DPCM 17 febbraio 2017 (GU n.87 del 13-4-2017)
Pubblicato sulla Gazzetta Ufficiale il DPCM che sostituisce quello del 24 gennaio 2013 che innova la struttura .organizzativa statale al fine di una razionalizzazione e migliore definizione delle competenze e dell'assetto istituzionale.

di Andrea Chittaro e Roberto Setola

NUOVA DIRETTIVA PER LA PROTEZIONE CIBERNETICA E LA SICUREZZA INFORMATICA

Andrea CHITTARO è responsabile della Corporate Security di SNAM. Fa parte del Consiglio direttivo dell'Associazione Italiana Professionisti della Security Aziendale (AIPSA). È docente e membro del Comitato Scientifico presso il Master in Homeland Security dell'Università Campus Biomedico e presso del Corso di formazione per professionisti della Security Aziendale dell'Università Vita e salute S. Raffaele di Milano.

Roberto SETOLA è professore associato (settore ING-INF/04 Automatica) presso l'Università Campus BioMedico di Roma dove ricopre anche il ruolo di Direttore del Laboratori Sistemi Complessi e Sicurezza. È il Direttore Scientifico del Master universitario di II livello in "Homeland Security: Sistemi, Metodi e Strumenti per la Security ed in Crisis Management".

Il nuovo DPCM sulla cyber security (che continua ad essere indicata in maniera non del tutto appropriata come protezione cibernetica) nasce dalla esigenza, chiarita nelle premesse dello stesso DPCM, di "razionalizzare e semplificare l'architettura istituzionale" delineata con analogo provvedimento del 2013 con l'obiettivo di "migliorare le funzioni di coordinamento e raccordo".

In estrema sintesi, le principali modifiche riguardano il maggior ruolo assunto dal Nucleo per la Sicurezza Cibernetica, che diviene un hub attivo h24, nonché il soggetto deputato a gestire situazioni di crisi, assorbendo, nella sostanza, quelli che erano i compiti del NISP nel precedente DPCM. Inoltre il Nucleo, nella nuova formulazione, trova collocazione all'interno del Dipartimento delle informazioni per la sicurezza (DIS) ed è presieduto da un Vice Direttore dello stesso organo. Tali cambiamenti si traducono in una semplificazione dell'organizzazione e in uno spostamento del baricentro della tematica all'interno del DIS, superando la centralità dell'Ufficio del Consigliere Militare che da molti era considerata una anomalia. Infine è istituito presso il MISE un "centro di valutazione e certificazione nazionale" per i sistemi destinati ad essere utilizzati per il funzionamento di reti, servizi e infrastrutture critiche aspetto, questo, che appare non del tutto immune da problematicità. Alcune criticità persistono anche nei criteri che stabiliscono le modalità di individuazione e coinvolgimento dei soggetti privati. Su questo punto, infatti, le uniche modifiche introdotte dal nuovo DPCM riguardano l'inclusione fra gli "operatori privati" anche di quelli individuati dalla direttiva NIS (Directive UE/2016/1148) intervento che, come meglio illustrato in seguito, non sembra contribuire ad una puntuale definizione di chi siano gli interlocutori privati e le modalità di interazione di questi con la componente pubblica.

L'art. 1, che risulta sostanzialmente immutato rispetto all'analogo provvedimento del 2013, individua quale oggetto del DPCM la definizione dell'architettura istituzionale che, in un contesto unitario, sia deputata alla sicurezza nazionale delle infrastrutture critiche materiali e immateriali. In questo quadro, il DPCM mira a definire una prospettiva funzionale all'innalzamento della resilienza di tali infrastrutture, operando non solo sulla prevenzione delle minacce e sulla riduzione delle vulnerabilità ma anche sulla tempestività della risposta e sulla capacità di rapido ripristino delle funzionalità.

È singolare però che nell'ambito delle definizioni di cui all'art. 2, manchi del tutto il riferimento a cosa vada inteso per "infrastruttura critica". L'art. 2, di converso, introduce, la figura degli "*operatori di servizi essenziali*", derivata dalla direttiva NIS. Un tale approccio lascia presagire, in meri termini ipotetici, che il legislatore abbia voluto individuare una qualche sorta di correlazione fra gli operatori di servizi essenziali e le infrastrutture critiche e che si potrà trovare una adeguata sintesi nell'ambito dell'iter legislativo per il recepimento della NIS (il cui termine è previsto per luglio del 2018).
Il nuovo assetto, come illustrato nella figura 1, conserva l'impostazione del precedente DPCM e vede la responsabilità politica in capo al Presidente del Consiglio, quale responsabile ultimo della sicurezza nazionale anche nello spazio cibernetico.

In questa sua veste il Presidente del Consiglio presiede il **CISR** (*Comitato Interministeriale per la Sicurezza della Repubblica*) e adotta e aggiorna il *quadro strategico nazionale per la sicurezza dello spazio cibernetico* e *il piano nazionale per la protezione cibernetica e la sicurezza informatica nazionale* (quest'ultimo recentemente aggiornato e pubblicato sulla GU del 31 maggio 2017).

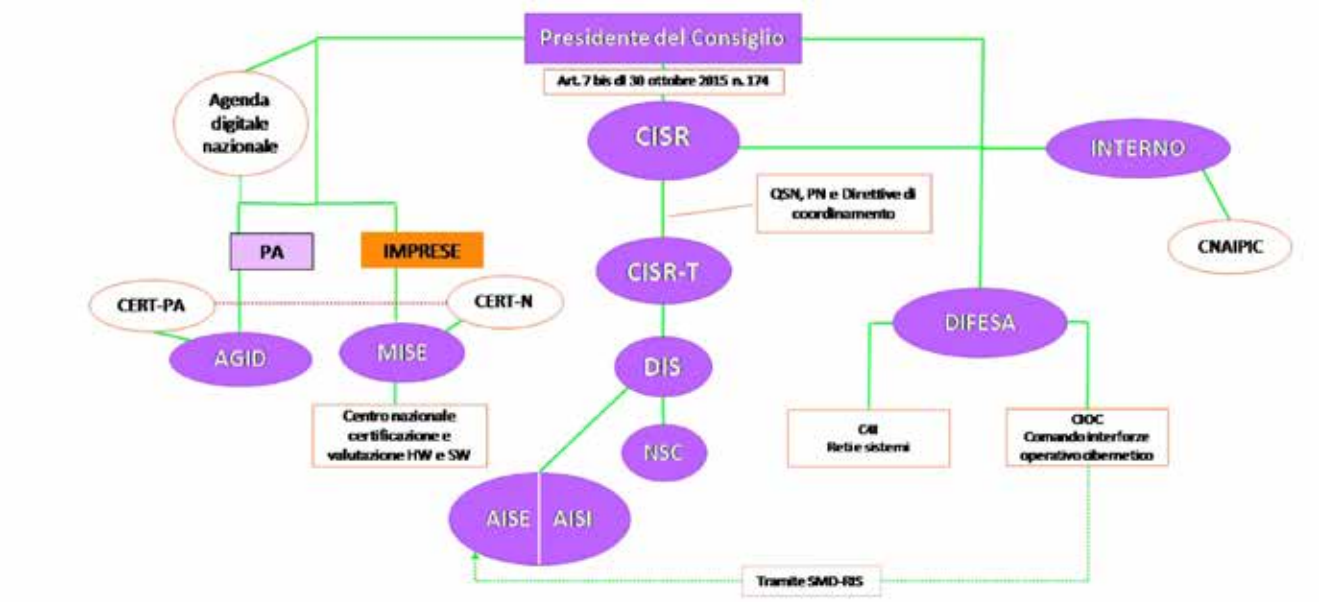

Figura 1 *- ARCHITETTURA NAZIONALE CYBER (Fonte Piano Nazionale per la Protezione Cibernetica e la Sicurezza Informatica, Marzo 2017)*

A supporto del CISR opera un organismo collegiale di supporto (ora denominato "***CISR tecnico***"), che posto sotto la guida del Direttore generale del DIS diviene il vero punto di coordinamento e di raccordo fra gli indirizzi politici e strategici definiti dal CISR e le diverse strutture operative. In questa sua veste il Direttore del DIS adotta le "***Linee di azione per la sicurezza Nazionale***" con l'obiettivo di innalzare e migliorare i livelli di sicurezza dei sistemi e delle reti.

Sempre all'interno del DIS è istituito il "***Nucleo per la sicurezza cibernetica***" (NSC), che si occupa degli aspetti di prevenzione e preparazione rispetto alla minaccia cibernetica e dell'attivazione delle procedure di allertamento, mantenendo sostanzialmente le medesime funzioni previste dal precedente DPCM, nel quale, però, il Nucleo operava presso l'Ufficio del Consigliere Militare e da questi era presieduto. Il succitato nucleo, il cui responsabile è oggi individuato in un vice direttore del DIS, prevede la partecipazione dei rappresentanti dei ministeri degli Esteri, degli Interni, della Difesa, della Giustizia, dello Sviluppo Economico, dell'Economia e delle Finanze, del dipartimento della Protezione Civile, dell'AGID, del Consigliere Militare e delle agenzie di intelligence (con la singolare assenza del ministero delle Infrastrutture e Trasporti). Il NSC ha compiti operativi avendo, nello specifico, la responsabilità di:

a) promuovere la programmazione e la pianificazione operativa per dare attuazione ai deliberati del CISR;
b) mantenere attiva 24x7 l'unità per l'allertamento e la risposta a situazioni di crisi cibernetica;
c) valutare e promuovere procedure di condivisione delle informazioni ai fini della diffusione di allarmi relativi ad eventi cibernetici e per la gestione delle crisi;
d) acquisire le informazioni, dai dicasteri e dai soggetti competenti, circa i casi di violazioni della sicurezza o di perdita dell'integrità dei sistemi informativi;
e) promuovere e coordinare lo svolgimento di esercitazioni che riguardano la simulazione di eventi di natura cibernetica;
f) fungere da punto di riferimento nazionale con le altre organizzazioni internazionali e sovranazionali in materia di sicurezza cibernetica.

Il Nucleo assume un ruolo di vero e proprio hub nella gestione di eventi di crisi, avendo il compito, ai sensi del comma 3 dell'art.9, di acquisire le segnalazioni di evento cibernetico sia dai soggetti nazionali che internazionali e di diramare gli allarmi alle amministrazioni e agli operatori privati. Esso, sulla falsa riga del modello adottato dalla Protezione Civile per la gestione di un evento di crisi, ha anche il compito di effettuare la valutazione delle dimensioni, intensità e natura degli eventi, al fine di stabilire se lo stesso possa essere gestito in autonomia dalle singole amministrazioni ovvero richieda un intervento coordinato da parte di una pluralità di istituzioni che saranno, a tal fine, coordinate dal Nucleo medesimo. Per la gestione concreta delle crisi il Nucleo è integrato, in ragione delle necessità, con rappresentanti di altri enti ed amministrazioni. Nella sostanza, come già evidenziato, il nuovo organismo assorbe quelle che erano le competenze che il precedente DPCM assegnava al NISP.
L'art. 11 titola "Operatori Privati" e individua quelli che sono gli "obblighi" che la controparte privata deve osservare. Il primo comma dello stesso articolo, che appare solo in minima parte innovato rispetto al precedente DPCM, traccia, sebbene in modo alquanto approssimativo, il profilo di questi operatori privati e, nello specifico, vengono individuati: gli operatori privati che forniscono reti pubbliche di comunicazione o servizi di comunicazione elettronica accessibile al pubblico; gli operatori di servizi essenziali e i fornitori di servizi digitali (definiti ai sensi della direttiva NIS); operatori che gestiscono infrastrutture critiche di rilievo nazionale ed europeo (ivi comprese quelle individuate dal DM Interno del 9/1/2008).

Quello che sembra emergere dalla lettura di questi commi è un tentativo da parte del legislatore di confezionare una definizione "ombrello" quanto più ampia possibile all'interno della quale poter di volta in volta individuare i soggetti "privati" di effettivo interesse. Questa strategia "generalista", che fu introdotta ed adottata dal DM Interno del 2008 e che poteva avere a quel tempo una *sua ratio* in quanto la materia "infrastrutture critiche" era ancora agli albori, appare oggi, a distanza di oltre nove anni e alla luce degli sviluppi del settore, decisamente anacronistica, necessitando la materia di una sua formalizzazione legislativa,

non fosse altro che per i mutamenti del contesto socio-politico e della crescente rilevanza delle minacce di tipo cyber-war a tali infrastrutture. **Tale impostazione si traduce in una difficoltà per il singolo "operatore privato" di valutare autonomamente se e in che misura esso sia oggetto delle prescrizioni del DPCM** poiché avrebbe l'obbligo di:

a) Comunicare al Nucleo per la Sicurezza Cibernetica ogni significativa violazione dei propri sistemi informativi;
b) Adottare le best-practices e le misure per la sicurezza cibernetica;
c) Fornire informazioni agli organismi di informazione e consentire l'accesso ai Security Operation Center e agli archivi informatici di interesse;
d) Collaborare alla gestione delle crisi cibernetiche.

Occorre inoltre evidenziare che sebbene l'art. 1 ponga quale obiettivo del DPCM la sicurezza delle infrastrutture critiche in un "contesto unitario e integrato" esso, in ultima analisi, si focalizza esclusivamente sulla minaccia cyber perseverando in una visione frammentaria e non olistica della sicurezza di questi sistemi e, soprattutto, non raccordandosi con le altre norme sul tema, a partire dal DL n. 61 del 11/4/2011 (ovvero la direttiva europea 2008/114/CE sulle infrastrutture critiche che vede nell'Ufficio del Consigliere Militare e nel NISP gli organi deputati all'indirizzo strategico e nei Prefetti gli interlocutori operativi) e con il DM Interno del 9/1/2008 (che individua il CNAIPIC quale interlocutore preferenziale). Un'organizzazione così concepita comporta la presenza di una pluralità di interlocutori pubblici con competenze e visioni parziali che si traduce in una architettura non ancora sufficientemente razionalizzata con possibili significative inefficienze. Dal punto di vista del partenariato pubblico-privato, va evidenziato che il citato DL 61/2011 individuava nella figura del *Security Liaison Officer*, il referente aziendale normativamente deputato a relazionarsi con la parte pubblica per le tematiche di sicurezza nel loro complesso. La mancata attuazione del Decreto, così come l'assenza di uno specifico riferimento nel DPCM di chi debba essere l'interlocutore privato, rappresenta un significativo gap rispetto a ciò che avviene in altri paesi europei compresa la mancata, possibile valorizzazione del ruolo del Security Manager così come definitivo dalla norma UNI10459-2015.

Un ultimo elemento di innovazione è fornito da quanto indicato nel comma 2 dell'art. 11, ovvero l'istituzione presso il MISE di un "**Centro di Valutazione e Certificazione Nazionale**" per la verifica "delle condizioni di sicurezza e dell'assenza di vulnerabilità di prodotti, apparati e sistemi destinati ad essere utilizzati per il funzionamento di reti, servizi e infrastrutture critiche, nonché di ogni altro operatore per cui sussista un interesse nazionale". Questo aspetto rappresenta una concreta e significativa innovazione e un elemento di forte interesse sia per gli operatori di infrastrutture critiche che per l'industria nazionale. Occorre però evidenziare che i contorni, le finalità e gli obiettivi del Centro risultano non ancora ben definiti.
In primo luogo la verifica della "dell'assenza di vulnerabilità" appare di difficile realizzazione in quanto nessuno schema certificatorio può garantire la totale assenza di vulnerabilità di un elemento ma al più la verifica della assenza di tutte le vulnerabilità note al momento in cui si effettua la verifica (nulla potendo dire per ciò che riguarda vulnerabilità non già note).
La denominazione del centro appare potenziale elemento di confusione. Infatti occorre considerare che:

- il DPCM 11 aprile 2002 individua l'Ente di Certificazione nazionale nell'Autorità Nazionale di Sicurezza (ANS), mentre ai sensi del DPCM 30 ottobre 2003 opera presso ISCOM (Istituto Superiore di Comunicazione che è una struttura del MISE) l'Organismo di Certificazione (OSCI). Per cui non è chiaro se tale organismo sostituisca, integri o affianchi tali strutture già esistenti;
- ai sensi del DPCM 11 aprile 2002 le attività di valutazione sono svolte da laboratori tecnici, denominati Centri di Valutazione (Ce.Va) all'uopo abilitati dal ANS sia per gli aspetti di sicurezza dei dispositivi sia per le competenze professionali. Fra quelli attualmente abilitati ne esiste uno all'interno del ISCOM. Anche in questo caso non è chiaro se il legislatore abbia voluto con tale locuzione individuare le strutture già esistenti, ovvero individuare strutture diverse.

Ora, se da un lato appare estremamente utile un processo di certificazione degli apparati (ed in alcuni casi dei prodotti) utilizzati dai diversi operatori, soprattutto per quel che riguarda la componente hardware e firmware, l'idea di certificare i loro "sistemi" appare decisamente utopistica. Questo in considerazione della complessità intrinseca di questi sistemi, che sono costituiti da una pluralità di infrastrutture disperse sul territorio nazionale ed in esercizio 24x365 che si caratterizzano per un numero enorme di componenti con architetture fortemente stratificate ed eterogenee e con un istallato con una vita media dell'ordine delle decine di anni. A tutto ciò va aggiunta la necessità di considerare le peculiarità del processo sotteso che rende nei fatti unico e differente ogni singolo sistema. In aggiunta, un processo di certificazione (a prescindere se si adotti lo schema ITSEC o i Common Criteria) richiede la conoscenza di tutti gli aspetti progettuali, costruttivi e implementativi dei vari sistemi, con la conseguente necessità di generare una mole enorme di documentazione "cartacea" che nella sostanza non si tradurrebbe in alcun effettivo miglioramento della sicurezza dei sistemi stessi. **Una soluzione differente che appare maggiormente *feasible*, adottata da altri stati a partire dagli Stati Uniti, è quella di effettuare non una certificazione di questi sistemi ma, piuttosto, una loro validazione.** Ovvero nel sottoporre il sistema (ovvero parte di esso) ad una campagna di test in grado di verificarne il comportamento effettivo rispetto a determinate classi di vulnerabilità/minacce. Tale soluzione, per ovviare ai problemi legati alle interferenze con le attività in esercizio, potrebbe essere attuata anche presso opportuni sistemi di test-bed (casa che, ad esempio è fatto negli USA ricorrendo, fra gli altri, ai Idaho National Lab). L'approccio attraverso la validazione introdurrebbe il vantaggio di limitare la produzione di documentazione cartacea consentendo di focalizzare gli sforzi sull'effettivo riscontro delle vulnerabilità con significativi risparmi economici e di tempo a parità di risultati.

Sorprende, infine, l'assenza di qualunque riferimento al fattore umano sia in termini di valutazione/certificazione/validazione delle procedure di gestione di questi sistemi e, soprattutto, che per quel che riguarda i ruoli, la formazione e le competenze del personale degli operatori privati. ©

BIBLIOGRAFIA

- DPCM 17 febbraio 2017 "Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionali" (GU n.87 del 13-4-2017)
- DPCM 24 gennaio 2013, "Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionale" (GU 19 marzo 2013, n. 66)
- Direttiva UE/2016/1148 "Network and Information Security
- Piano nazionale per la protezione cibernetica e la sicurezza informatica nazionale.