Anno XIII
Marzo 2014
Poste Italiane S.p.A.
Spedizione in Abbonamento Postale
D.L. 353/03 (Conv. in L. 27/02/2004 n° 46)
Art. 1, Comma 1 – Roma Aut.n C/RM/44/2012
per "ICT SECURITY" id sap 30619433-015
Prezzo € 4,00

ICT Security

2014 116

www.tecnaeditrice.com

CYBER CRIME CONFERENCE

15/16 Aprile 2014

- La strategia italiana in materia di cyber-security
- Cyber risks, social network e rischi reputazionali
- Boyd e app spingono il cybercrime nell'indifferenza generale
- La Direttiva Comunitaria per prevenire e difenderci dagli attacchi informatici

TecnaEditrice

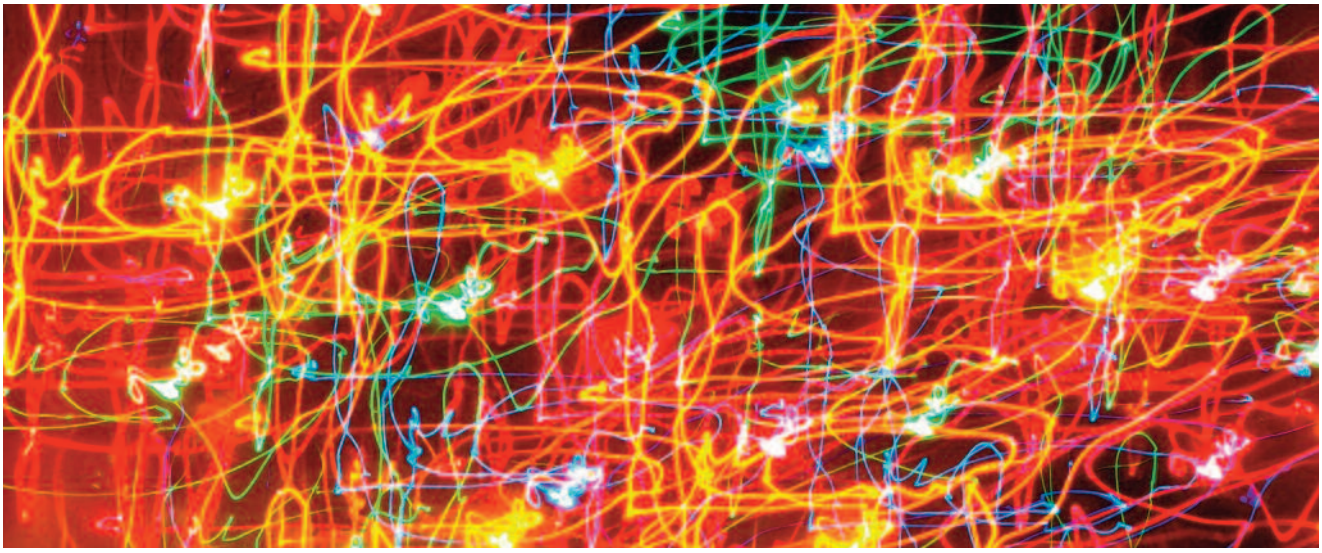
La strategia italiana in materia di cyber-security

Il processo di rinnovamento che, dall'emanazione della Legge n. 124 del 2007 sta vedendo come protagonista il comparto dell'*intelligence* italiana, ha vissuto nel 2013 una notevole fase di accelerazione su più fronti.

Numerose, infatti, sono state le linee strategiche che hanno registrato un significativo progresso, come la sempre maggiore apertura verso i cittadini e il mondo delle imprese, delle università e della ricerca, un ampio riassetto organizzativo volto a razionalizzare ed accrescere l'efficienza delle risorse, il consolidamento dell'unitarietà dell'azione dell'*intelligence* anche attraverso sempre più fitte sinergie interistituzionali[1].

Sul fronte delle macro aree di applicazione, invece, la tematica certamente predominante è apparsa essere sicuramente quella della *cyber-security*, declinata sia sotto il profilo strategico e operativo, che sotto le sue inevitabili congiunzioni interdisciplinari, soprattutto con le dinamiche economico-finanziarie e con la tutela del *know how*.

Se il Decreto del Presidente del Consiglio dei Ministri del 24 gennaio 2013, recante "*indirizzi per la protezione cibernetica e la sicurezza in-*



formatica nazionale", può essere considerato senza ombra di dubbio il primo vero atto d'impulso di numerose e mirate iniziative di coordinamento e di convergenza tra la comunità di *intelligence* e le diverse Amministrazioni dello Stato, i documenti strategici nazionali in tema di *cyber-security* – pubblicati il 20 febbraio 2014 – rappresentano senz'altro un ideale "punto di arrivo" di questa fase prettamente costitutiva e preliminare.

Punto di arrivo che, in realtà, costituisce esclusivamente un nuovo punto di partenza verso obiettivi ancor più rilevanti ed ambiziosi, fissati proprio nei documenti strategici appena pubblicati.

Il primo dei due documenti è il "*Quadro strategico nazionale per la sicurezza dello spazio cibernetico*", ovvero la strategia di medio-lungo periodo, mentre il secondo è il "*Piano nazionale per la protezione cibernetica e la sicurezza informatica*", che, direttamente collegato al *Quadro strategico nazionale*, ne sviluppa le linee operativa di breve periodo (2014-2015).

Con tali documenti, redatti conformemente agli accordi e agli indirizzi strategici fissati in ambito NATO ed Unione Europea, l'Italia quindi si è dotata – per la prima volta – di un assetto organizzativo integrato volto a mitigare le "minacce cibernetiche" rivolte verso quegli *asset* nazionali da cui dipendono la sicurezza, la stabilità e lo sviluppo del nostro Paese.

IL QUADRO STRATEGICO NAZIONALE PER LA SICUREZZA DELLO SPAZIO CIBERNETICO

Tra i due, il *Quadro strategico nazionale* è il documento di più alto livello ed ha come scopo quello di delineare le linee strategiche nazionali nel medio-lungo periodo.

E' deputato, infatti, a contenere l'indicazione dei profili e delle tendenze evolutive delle minacce e delle vulnerabilità dei sistemi e delle reti d'interesse nazionale, la definizione dei ruoli e dei compiti dei diversi soggetti, sia pubblici che privati, e di quelli nazionali operanti al di fuori del territorio del Paese, nonché l'individuazione degli strumenti e delle procedure con cui perseguire l'accrescimento della capacità del Paese di prevenzione e risposta nei confronti delle minacce provenienti dal cyber-spazio,

AVV. STEFANO MELE

Avvocato specializzato in Diritto delle Tecnologie, Privacy, Sicurezza delle informazioni e Intelligence. Dottore di ricerca presso l'Università degli Studi di Foggia. Lavora a Milano come "of Counsel" di Carnelutti Studio Legale Associato e collabora presso le cattedre di Informatica Giuridica e Informatica Giuridica avanzata della Facoltà di Giurisprudenza dell'Università degli Studi di Milano. Esperto di cyber-security, cyber-intelligence, cyber-terrorism e cyber-warfare:

- *Direttore di Ricerca su "Cyber-security & Cyber-Intelligence" del Ce.Mi.S.S. (Centro Militare di Studi Strategici);*
- *Consulente per organizzazioni nazionali ed estere, sia militari che civili;*
- *Docente presso Istituti di formazione e di ricerca del Ministero della Difesa italiano e della NATO;*
- *Docente di "Intelligence e utilizzo delle informazioni per la gestione della sicurezza nei Paesi a rischio" all'interno del Certificate of Training in United Nations Peace Support Operations (COTIPSO) per operatori delle Nazioni Unite (ONU) ed altro personale NGO;*
- *Coordinatore dell'Osservatorio "Info-Warfare e Tecnologie emergenti" dell'Istituto Italiano di Studi Strategici 'Niccolò Machiavelli'.*

anche in un'ottica di diffusione della cultura della sicurezza.
Sei sono i pilastri strategici su cui il nostro Governo ha deciso di incentrare la sua strategia:

1. Il miglioramento delle capacità tecnologiche, operative e di analisi degli attori istituzionali interessati.
2. Il potenziamento delle capacità di difesa delle infrastrutture critiche nazionali e degli attori di rilevanza strategica per il sistema-Paese.
3. L'incentivazione della cooperazione tra istituzioni e imprese nazionali.
4. La promozione e diffusione della cultura della sicurezza.
5. Il rafforzamento delle capacità di contrasto alla diffusione di attività e contenuti illegali on-line.
6. Il rafforzamento della cooperazione internazionale in materia di sicurezza cibernetica.

Per il raggiungimento dei suddetti indirizzi strategici, inoltre, direttamente all'interno del *Quadro strategico nazionale* sono identificati anche gli undici indirizzi operativi previsti dal Governo, il cui approfondimento però è demandato al "*Piano nazionale per la protezione cibernetica e la sicurezza informatica*". Questi – com'è logico che sia – spaziano da specifiche focalizzazioni su aspetti meramente tecnici e tecnologici, passando per l'incremento delle capacità di *early warning* e di *incident response*, fino all'ormai imprescindibile cooperazione interna ed internazionale.
E' importante sottolineare, inoltre, come la strategia italiana miri "*ad accrescere la capacità di risposta del Paese alle presenti e future sfide riguardanti il cyber-space, indirizzando gli sforzi nazionali verso obiettivi comuni e soluzioni condivise, nella consapevolezza che la protezione dello spazio cibernetico è un processo più che un fine, che la continua innovazione tecnologica introduce inevitabilmente nuove vulnerabilità, e che le caratteristiche stesse della minaccia cibernetica rendono la difesa, per ora, di tipo prevalentemente – anche se non esclusivamente – reattivo*"[2].
Ciò pone in evidenza due elementi di rilevante importanza. Il primo, inerente al fatto che la strategia è un processo e che la sicurezza assoluta, soprattutto quando si parla di tecnologie in costante evoluzione, è un obiettivo difficilmente raggiungibile. Il secondo, che l'approccio strategico dell'Italia per questo settore è "*per ora* [...] *anche se non esclusivamente*" di tipo prevalentemente difensivo e di mera reazione ad un'ipotetica aggressione, facendo trasparire un'evidente riflessione interna verso quell'approccio di *active defence* ben consolidato e tipico delle dottrine anglosassoni.
Nulla si dice, invece, se questa reazione debba essere esclusivamente "cibernetica", oppure possa sostanziarsi anche in un attacco cinetico.

La necessità, in sostanza, non è solo quella di essere "al passo con i tempi" ma anche di coglierne le "anticipazioni", così da prevenire le future minacce atte a minare lo sviluppo economico, sociale, scientifico e industriale, nonché la stabilità politico-militare del nostro Paese".

IL PIANO NAZIONALE PER LA PROTEZIONE CIBERNETICA E LA SICUREZZA INFORMATICA

La seconda parte della strategia italiana per il cyber-spazio, invece, si esplica attraverso il "*Piano nazionale per la protezione cibernetica e la sicurezza informatica*", che, come detto in precedenza, rappresenta il documento operativo di breve periodo – incentrato sul biennio 2014-2015 – volto ad individuare gli obiettivi da conseguire e le linee di azione da porre in essere per realizzare quanto contenuto nel *Quadro strategico nazionale*.
Attraverso quest'ulteriore documento, "*l'Italia si dota di una strategia organica, alla cui attuazione sono chiamati a concorrere non solo gli attori, pubblici e privati, richiamati nel Quadro Strategico Nazionale ma anche tutti coloro che, su base quotidiana, fanno uso delle moderne tecnologie informatiche, a partire dal singolo cittadino. Tale strategia associa alla sua valenza organica un tratto di flessibilità, indispensabile a fronte delle rapide evoluzioni tecnologiche dello spazio cibernetico e delle relative sfide di sicurezza. La necessità, in sostanza, non è solo quella di essere "al passo con i tempi" ma anche di coglierne le "anticipazioni", così da prevenire le future minacce atte a minare lo sviluppo economico, sociale, scientifico e industriale, nonché la stabilità politico-militare del nostro Paese*"[3].
Undici sono i punti operativi predisposti all'interno del *Piano*:

1. Potenziamento delle capacità di intelligence, di Polizia e di difesa civile e militare.
2. Potenziamento dell'organizzazione e delle modalità di coordinamento e di interazione a livello nazionale tra soggetti pubblici e privati.
3. Promozione e diffusione della cultura della sicurezza informatica. Formazione e addestramento.
4. Cooperazione internazionale ed esercitazioni.
5. Operatività del CERT nazionale, del CERT-PA e dei CERT dicasteri.
6. Interventi legislativi e *compliance* con obblighi internazionali.
7. *Compliance* a standard e protocolli di sicurezza.

8. Supporto allo sviluppo industriale e tecnologico.
9. Comunicazione strategica.
10. Ottimizzazione della spesa nei settori della *cyber-security* e *cyber-defence*.
11. Implementazione di un sistema di *information risk management* nazionale.

In merito al *Piano nazionale*, occorre evidenziare come la predisposizione di uno specifico documento atto ad incidere anche sul piano operativo eviti di incorrere in una delle mancanze più frequenti in molti documenti di sicurezza nazionale, i quali spesso si limitano a prevedere esclusivamente delle generiche affermazioni di principio senza alcun approfondimento "operativo" e inutili dal punto di vista della conseguente pianificazione strategica.

Di seguito, infine, un'immagine estratta dal documento strategico che ben sintetizza il rapporto tra *Quadro strategico nazionale* e *Piano nazionale*.

RIFLESSIONI CONCLUSIVE

Nel complesso, il giudizio sulla *cyber-strategy* italiana è certamente positivo. Essa, infatti, si innesta perfettamente nel quadro delineato a livello internazionale dagli altri Stati sovrani, abbracciando *in toto* quei principi strategici comuni divenuti ormai imprescindibili per un corretto approccio alla minaccia[4].

Inutile dire che l'attuazione delle linee strategico-operative tracciate nella *cyber-strategy* italiana sarà il vero banco di prova per il nostro Governo, soprattutto considerata la mole di lavoro e le congiunture economiche particolarmente sfavorevoli.

Il meccanismo è stato ben avviato. A questo punto, però, è fondamentale operare mantenendo la corretta visione strategica, anche tramite un'analisi approfondita ed aggiornata delle *best practice* internazionali, già previste peraltro dall'art. 5, comma 3, lett. *d)*, del DPCM del 24 gennaio 2013. ■

1 Presidenza del Consiglio dei Ministri – Sistema di Informazioni per la sicurezza della Repubblica, "Relazione sulla politica dell'informazione per la sicurezza 2013", 2014.

2 Presidenza del Consiglio dei Ministri, "Quadro strategico nazionale per la sicurezza dello spazio cibernetico", 2014, pag. 11.

3 Presidenza del Consiglio dei Ministri, "Piano nazionale per la protezione cibernetica e la sicurezza informatica", 2014, pag. 5.

4 Per un'analisi comparata dei principi strategici in materia di cyber-security, si veda Stefano Mele, "I principi strategici delle politiche di cybersecurity", 2013, in http://www.sicurezzanazionale.gov.it/sisr.nsf/il-mondo-intelligence/principi-strategici-delle-politiche-di-cyber-security.html.

Immagine a pag. 7 del "Piano nazionale per la protezione cibernetica e la sicurezza informatica"