ISTITUITO IL "NUCLEO PER LA SICUREZZA CIBERNETICA"

di Roberto Setola

Lo scorso 19 marzo, dopo un'attesa di quasi due mesi, ha visto la luce il DPCM 24 gennaio 2013 "*Direttiva recante indirizzi per la protezione e la sicurezza informatica nazionale*". **Tale decreto va a riempire un vuoto esistente da troppo tempo nel nostro ordinamento cogliendo la portata sistemica** (e, quindi, necessariamente interministeriale) **del problema della sicurezza informatica della nazione, delle sue infrastrutture e dei singoli cittadini**. Nella sua essenza il DPCM, con l'obiettivo di razionalizzare e semplificare il quadro delinea una strategia di intervento che mira, lodevolmente, a coinvolgere i diversi attori pubblici e privati raccordandoli in un quadro strategico nazionale che attribuisce a ciascuno i propri ruoli e responsabilità, pur nella consapevolezza della difficoltà del compito. Il DPCM parte, infatti, dall'assunto, esplicitato anche nel testo, che l'attuale scenario vede la presenza di molteplici attori i cui ruoli sono in parte in sovrapposizione se non in conflitto al punto che il legislatore ritiene necessario procedere a una "*graduale e progressiva razionalizzazione dei ruoli*". Partendo da una azione "*integrata che metta a fattor comune le diverse attribuzioni istituzionali*".

A tal fine il DPCM delinea una architettura istituzionale su tre livelli. **Il primo di indirizzo politico e coordinamento strategico, ha il compito di delineare gli obiettivi strategici anche mediante la redazione di un Piano Nazionale per la Sicurezza dello Spazio Cibernetico ed alla predisposizione degli atti normativi necessari**. Tale compito è attribuito al Comitato Interministeriale per la Sicurezza della Repubblica (CISR) che ha la responsabilità della redazione del piano nazionale e l'emanazione degli atti ad esso connessi inclusivi delle proposte di modifiche normative che si rendessero necessarie. Tale scelta appare coerente con i dettami della L. 124/2007 che attribuisce a tale organo il compito di delineare le strategie per la sicurezza della nazione sotto la direzione del Sottosegretario delegato per la sicurezza della Repubblica. L'aver delineato (o quanto meno iniziato a delineare) una visione sistemica per la sicurezza del Sistema Paese, con una eccezione più ampia della sola sicurezza nazionale e dei confini, sotto un unico organismo strategico consentirà di favorire una visione integrale ed olistica del problema della sicurezza andando ad abbracciare quella filosofia "*All-Hazard*" che, pur se non esplicitamente citata nel testo, sembra iniziare a far breccia anche nel nostro ordinamento sulla falsa riga di quanto stanno facendo tutte le democrazie più evolute.

Il CISR si avvale, come specificato dall'art. 5, quale proprio organo tecnico del Dipartimento delle Informazioni per la Sicurezza (DIS) che ha il compito di svolgere le attività preparatorie di verifica dell'attuazione e di individuazione di minacce e vulnerabilità. Il DIS a sua volta ha la facoltà di stipulare accordi di collaborazione con università, enti di ricerca e aziende. Per altro, con una apertura significativa, è affidato allo stesso DIS il compito di promuovere e diffondere una cultura della sicurezza, superando in questo modo una visione dei nostri servizi di *intelligence* quasi esclusivamente orientati ad una funzione di acquisizione di informazione per spostarsi verso una funzione maggiormente di *hub* in grado anche di effettuare quella opportuna condivisione e *sharing* verso il nostro tessuto produttivo ed i cittadini.

Il terzo livello che ha il compito di gestire le diverse situazioni di crisi, curando e coordinando le risposte da adottare per contrastare la minacci e per ciò che attiene il ripristino delle funzionalità dei sistemi, **è attribuito al NISP (Nucleo Interministeriale Situazione e Pianificazione)** stante il suo ruolo di massimo organismo di coordinamento in situazione di emergenza nazionale.
Il secondo livello ha un compito di raccordo fra CISR e le diverse amministrazioni coinvolte e provvede alla programmazione delle attività interministeriali. Tale livello ha anche il compito di attivare le opportune azioni di allertamento in caso di crisi. Per la natura della sua specificità, il DPCM specifica che la struttura deputata opera "a carattere permanente". Su questo livello, che è la struttura maggiormente responsabilizzata dal punto di vista operativo, è necessario effettuare una attenta riflessione, soprattutto, **sull'aver attribuito tale competenza all'Ufficio del Consigliere Militare di Palazzo Chigi dove andrebbe istituito un "Nucleo per la Sicurezza Cibernetica"**. Tale scelta appare alquanto anomala sebbene in linea con quanto già decretato con il D.Lgs 61/2011 per quel che riguarda le Infrastrutture Critiche anche perché tale ufficio non pare strutturato per attività h24.
Analogamente lascia perplessi il ruolo affidatogli dal DPCM di ricevere, anche da soggetti internazionali, "segnalazioni di evento cibernetico" in quanto qualora esse si riferiscano a vulnerabilità sembra duplicare quello che dovrebbe essere il ruolo del CERT nazionale, qualora, invece, siano informazioni concernenti eventi in atto (ovvero accaduti) esse potrebbero configurarsi come notizie di reato la cui gestione appare esimere dai compiti precipui di tale ufficio. Per questi ultimi, tale ruolo poteva essere attribuito, se non altro per continuità con quanto già si fa, in modo egregio in ambito G8 e Meridian, alla Polizia Postale (e per essa al CNAIPIC) preservando e valorizzando in questo modo competenze ed investimenti già realizzati. Per altro l'art. 11 dello stesso DPCM evidenzia che i soggetti nazionali devono comunicare tali violazioni proprio attraverso il CNAIPIC.

Il fatto che, infine, vengano a crearsi due strutture parallele all'intero della stessa Presidenza del Consiglio di supporto al CISR su tematiche molto contigue potrà creare sovrapposizioni e discrasie e, certamente, non appare del tutto coerente con la citata volontà di razionalizzazione e snellimento organizzativo. In questa ottica, sembrerebbe maggiormente logico e razionale attribuire al DIS un ruolo di segreteria unica del CISR con

competenze sia relative a quelle connesse con la definizione del piano strategico nazionale che le attività operative di raccordo, nonché la valutazione delle minacce in essere o potenziali. Con la stessa ottica, sarebbe auspicabile una maggiore sinergia fra le strutture delineate dal DPCM e l'Agenzia per l'Italia Digitale e un più stretto coordinamento con il Ministero delle Attività Produttive al fine di dar vita ad una sorta di cabina di regia unitaria, vecchia idea ripetutamente auspicata ma mai concretamente attuata, all'interno della quale delineare una strategia unitaria del Sistema Paese nel campo digitale. Purtroppo quanto emerge dal DPCM, e da altri atti, sembra invece favorire una duplicazione di funzioni volta più a conservare dinamiche e situazioni pregresse, che non mirante a quella efficienza tanto auspicata.

Occorre evidenziare che, dopo una sì lunga gestazione, ci si attendeva un decreto curato anche nei minimi dettagli: purtroppo **esistono non poche ambiguità lessicali, ma anche fattuali, che potrebbero rendere complessa l'attuazione del dettame del DPCM**. Questo a partire dal termine CIBERNETICA, che vorrebbe essere la traduzione del termine inglese *cyber*, peccato che tale termine in italiano ha un senso diverso (e nello specifico indica la scienza che studia i fenomeni di autoregolazione dei sistemi - oggi più comunemente indicata come controlli automatici o automatica - e che, per altro, si traduce più correttamente in lingua inglese con il termine "*cybernetics*".
Volendo partire dall'art. 1 si evidenzia che in esso l'obiettivo è quello di "*definire in un contesto unitario ed integrato, l'architettura istituzionale deputata alla tutela della sicurezza nazionale relativamente alle INFRASTRUTTURE CRITICHE*". Peccato che non solo non definisce cosa esse siano, ma nell'art. 2 si parla di spazio cibernetico come insieme delle "INFRASTRUTTURE INFORMATICHE INTERCONNESSE", e le minacce fanno riferimento a "RETI E SISTEMI INFORMATIVI" (sistemi informatici ed informativi non sono proprio la stessa cosa...), per poi superare tale ambiguità nell'art. 3 dove l'oggetto divengono i "SISTEMI E RETI DI INTERESSE NAZIONALE", mentre nell'art. 7 comma 5 si fa riferimento a "SOGGETTI EROGATORI DI SERVIZI DI PUBBLICA UTILITÀ" per poi estendersi ad includere nell'articolo 11 "*Operatori privati che forniscono reti di pubbliche comunicazioni o servizi di comunicazione elettronica accessibili al pubblico, quelli che gestiscono infrastrutture critiche di rilievo nazionale ed europeo, il cui funzionamento è condizionato dall'operatività di sistemi informatici e telematici*".

Giusto continuando con la lettura dell'art. 2 si apprende al punto i) che la sicurezza cibernetica riguarda la "DISTRUZIONE O BLOCCO" del regolare funzionamento delle reti e dei sistemi informativi, mentre al punto l) si legge che affinché ci sia una minaccia cibernetica è sufficiente che la stessa "DISTRUGGA O OSTACOLI" il loro corretto funzionamento, sebbene per avere un evento cibernetico, come definito al successivo punto m), è necessario che lo stesso "DISTRUGGA O BLOCCHI" il loro regolare funzionamento (il solo ostacolo potrebbe rappresentare, per molti sistemi *mission critical*, un serio problema e, per altro, è estremamente raro che un attacco di tipo DoS o DDoS possa provocare un blocco completo, ma più probabilmente indurrà forti degradazioni). Si nota nei diversi articoli, inoltre, come la lista degli organismi internazionali di cooperazione si modifichi citando a volte alcuni e a volte altri.

Volendo, però, guardare il bicchiere mezzo pieno, **la volontà di adottare un piano di sicurezza nazionale è sicuramente un aspetto positivo** (sarebbe stato opportuno definire anche un orizzonte temporale per la sua adozione e successivo aggiornamento), così come il tentativo di superare la frammentazione di competenze favorendo una visione unitaria e sistemica della problematica.

Altro aspetto positivo è quello di individuare, quale uno degli elementi fondanti, una crescita della cultura della sicurezza. Aspetto questo estremamente importante che vede, e deve vedere, anche e soprattutto in un contesto di alta tecnologia, il primato del operatore umano sia quale risorsa fondamentale per l'attuazione di qualunque strategia di successo che, al tempo stesso, potenziale anello debole della catena. In questa ottica l'apertura verso il mondo universitario e della società civile sembra più che positivo nella speranza che il tutto non si limiti ad una mera organizzazione di convegni ovvero allo stilare liste di nuovi oneri burocratici ed organizzativi a carico degli operatori, ma diventi una interfaccia fra coloro che sono preposti alla sicurezza della nazione e coloro che gestiscono quotidianamente le infrastrutture critiche e, più in generale, sono gli attori del tessuto produttivo del Paese. Questo si può attuare facendo sì che il comitato di cui all'art. 6 sia una fucina di materiale da diffondere non quale "obblighi da fare" ma quali strumenti di supporto affinché i diversi attori, mediante attività di auto-valutazione, possano meglio comprendere la propria esposizione ed avere strumenti per delineare strategie e tattiche di azioni. **Per raggiungere tale obiettivo è fondamentale che tale comitato sia lo strumento, non solo per portare all'interno del CISR competenze e conoscenze "accademiche e professionali", ma anche il luogo tramite il quale veicolare verso l'esterno la rilevanza per il Sistema Paese dei temi legati alla sicurezza *cyber*, e non solo *cyber***, sollecitando una maggiore attenzione e creatività su queste tematiche. Lo scenario attuale evidenzia che, sebbene esistano in Italia diverse eccellenze riconosciute anche a livello internazionale per quel che riguarda competenze scientifiche sui diversi segmenti della *security*, la capacità di impattare sul sistema formativo nazionale appare non adeguata.
In questa ottica un approccio che preveda una elaborazione condivisa del Piano Nazionale magari con procedure simili al *green paper* della Commissione Europea (ovvero rilascio di un documento preliminare anche con domande e quesiti aperti, per sollecitare una condivisione di responsabilità e visioni) sarebbe fortemente auspicabile. Il DPCM rappresenta una cornice che, per quanto imperfetta e migliorabile, è sicuramente un primo importante passo che ci aiuta a recuperare un ritardo accumulato nel corso degli anni a causa, purtroppo, di quella parcellizzazione delle competenze evidenziate dallo stesso DPCM che ha creato una serie di paralisi a causa del contrapporsi di visioni settoriali non conciliante.
Abbiamo quasi un decennio di ritardo rispetto ad altri paese ma, sfruttando anche l'esperienza e gli errori commessi, potremmo facilmente recuperare tale *gap* e rendere il Paese e, soprattutto, il suo tessuto produttivo, in grado di gestire le sfide e le minacce legate all'evoluzione ed alla diffusione capillare delle tecnologie *cyber*. Occorre però essere pragmatici e fattivi... e, soprattutto, celeri. ©