critiche materiali e immateriali, con

particolare riguardo alla protezione cibernetica e alla sicurezza

informatica nazionali, e l'art. 38, comma 1-bis, ai sensi del quale

il Governo allega alla relazione sulla politica dell'informazione per

la sicurezza e sui risultati ottenuti, che presenta annualmente al

Parlamento, un documento di sicurezza nazionale, concernente le

attivita' relative alla protezione delle infrastrutture critiche

materiali e immateriali, nonche' alla protezione cibernetica e alla

sicurezza informatica;

Visto l'art. 4, comma 3, lett. d-bis) della citata legge 3 agosto

2007, n. 124, ai sensi del quale il Dipartimento delle informazioni

per la sicurezza coordina le attivita' di ricerca informativa

finalizzate a rafforzare la protezione cibernetica e la sicurezza

informatica nazionali;

Visto l'articolo 1 della legge 1° aprile 1981, n. 121;

Visti il decreto-legge 27 luglio 2005, n. 144, convertito, con

modificazioni, dalla legge 31 luglio 2005, n. 155, recante misure

urgenti per il contrasto del terrorismo internazionale che,

all'articolo 7-bis, dispone che, ferme restando le competenze dei

Servizi di informazione per la sicurezza, i competenti organi del

Ministero dell'interno assicurano i servizi di protezione informatica

delle infrastrutture critiche informatizzate di interesse nazionale

ed il decreto del Ministro dell'interno 9 gennaio 2008, con il quale

sono state individuate le predette infrastrutture ed e' stata

prevista l'istituzione del Centro nazionale anticrimine informatico

per la protezione delle infrastrutture critiche;

Visti l'art. 14 del decreto legislativo 30 luglio 1999, n. 300,

recante "Riforma dell'organizzazione del Governo, a norma

dell'articolo 11 della legge 15 marzo 1997, n. 59", che attribuisce,

tra l'altro, al Ministero dell'interno competenze in materia di

difesa civile ed il decreto del Ministro dell'interno 28 settembre

2001 che istituisce la Commissione interministeriale tecnica di

difesa civile;

Visti il decreto legislativo 15 marzo 2010, n. 66, recante "Codice dell'ordinamento militare" e, in particolare, l'art. 89 che individua le attribuzioni delle Forze armate e le disposizioni e direttive conseguenti che disciplinano i compiti attinenti alla difesa cibernetica;

Visto il decreto legislativo 1° agosto 2003, n. 259 recante "Codice delle comunicazioni elettroniche" e, in particolare, le disposizioni che affidano al Ministero dello sviluppo economico competenze in materia di sicurezza ed integrita' delle reti pubbliche di comunicazione e dei servizi di comunicazione elettronica accessibili

al pubblico;

Visto il decreto-legge 22 giugno 2012, n. 83, convertito, con

modificazioni, dalla legge 7 agosto 2012, n. 134, che ha istituito

l'Agenzia per l'Italia digitale, cui sono affidate, tra l'altro, le

funzioni attribuite all'Istituto superiore delle comunicazioni e

delle tecnologie dell'informazione in materia di sicurezza delle

reti, nonche' quelle di coordinamento, indirizzo e regolazione gia'

affidate a DigitPA;

Visto il decreto legislativo 7 marzo 2005, n. 82, recante il Codice

dell'amministrazione digitale e, in particolare, le disposizioni in

materia di sicurezza informatica;

Visto il decreto interministeriale 14 gennaio 2003, cosi' come

modificato dal decreto 5 settembre 2011, che ha istituito

l'Osservatorio per la sicurezza delle reti e la tutela delle

comunicazioni;

Vista la legge 24 febbraio 1992, n. 225, recante "Istituzione del

Servizio nazionale della protezione civile;

Visto il decreto legislativo 11 aprile 2011, n. 61, attuativo della

direttiva 2008/114/CE recante l'individuazione e la designazione

delle infrastrutture critiche europee e la valutazione della

necessita' di migliorarne la protezione;

Visto l'art. 5, comma 2, lett. h), della legge 23 agosto 1988, n.

400;

Visto il decreto legislativo 30 luglio 1999, n. 303, recante

"Ordinamento della Presidenza del Consiglio dei Ministri a norma

dell'articolo 11 della legge 15 marzo 1997, n. 59";

Visto il decreto del Presidente del Consiglio dei ministri 1°

ottobre 2012 recante "Ordinamento delle strutture generali della

Presidenza del Consiglio dei Ministri";

Visto il decreto del Presidente del Consiglio dei Ministri 5 maggio

2010, recante l'Organizzazione nazionale per la gestione di crisi;

Vista la mozione approvata in data 23 maggio 2012, con la quale il

Parlamento ha impegnato il Governo a porre in essere ogni idonea

iniziativa per giungere alla costituzione presso la Presidenza del

Consiglio dei Ministri di un Comitato interministeriale con il

compito di elaborare una strategia nazionale per la sicurezza dello

spazio cibernetico, di definire gli indirizzi generali e le direttive

da perseguire nel quadro della politica nazionale ed internazionale

in tale settore e di individuare, infine, gli interventi normativi

ritenuti necessari;

Ritenuto che, in ragione delle caratteristiche della minaccia

cibernetica quale rischio per la sicurezza nazionale, sia necessario

definire un quadro strategico nazionale, con la specificazione dei

ruoli che le diverse componenti istituzionali devono esercitare per

assicurare la sicurezza cibernetica del Paese e la predisposizione di

meccanismi e procedure di azione secondo un approccio

interdisciplinare e coordinato, su piu' livelli, che coinvolga tutti

gli attori pubblici, ferme restando le attribuzioni previste dalla

normativa vigente per ciascuno di essi, nonche' gli operatori privati

interessati;

Ritenuto altresi' necessario creare le condizioni, attraverso la

definizione e precisazione di compiti ed attivita' delle diverse

componenti istituzionali ed anche con l'individuazione di organi

nazionali di riferimento per la sicurezza cibernetica in grado di

interagire con le corrispondenti autorita' estere, affinche' l'Italia

possa partecipare pienamente ai diversi consessi di cooperazione

internazionale, sia in ambito bilaterale e multilaterale, sia dell'UE

e della NATO;

Considerato l'attuale quadro legislativo, improntato alla

distribuzione di funzioni e compiti aventi rilievo per la sicurezza

cibernetica tra molteplici soggetti istituzionali competenti nelle

diverse fasi della prevenzione degli eventi dannosi nello spazio

cibernetico; dell'elaborazione di linee guida e standard tecnici di

sicurezza; della difesa dello Stato da attacchi nello spazio

cibernetico; della prevenzione e repressione dei crimini informatici;

della preparazione e della risposta nei confronti di eventi

cibernetici;

Ritenuto che, sulla base del citato dato normativo, la definizione

di un quadro strategico nazionale in materia di sicurezza cibernetica

debba procedere secondo un percorso di graduale e progressiva

razionalizzazione di ruoli, strumenti e procedure con l'obiettivo di

accrescere la capacita' del Paese di assicurare la sicurezza dello

spazio cibernetico, ove necessario anche con interventi di carattere

normativo;

Ritenuto che, nell'immediato, debbano essere create le condizioni

perche', a legislazione vigente, possa essere sviluppata un'azione

integrata che metta a fattor comune le diverse attribuzioni

istituzionali delineate dal quadro normativo, ed inoltre assicuri, in

una logica di partenariato, il pieno apporto, nel rispetto di quanto

previsto dalla normativa vigente, anche delle competenze proprie

degli operatori privati, interessati alla gestione di sistemi e reti

di interesse strategico;

Ravvisata a tali fini la necessita' di impartire indirizzi

affinche' venga a delinearsi un'architettura istituzionale basata

sulla chiara individuazione dei soggetti chiamati ad intervenire e

dei compiti ad essi affidati, nel rispetto delle competenze gia'

attribuite dalla legge alle diverse componenti e dei meccanismi di

interazione tra di esse;

Ritenuto che tale architettura debba svilupparsi su tre distinti

livelli d'intervento, di cui il primo di indirizzo politico e

coordinamento strategico, cui affidare l'individuazione degli

obiettivi funzionali a garantire la protezione cibernetica e la

sicurezza informatica nazionali, anche attraverso l'elaborazione di

un Piano nazionale per la sicurezza dello spazio cibernetico, e che

tale livello debba anche sovraintendere allo studio e alla

predisposizione di proposte di intervento normativo che agevolino il

raggiungimento dei citati obiettivi; il secondo di supporto, a

carattere permanente, con funzioni di raccordo nei confronti di tutte

le Amministrazioni ed enti competenti, ai fini dell'attuazione degli

obiettivi e delle linee di azione indicate dalla pianificazione

nazionale e che provveda, al contempo, a programmare l'attivita'

operativa a livello interministeriale e ad attivare le procedure di

allertamento in caso di crisi; il terzo livello, di gestione delle

crisi, con il compito di curare e coordinare le attivita' di risposta

e di ripristino della funzionalita' dei sistemi, avvalendosi di tutte

le componenti interessate;

Ritenuto che, nel quadro del livello di supporto all'attuazione

della pianificazione nazionale, debbano essere disciplinate in

maniera peculiare, tenuto conto della loro specificita', le attivita'

di informazione per la sicurezza con l'obiettivo di potenziare le

attivita' di ricerca informativa e di analisi finalizzate a

rafforzare la protezione cibernetica e la sicurezza informatica,

facendo ricorso agli strumenti ed alle procedure di cui alla legge n.

124/2007 e, in particolare, alle direttive del Presidente del

Consiglio ai sensi dell'art. 1, comma 3-bis;

Ritenuto che il modello organizzativo-funzionale cosi' delineato

debba assicurare il pieno raccordo, in particolare, con le funzioni

del Ministero dello sviluppo economico e dell'Agenzia per l'Italia

digitale, nonche' con l'attivita' e le strutture di difesa dello

spazio cibernetico del Ministero della difesa, con quelle del

Ministero dell'interno, dedicate alla prevenzione e al contrasto del

crimine informatico e alla difesa civile, e con quelle della

protezione civile;

Considerato che la legge attribuisce al Comitato interministeriale

per la sicurezza della Repubblica (CISR) di cui all'articolo 5 della

legge n. 124/2007 compiti di consulenza, proposta e deliberazione

sugli indirizzi e sulle finalita' generali della politica

dell'informazione per la sicurezza, nonche' di elaborazione degli

indirizzi generali e degli obiettivi fondamentali da perseguire nel

quadro della politica dell'informazione per la sicurezza e che, in

particolare, ai sensi dell'art. 1, comma 3-bis, della predetta legge,

introdotto dalla legge n. 133/2012, il CISR e' sentito ai fini

dell'adozione da parte del Presidente del Consiglio dei ministri

delle direttive in materia di sicurezza cibernetica;

Ravvisata l'esigenza di dover assicurare, nella materia della

sicurezza cibernetica, un solido e affidabile meccanismo di raccordo

tra la politica dell'informazione per la sicurezza e gli altri ambiti

di azione che vengono in rilievo nella specifica materia, e di dovere

per questo concentrare in un unico organismo interministeriale

l'organo di indirizzo politico e di coordinamento strategico nel

campo della sicurezza cibernetica;

Ritenuto in considerazione dei compiti attribuiti dalla legge al

CISR e della composizione del Comitato, di individuare tale organismo

interministeriale nello stesso CISR, attribuendogli, ai sensi

dell'art. 5, comma 2, lett. h) della legge 23 agosto 1988, n. 400, i

compiti suindicati;

Ritenuto che il CISR, nell'esercizio delle citate funzioni, debba

essere adeguatamente e costantemente supportato da una attivita'

istruttoria, di approfondimento e di valutazione e che a tali fini il

Comitato interministeriale possa avvalersi dell'organismo collegiale

di coordinamento istituito presso il DIS, ai sensi dell'art. 4, comma

5, del DPCM 26 ottobre 2012, n. 2, recante l'organizzazione ed il

funzionamento del Dipartimento delle informazione per la sicurezza;

Ritenuto altresi' che per un efficace assolvimento dei compiti

attribuiti al CISR sia necessario assicurare un qualificato

contributo di carattere scientifico di informazione, di valutazione e

di proposta e che, per questo, appare opportuno istituire presso la

Scuola di formazione del DIS un organo dedicato, cui affidare anche

compiti funzionali alla promozione e diffusione di una cultura della

sicurezza cibernetica;

Ravvisata la necessita', ai fini dell'attuazione delle linee di

intervento contenute nel Piano nazionale di sicurezza dello spazio

cibernetico, in particolare per cio' che riguarda la preparazione e

la pianificazione interministeriale per la gestione delle crisi, che

parallelamente alle attivita' di acquisizione informativa e di

analisi demandate agli organismi informativi di cui alla legge n.

124/2007, le attivita' delle diverse Amministrazioni ed enti svolte

secondo le previsioni normative trovino una sede di raccordo che

agevoli e favorisca lo svolgimento in forma coordinata delle

attribuzioni di ciascuna componente;

Ritenuto a tale scopo, di prevedere la costituzione in via

permanente di un Nucleo per la sicurezza cibernetica, da istituire

presso l'Ufficio del Consigliere militare del Presidente del

Consiglio dei Ministri;

Ritenuto infine, che una ulteriore e specifica esigenza di

coordinamento si ponga con riguardo alla gestione operativa delle

crisi e all'adozione delle misure necessarie al ripristino della

funzionalita' dei sistemi, richiedendo la chiara definizione di ruoli

e procedure in modo da garantire un processo decisionale unitario e,

al contempo, l'interazione degli organi nazionali preposti alla

gestione dell'emergenza con gli omologhi organismi esistenti a

livello internazionale, e che, per le suddette finalita', debba

essere previsto un organo interministeriale da attivare in caso di

crisi;

Ritenuto di individuare tale organo nel Nucleo interministeriale

situazione e pianificazione di cui al DPCM 5 maggio 2010,

prevedendone una configurazione, quale "Tavolo interministeriale di

crisi cibernetica", funzionale all'ottimale gestione delle crisi di

natura cibernetica, e di disporre che detto organo, per gli aspetti

tecnici di computer emergency response, si avvalga del CERT nazionale

istituito presso il Ministero dello sviluppo economico ai sensi del

decreto legislativo n. 259/2003;

Sentito il Comitato interministeriale per la sicurezza della

Repubblica;

Dispone:

Art. 1

Oggetto

1. Il presente decreto definisce, in un contesto unitario e

integrato, l'architettura istituzionale deputata alla tutela della

sicurezza nazionale relativamente alle infrastrutture critiche

materiali e immateriali, con particolare riguardo alla protezione

cibernetica e alla sicurezza informatica nazionali, indicando a tal

fine i compiti affidati a ciascuna componente ed i meccanismi e le

procedure da seguire ai fini della riduzione della vulnerabilita',

della prevenzione dei rischi, della risposta tempestiva alle

aggressioni e del ripristino immediato della funzionalita' dei

sistemi in caso di crisi.

2. I soggetti compresi nell'architettura istituzionale di cui al

comma 1 operano nel rispetto delle competenze gia' attribuite dalla

legge a ciascuno di essi.

3. Il modello organizzativo-funzionale delineato con il presente

decreto persegue la piena integrazione con le attivita' di competenza

del Ministero dello sviluppo economico e dell'Agenzia per l'Italia

digitale, nonche' con quelle espletate dalle strutture del Ministero

della difesa dedicate alla protezione delle proprie reti e sistemi

nonche' alla condotta di operazioni militari nello spazio

cibernetico, dalle strutture del Ministero dell'interno, dedicate

alla prevenzione e al contrasto del crimine informatico e alla difesa

civile, e quelle della protezione civile.

Art. 2

Definizioni

1. Ai fini del presente decreto si intende per:

a) Presidente: il Presidente del Consiglio dei Ministri;

b) CISR: il Comitato interministeriale per la sicurezza della

Repubblica di cui all'art. 5 della legge n. 124/2007;

c) DIS: il Dipartimento delle informazioni per la sicurezza di

cui all'art. 4 della legge n. 124/2007;

d) Agenzie: l'Agenzia informazioni e sicurezza esterna e

l'Agenzia informazioni e sicurezza interna di cui agli articoli 6 e

7, della legge 3 agosto 2007, n. 124;

e) organismi di informazione per la sicurezza: il DIS, l'AISE e

l'AISE di cui agli articoli 4, 6 e 7 della legge 3 agosto 2007, n.

124;

f) NISP: Nucleo interministeriale situazione e pianificazione di

cui al DPCM 5 maggio 2010;

g) Consigliere militare: il Consigliere militare del Presidente

del Consiglio dei Ministri di cui all'articolo 11 del DPCM 1° ottobre

2012;

h) spazio cibernetico: l'insieme delle infrastrutture

informatiche interconnesse, comprensivo di hardware, software, dati

ed utenti, nonche' delle relazioni logiche, comunque stabilite, tra

di essi;

i) sicurezza cibernetica: condizione per la quale lo spazio

cibernetico risulti protetto grazie all'adozione di idonee misure di

sicurezza fisica, logica e procedurale rispetto ad eventi, di natura

volontaria od accidentale, consistenti nell'acquisizione e nel

trasferimento indebiti di dati, nella loro modifica o distruzione

illegittima, ovvero nel danneggiamento, distruzione o blocco del

regolare funzionamento delle reti e dei sistemi informativi o dei

loro elementi costitutivi;

l) minaccia cibernetica: 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 o organizzazioni,

statuali e non, pubbliche o private, finalizzate all'acquisizione e

al trasferimento indebiti di dati, alla loro modifica o distruzione

illegittima, ovvero a danneggiare, distruggere o ostacolare il

regolare funzionamento delle reti e dei sistemi informativi o dei

loro elementi costitutivi;

m) evento cibernetico: avvenimento significativo, di natura

volontaria od accidentale, consistente nell'acquisizione e nel

trasferimento indebiti di dati, nella loro modifica o distruzione

illegittima, ovvero nel danneggiamento, distruzione o blocco del

regolare funzionamento delle reti e dei sistemi informativi o dei

loro elementi costitutivi;

n) allarme: comunicazione di avviso di evento cibernetico da

valutarsi ai fini dell'attivazione di misure di risposta pianificate;

o) situazione di crisi: situazione in cui l'evento cibernetico

assume dimensioni, intensita' o natura tali da incidere sulla

sicurezza nazionale o da non poter essere fronteggiato dalle singole

amministrazioni competenti in via ordinaria ma con l'assunzione di

decisioni coordinate in sede interministeriale.

Art. 3

Presidente del Consiglio dei Ministri

1. Il Presidente:

a) adotta, curandone l'aggiornamento, su proposta del CISR, il

quadro strategico nazionale per la sicurezza dello spazio

cibernetico, contenente l'indicazione dei profili e delle tendenze

evolutive delle minacce e delle vulnerabilita' dei sistemi e delle

reti di interesse nazionale, la definizione dei ruoli e dei compiti

dei diversi soggetti, pubblici e privati, e di quelli nazionali

operanti al di fuori del territorio del Paese, l'individuazione degli

strumenti e delle procedure con cui perseguire l'accrescimento della

capacita' del Paese di prevenzione e risposta rispetto ad eventi

nello spazio cibernetico, anche in un'ottica di diffusione della

cultura della sicurezza;

b) adotta, su deliberazione del CISR, il 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;

c) emana le direttive ed ogni atto d'indirizzo necessari per

l'attuazione del Piano di cui alla lettera b);

d) impartisce, sentito il CISR, le direttive al DIS e alle

Agenzie ai sensi dell'art. 1, comma 3-bis, della legge n. 124/2007.

Art. 4

Comitato interministeriale per la sicurezza della Repubblica

1. Nella materia della sicurezza dello spazio cibernetico, il CISR,

nella composizione prevista dall'art. 5, comma 3, della legge n.

124/2007:

a) propone al Presidente l'adozione del quadro strategico

nazionale di cui all'art. 3, comma 1, lett. a);

b) delibera il Piano nazionale per la sicurezza dello spazio

cibernetico di cui all'art. 3, comma 1, lett. b), ai fini

dell'adozione da parte del Presidente;

c) esprime parere, ai sensi dell'art. 5, comma 2, lett. h), della

legge n. 400/1988, sulle direttive del Presidente di cui all'art. 3,

comma 1, lett. c);

d) e' sentito, ai sensi dell'art. 1, comma 3-bis, della legge 3

agosto 2007, n. 124, ai fini dell'adozione delle direttive del

Presidente agli organismi di informazione per la sicurezza;

e) esercita l'alta sorveglianza sull'attuazione del Piano

nazionale per la sicurezza dello spazio cibernetico;

f) approva linee di indirizzo per favorire l'efficace

collaborazione tra i soggetti istituzionali e gli operatori privati

interessati alla sicurezza cibernetica, nonche' per la condivisione

delle informazioni e per l'adozione di best pratices e di misure

rivolte all'obiettivo della sicurezza cibernetica;

g) elabora, ai sensi dell'art. 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) promuove 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 e multilaterale, sia dell'UE e della NATO, al fine della

definizione e adozione di politiche e strategie comuni di prevenzione

e risposta;

i) formula le proposte di intervento normativo ed organizzativo

ritenute necessarie al fine del potenziamento delle misure di

prevenzione e di risposta alla minaccia cibernetica e quelle per la

gestione delle crisi;

l) partecipa, con funzioni di consulenza e di proposta, alle

determinazioni del Presidente in caso di crisi.

2. Alle riunioni del CISR aventi ad oggetto la materia della

sicurezza cibernetica partecipa, senza diritto di voto, il

Consigliere militare.

3. Si applicano, anche ai fini di cui al comma 2, le disposizioni

dell'art. 5, commi 4 e 5, della legge 3 agosto 2007, n. 124.

Art. 5

Organismo di supporto al CISR

1. Alle attivita' di supporto per lo svolgimento da parte del CISR

delle funzioni di cui all'articolo 4 del presente decreto, provvede

l'organismo collegiale di coordinamento, presieduto dal Direttore

generale del DIS, nella composizione di cui all'art. 4, comma 5, del

DPCM 26 ottobre 2012, n. 2, recante l'organizzazione ed il

funzionamento del Dipartimento delle informazione per la sicurezza.

2. Alle riunioni dell'organismo collegiale di coordinamento

riguardanti la materia della sicurezza cibernetica partecipa il

Consigliere militare.

3. L'organismo collegiale di coordinamento di cui al comma 1:

a) svolge attivita' preparatoria delle riunioni del CISR dedicate

alla materia della sicurezza cibernetica;

b) assicura l'istruttoria per l'adozione degli atti e per

l'espletamento delle attivita', da parte del CISR, di cui

all'articolo 4, comma 1, del presente decreto;

c) espleta le attivita' necessarie a verificare l'attuazione

degli interventi previsti dal Piano nazionale per la sicurezza dello

spazio cibernetico e l'efficacia delle procedure di coordinamento tra

i diversi soggetti, pubblici e privati, chiamati ad attuarli;

d) coordina, in attuazione degli indirizzi approvati dal CISR e

sulla base degli elementi forniti dalle Amministrazioni ed enti

competenti, dagli organismi di informazione per la sicurezza, dal

Nucleo per la sicurezza cibernetica di cui all'art. 8 e dagli

operatori privati, nonche' avvalendosi del comitato scientifico di

cui all'art. 6, la formulazione delle indicazioni necessarie allo

svolgimento delle attivita' di individuazione delle minacce alla

sicurezza dello spazio cibernetico, al riconoscimento delle

vulnerabilita', nonche' per l'adozione di best practices e misure di

sicurezza;

4. Per le finalita' di cui al comma 3, l'organismo collegiale di

coordinamento compie approfondimenti ed acquisisce ogni utile

contributo e valutazione ritenuti necessari.

Art. 6

Comitato scientifico

1. Presso la Scuola di formazione di cui all'art. 11 della legge n.

124/2007 e' istituito un comitato scientifico composto da esperti nel

campo delle discipline d'interesse ai fini della sicurezza

cibernetica provenienti dalle universita', dagli enti di ricerca,

dalle pubbliche amministrazioni e dal settore privato, con il compito

di predisporre ipotesi di intervento rivolte a migliorare gli

standard ed i livelli di sicurezza dei sistemi e delle reti, nel

quadro delle azioni finalizzate ad incrementare le condizioni di

sicurezza dello spazio cibernetico d'interesse del Paese, al fine di

assicurare ogni necessario contributo per lo svolgimento delle

attivita' spettanti rispettivamente all'organismo collegiale di

coordinamento di cui all'articolo 5 ed al Nucleo per la sicurezza

cibernetica di cui all'articolo 8, nel campo della prevenzione e

della preparazione ad eventuali situazioni di crisi.

2. Il comitato formula altresi' proposte e progetti di promozione e

diffusione della cultura della sicurezza nel settore cibernetico.

Art. 7

Organismi di informazione per la sicurezza

1. Il DIS e le Agenzie svolgono la propria attivita' nel campo

della sicurezza cibernetica avvalendosi degli strumenti e secondo le

modalita' e le procedure stabilite dalla legge n. 124/2007.

2. Per le finalita' di cui al comma 1, il Direttore generale del

DIS, sulla base delle direttive adottate dal Presidente ai sensi

dell'art. 1, comma 3-bis, della legge n. 124/2007 e alla luce degli

indirizzi generali e degli obiettivi fondamentali individuati dal

CISR, cura, ai sensi dell'art. 4, comma 3, lett. d-bis), della citata

legge, il coordinamento delle attivita' di ricerca informativa

finalizzate a rafforzare la protezione cibernetica e la sicurezza

informatica nazionali.

3. Il DIS, attraverso i propri uffici, assicura il supporto al

Direttore generale per l'espletamento delle attivita' di

coordinamento di cui al comma 2. Il DIS provvede, altresi', sulla

base delle informazioni acquisite ai sensi dell'art. 4, comma 3,

lett. c), alla luce delle acquisizioni provenienti dallo scambio

informativo di cui all'art. 4, comma 3, lett. e), della legge n.

124/2007, e dei dati acquisiti ai sensi dell'art. 13, commi 1 e 2,

della citata legge, alla formulazione di analisi, valutazioni e

previsioni sulla minaccia cibernetica. Provvede, in base a quanto

disposto dal presente decreto, alla trasmissione di informazioni

rilevanti ai fini della sicurezza cibernetica al Nucleo per la

sicurezza cibernetica di cui all'art. 8, alle pubbliche

amministrazioni e agli altri soggetti, anche privati, interessati

all'acquisizione di informazioni, ai sensi dell'art. 4, comma 3,

lett. f) della legge n. 124/2007.

4. Le Agenzie, ciascuna nell'ambito delle rispettive attribuzioni,

svolgono, secondo gli indirizzi definiti dalle direttive del

Presidente e le linee di coordinamento delle attivita' di ricerca

informativa stabilite dal Direttore generale del DIS ai sensi del

comma 2, le attivita' di ricerca e di elaborazione informativa

rivolte alla protezione cibernetica e alla sicurezza informatica

nazionali.

5. Per lo svolgimento delle attivita' previste dal presente

articolo, il DIS e le Agenzie corrispondono con le pubbliche

amministrazioni, i soggetti erogatori di servizi di pubblica

utilita', le universita' e con gli enti di ricerca, stipulando a tal

fine apposite convenzioni ai sensi dell'art. 13, comma 1, della legge

n. 124/2007. Per le stesse finalita', le pubbliche amministrazioni ed

i soggetti erogatori di servizi di pubblica utilita' consentono

l'accesso del DIS e delle Agenzie ai propri archivi informatici

secondo le modalita' e con le procedure previste dal DPCM n. 4/2009,

adottato ai sensi dell'art. 13, comma 2, della predetta legge.

6. Il DIS, ai sensi dell'art. 4, comma 3, lett. m), della legge n.

124/2007, pone in essere ogni iniziativa volta a promuovere e

diffondere la conoscenza e la consapevolezza in merito ai rischi

derivanti dalla minaccia cibernetica e sulle misure necessarie a

prevenirli, anche sulla base delle indicazioni del comitato

scientifico di cui all'art. 6.

Art. 8

Nucleo per la sicurezza cibernetica

1. Presso l'Ufficio del Consigliere militare e' costituito, in via

permanente, il Nucleo per la sicurezza cibernetica, a supporto del

Presidente, nella materia della sicurezza dello spazio cibernetico,

per gli aspetti relativi alla prevenzione e preparazione ad eventuali

situazioni di crisi e per l'attivazione delle procedure di

allertamento.

2. Il Nucleo e' presieduto dal Consigliere militare ed e' composto

da un rappresentante rispettivamente del DIS, dell'AISE, dell'AISI,

del Ministero degli affari esteri, del Ministero dell'interno, del

Ministero della difesa, del Ministero dello sviluppo economico, del

Ministero dell'economia e delle finanze, del Dipartimento della

protezione civile e dell'Agenzia per l'Italia digitale. Per gli

aspetti relativi alla trattazione di informazioni classificate il

Nucleo e' integrato da un rappresentante dell'Ufficio centrale per la

segretezza di cui all'articolo 9 della legge n. 124/2007.

3. I componenti possono farsi assistere alle riunioni da altri rappresentanti delle rispettive amministrazioni in relazione alle materie oggetto di trattazione ed, in particolare, per le esigenze di raccordo di cui all'art. 9, comma 2, lett. a).

4. In relazione agli argomenti delle riunioni possono anche essere chiamati a partecipare rappresentanti di altre amministrazioni, di universita' o di enti e istituti di ricerca, nonche' di operatori privati interessati alla materia della sicurezza cibernetica.

5. Il Nucleo per la sicurezza cibernetica si riunisce almeno una volta al mese, su iniziativa del Consigliere militare o su richiesta

di almeno un componente del Nucleo.

Art. 9

Compiti del Nucleo per la sicurezza cibernetica

1. Per le finalita' di cui all'art. 8, comma 1, del presente

decreto, il Nucleo per la sicurezza cibernetica svolge funzioni di

raccordo tra le diverse componenti dell'architettura istituzionale

che intervengono a vario titolo nella materia della sicurezza

cibernetica, nel rispetto delle competenze attribuite dalla legge a

ciascuna di esse.

2. In particolare, nel campo della prevenzione e della preparazione

ad eventuali situazioni di crisi, il Nucleo per la sicurezza

cibernetica:

a) promuove, sulla base delle direttive di cui all'articolo 3,

comma 1, lett. c), la programmazione e la pianificazione operativa

della risposta a situazioni di crisi cibernetica da parte delle

amministrazioni e degli operatori privati interessati e

l'elaborazione delle necessarie procedure di coordinamento

interministeriale, in raccordo con le pianificazioni di difesa civile

e di protezione civile;

b) mantiene attivo, 24 ore su 24, 7 giorni su 7, l'unita' per

l'allertamento e la risposta a situazioni di crisi cibernetica;

c) valuta e promuove, in raccordo con le amministrazioni

competenti per specifici profili della sicurezza cibernetica, e

tenuto conto di quanto previsto dall'art. 7 riguardo all'attivita'

degli organismi di informazione per la sicurezza, 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;

d) acquisisce, per il tramite del Ministero dello sviluppo

economico, degli organismi di informazione per la sicurezza, delle

Forze di polizia e delle strutture del Ministero della difesa, le

comunicazioni circa i casi di violazioni o tentativi di violazione

della sicurezza o di perdita dell'integrita' significativi ai fini

del corretto funzionamento delle reti e dei servizi;

e) promuove e coordina, in raccordo con il Ministero dello

sviluppo economico e con l'Agenzia per l'Italia digitale per i

profili di rispettiva competenza, lo svolgimento di esercitazioni

interministeriali, ovvero la partecipazione nazionale in

esercitazioni internazionali che riguardano la simulazione di eventi

di natura cibernetica;

f) costituisce punto di riferimento nazionale per i rapporti con

l'ONU, la NATO, l'UE, altre organizzazioni internazionali ed altri

Stati, ferme restando le specifiche competenze del Ministero dello

sviluppo economico, del Ministero degli affari esteri, del Ministero

dell'interno, del Ministero della difesa e di altre amministrazioni

previste dalla normativa vigente, assicurando comunque in materia

ogni necessario raccordo.

3. Ai fini dell'attivazione delle azioni di risposta e ripristino

rispetto a situazioni di crisi cibernetica, il Nucleo:

a) riceve, anche dall'estero, le segnalazioni di evento

cibernetico e dirama gli allarmi alle amministrazioni e agli

operatori privati, ai fini dell'attuazione di quanto previsto nelle

pianificazioni di cui al comma 2, lett. a);

b) valuta se l'evento assume dimensioni, intensita' o natura tali

da incidere sulla sicurezza nazionale o non puo' essere fronteggiato

dalle singole amministrazioni competenti in via ordinaria, ma

richiede l'assunzione di decisioni coordinate in sede

interministeriale, provvedendo, ove necessario, a dichiarare la

situazione di crisi cibernetica e ad attivare il NISP, quale Tavolo

interministeriale di crisi cibernetica, informando tempestivamente il

Presidente sulla situazione in atto.

4. Il Nucleo per la sicurezza cibernetica elabora appositi report

sullo stato di attuazione delle misure di coordinamento ai fini della

preparazione e gestione della crisi previste dal presente decreto e

li trasmette, per le finalita' di cui all'articolo 5, comma 3, lett.

c), all'organismo collegiale di cui all'articolo 5.

Art. 10

NISP – Tavolo interministeriale di crisi cibernetica

1. Il NISP, quale Tavolo interministeriale di crisi cibernetica, e'

attivato dal Nucleo per la sicurezza cibernetica ai sensi

dell'articolo 9, comma 3, lett. b).

2. Il Tavolo, presieduto dal Consigliere militare, opera con la

presenza di un rappresentante per ciascuna delle amministrazioni

indicate dall'art. 5, comma 3, del DPCM 5 maggio 2010 e di un

rappresentante rispettivamente del Ministero dello sviluppo economico

e dell'Agenzia per l'Italia digitale, autorizzati ad assumere

decisioni che impegnano la propria amministrazione. Alle riunioni i

componenti possono farsi accompagnare da altri funzionari della

propria amministrazione. Alle stesse riunioni possono essere chiamati

a partecipare rappresentanti di soggetti ed enti di cui all'art. 5,

comma 6, del DPCM 5 maggio 2010, nonche' degli operatori privati di

cui all'art. 11 del presente decreto, e di altri eventualmente

interessati.

3. E' compito del Tavolo interministeriale di crisi cibernetica

assicurare che le attivita' di reazione e stabilizzazione di

competenza delle diverse Amministrazioni ed enti rispetto a

situazioni di crisi di natura cibernetica, vengano espletate in

maniera coordinata secondo quanto previsto dalle pianificazioni di

cui all'art. 9, comma 2, lett. a), avvalendosi, per gli aspetti

tecnici di risposta sul piano informatico e telematico, del Computer

Emergency Response Team (CERT) nazionale, istituito presso il

Ministero dello sviluppo economico.

4. Il Tavolo altresi':

a) mantiene costantemente informato il Presidente sulla crisi in

atto, predisponendo punti aggiornati di situazione;

b) assicura il coordinamento per l'attuazione a livello

interministeriale delle determinazioni del Presidente per il

superamento della crisi;

c) raccoglie tutti i dati relativi alla crisi;

d) elabora rapporti e fornisce informazioni sulla crisi e li

trasmette ai soggetti pubblici e privati interessati;

e) assicura i collegamenti finalizzati alla gestione della crisi

con gli omologhi organismi di altri Stati, della NATO, dell'UE o di

organizzazioni internazionali di cui l'Italia fa parte.

Art. 11

Operatori privati

1. Gli operatori privati che forniscono reti pubbliche di

comunicazione o servizi di comunicazione elettronica accessibili al

pubblico, quelli che gestiscono infrastrutture critiche di rilievo

nazionale ed europeo, il cui funzionamento e' condizionato

dall'operativita' di sistemi informatici e telematici, ivi comprese

quelle individuate ai sensi dell'art. 1, comma 1, lett. d), del

decreto del Ministro dell'interno 9 gennaio 2008, secondo quanto

previsto dalla normativa vigente, ovvero previa apposita convenzione:

a) comunicano al Nucleo per la sicurezza cibernetica, anche per

il tramite dei soggetti istituzionalmente competenti a ricevere le

relative comunicazioni ai sensi dell'art. 16-bis, comma 2, lett. b),

del decreto legislativo n. 259/2003, ogni significativa violazione

della sicurezza o dell'integrita' dei propri sistemi informatici,

utilizzando canali di trasmissione protetti;

b) adottano le best practices e le misure finalizzate

all'obiettivo della sicurezza cibernetica, definite ai sensi

dell'art. 16-bis, comma 1, lett. a), del decreto legislativo n.

259/2003, e dell'art. 5, comma 3, lett. d), del presente decreto;

c) forniscono informazioni agli organismi di informazione per la

sicurezza e consentono ad essi l'accesso alle banche dati d'interesse

ai fini della sicurezza cibernetica di rispettiva pertinenza, nei

casi previsti dalla legge n. 124/2007;

d) collaborano alla gestione delle crisi cibernetiche

contribuendo al ripristino della funzionalita' dei sistemi e delle

reti da essi gestiti.

Art. 12

Tutela delle informazioni

1. Per lo scambio delle informazioni classificate si osservano le

disposizioni di cui al DPCM 22 luglio 2011, n. 4 recante disposizioni

per la tutela amministrativa del segreto di Stato e delle

informazioni classificate.

2. Il DIS, attraverso l'Ufficio centrale per la segretezza,

assolve, altresi', ai compiti di cui al DPCM 22 luglio 2011, n. 4,

relativi alla tutela dei sistemi EAD delle pubbliche amministrazioni

e degli operatori privati di cui all'art. 11 del presente decreto,

che trattano informazioni classificate.

Art. 13

Disposizioni finali

1. Dal presente decreto non derivano nuovi oneri a carico del

bilancio dello Stato.

2. Il presente decreto e' pubblicato nella Gazzetta Ufficiale della

Repubblica italiana.

Roma, 24 gennaio 2013

Il Presidente del Consiglio dei Ministri

Monti

Il Ministro della difesa

Di Paola

Il Ministro dell'economia e delle finanze

Grilli

Il Ministro dell'interno

Cancellieri

Il Ministro dello sviluppo economico

e delle infrastrutture e dei trasporti

Passera

Il Ministro degli affari esteri

Terzi di Sant'Agata

Il Ministro della giustizia

Severino

Registrato alla Corte dei conti l'11 marzo 2013

Presidenza del Consiglio dei Ministri, registro n. 2, foglio n. 267