
Copasir: relazione sulla cyber sicurezza e la difesa delle infrastrutture critiche (15 luglio 2010)

By Agatino Grillo

Published: 23/07/2010 - 13:03

Il Comitato Parlamentare per la sicurezza della Repubblica ([Copasir](#)) ha pubblicato il **15 luglio 2010** la "Relazione sulle possibili implicazioni e minacce per la sicurezza nazionale derivanti dall'utilizzo dello spazio cibernetico" (qui la versione ufficiale in [pdf](#), 692 K, 62 pp.) dal sito <http://www.parlamento.it>, qui le versioni [epub](#) e [xhtml](#) a cura di www.ComplianeNet.it). La relazione è stata trasmessa ai presidenti della Camera e del Senato.

Si tratta di documento di circa 60 pagine che illustra lo **scenario della sicurezza informatica** internazionale e nazionale nel prossimo futuro e si articola come segue:

- premessa di sintesi delle nuove problematiche strategiche riferite ai compiti del Comitato;
- descrizione dell'attività svolta;
- illustrazione delle caratteristiche del fenomeno a livello globale;
- analisi delle ricadute per il nostro paese;
- presentazione delle principali risultanze delle attività di intelligence;
- proposta di interventi per rafforzare la capacità di analisi dei nostri apparati di sicurezza e per potenziare le attività di prevenzione e contrasto alle minacce informatiche.

Nelle sue conclusioni, il rapporto osserva che il "**limite principale**" dell'approccio nazionale alla cyber security "si riscontra nella dimensione della prevenzione della minaccia e nell'assenza di una pianificazione coordinata e unitaria al livello del vertice politico, per mettere al sicuro il più possibile i sistemi strategici nazionali connessi alla rete informatica".

Per ovviare a tali carenze, il Copasir raccomanda al Governo "di **dotarsi di un impianto strategico-organizzativo** che assicuri una leadership adeguata e predisponga chiare linee politiche per il contrasto alle minacce e il coordinamento tra gli attori interessati. Tale obiettivo potrebbe essere raggiunto assegnando questi compiti ad una struttura di coordinamento presso il Presidente del Consiglio dei ministri, o presso l'Autorità delegata, organizzata ridefinendo l'attività delle strutture esistenti,

con una rimodulazione delle attuali competenze e responsabilità".

Di seguito pubblichiamo l'indice e le raccomandazioni della relazione.

Indice della la "Relazione sulle possibili implicazioni e minacce per la sicurezza nazionale derivanti dall'utilizzo dello spazio cibernetico"

- Avvertenza
-
- 1. Premessa.
-
- 2. L'attività del comitato parlamentare per la sicurezza della repubblica.
-
- 3. Sicurezza globale ed utilizzo dello spazio cibernetico: definire il fenomeno.
-
- 4. La prevenzione della minaccia: panorama internazionale.
-
- A) l'Unione Europea.
-
- B) gli Stati Uniti d'America.
-
- C) il Regno Unito.
-
- D) Francia.
-
- E) la cooperazione in ambito Nato.
-
- 5. L'attività di contrasto alla minaccia in Italia.
-
- 5.1. La protezione delle infrastrutture critiche in Italia.
-
- 5.2. L'attività dei servizi di intelligence italiani.
-
- 6. Conclusioni e raccomandazioni.
-
- Allegato 1 - Le principali categorie da fonti di attacco cibernetico secondo il Computer Emergency Readiness Team del DHS (department of homeland security USA)

-
Allegato 2 - Elenco esemplificativo delle principali tipologie di minaccia informatica

-
Allegato 3 - Alcuni dei principali casi concreti di cyber crime a scopo di frode finanziaria.

-
Operazione phish phry. (65)

-
Caso heartland payment systems.

-
Il phishing mirato: un caso particolare.

-
Il fallito attacco britannico alla sumitomo bank.

-
Il caso dell'indian eastern railway.

-
I casi d'attacco a biglietti elettronici.

-
L'attacco al trasporto aereo.

-
Incertezze tecnologiche e giuridiche.

□

6. Conclusioni e raccomandazioni

La sicurezza dello spazio cibernetico è articolata su componenti di varia natura: politica, economica, normativa, tecnica; componenti che si devono integrare con le dinamiche operative affidate alle Forze di Polizia, alle Forze armate e, soprattutto, nella prospettiva della presente relazione, ai nostri apparati di intelligence.

Accanto ad essi, vi sono altri organi pubblici e privati, che non svolgono esattamente una funzione operativa, ma sono un supporto prezioso alla tutela della integrità e dell'efficienza della rete di sicurezza nazionale. I soggetti che a vario titolo e con diverse competenze sono coinvolti nel processo di contrasto alle minacce sono numerosi e sono stati individuati nel corso della trattazione della presente relazione. In sede di conclusione e per la formulazione di raccomandazioni operative, giova sottolineare come questa pluralità di soggetti, importanti per la qualità delle operazioni che spesso riescono a garantire, possa rappresentare, laddove non adeguatamente coordinata e sollecitata al costante aggiornamento operativo, un limite per la tutela della sicurezza della nazione.

Le azioni intraprese dai singoli dicasteri (con particolare riguardo al Ministero dell'interno e ai nostri apparati di intelligence), dalle strutture della Presidenza del Consiglio dei ministri, dagli operatori pubblici e privati sono servite, fino ad oggi, a colmare singoli vuoti organizzativi. In prospettiva, occorre una pianificazione strategica in materia di contrasto alla minaccia cibernetica, parte di una strategia nazionale di sicurezza che possa dettare le linee guida a tutti i soggetti interessati, coordinandone gli sforzi ed assumendosi, innanzitutto, l'onere di pianificare le azioni per la messa in sicurezza delle infrastrutture critiche di sicurezza nazionale. Queste ultime, inoltre, dovrebbero essere oggetto di una rapida e completa classificazione, attraverso una mappatura puntuale e la definizione conseguente del loro perimetro, siano esse materiali o immateriali.

Come conseguenza, una strategia di sicurezza cibernetica nazionale dovrebbe prevedere l'aggiornamento delle normative alle fattispecie più moderne e in costante, rapida evoluzione – legate alle minacce provenienti dallo spazio cibernetico.

In sintesi, si può affermare che l'Italia abbia, sin qui, messo in campo risorse e strumenti idonei a contrastare le minacce legate al cyber-crime e alla tutela dei prodotti dell'ingegno, dei marchi e dei brevetti industriali. Occorre essere consapevoli che, rispetto a qualsiasi attacco condotto con mezzi cibernetici, il successo è direttamente proporzionale alla velocità di applicazione delle contromisure. Esse debbono essere predisposte prima che avvenga l'attacco, in una prospettiva che, in ragione della dimensione globale della minaccia cibernetica e della pluralità dei soggetti che potrebbero essere coinvolti, supera i confini nazionali e va organizzata secondo logiche di sicurezza integrate e con strategie di intervento che coinvolgano tutti gli attori della sicurezza.

Il limite principale si riscontra nella dimensione della prevenzione della minaccia e nell'assenza di una pianificazione coordinata e unitaria al livello del vertice politico, per mettere al sicuro il più possibile i sistemi strategici nazionali connessi alla rete informatica.

Per ovviare a tali carenze, si ritiene di dover raccomandare al Governo di dotarsi di un impianto strategico-organizzativo che assicuri una leadership adeguata e predisponga chiare linee politiche per il contrasto alle minacce e il coordinamento tra gli attori interessati. Tale obiettivo potrebbe essere raggiunto assegnando questi compiti ad una struttura di coordinamento presso il Presidente del Consiglio dei ministri, o presso l'Autorità delegata, organizzata ridefinendo l'attività delle strutture esistenti, con una rimodulazione delle attuali competenze e responsabilità.

Questa struttura, ferme restando le attribuzioni stabilite con provvedimenti normativi degli organi istituzionali, dovrebbe svolgere i seguenti compiti:

- definire compiutamente la minaccia e predisporre un documento di sicurezza nazionale dedicato alla protezione delle infrastrutture critiche materiali e immateriali;
- predisporre un piano d'intervento che definisca il perimetro della sicurezza cibernetica italiana, definendo i ruoli e le responsabilità di tutti i soggetti responsabili della sicurezza informatica nazionale;
- redigere, in stretto coordinamento con gli interlocutori istituzionali e privati, a cominciare dai nostri apparati di intelligence, le politiche strategiche di protezione, resilienza e sicurezza cibernetica; – sviluppare la collaborazione pubblico-privato per migliorare l'azione di prevenzione e contrasto al cyber-crime;
- promuovere piani di formazione specialistica comuni tra i vari soggetti interessati a livello nazionale ed internazionale, anche favorendo campagne di informazione mirata verso soggetti di importanza strategica, per elevare il livello di consapevolezza dei rischi nel cyber-spazio;
- predisporre piani di disaster recovery per i dati di valore strategico per la sicurezza della Repubblica;

- coordinare la partecipazione di delegazioni italiane ai tavoli di cooperazione internazionale, in ambito bilaterale e multilaterale, UE e NATO.

Per quanto attiene più specificamente al potenziamento dell'attività di intelligence, è necessario raccomandare la pronta definizione di una più ampia partecipazione dei servizi per l'informazione e la sicurezza della Repubblica alle occasioni e alle iniziative di coordinamento internazionale, in virtù della natura a-geografica e transnazionale della minaccia.

Ci si riferisce, in particolar modo:

- all'esigenza di individuare un punto di contatto nazionale per il « Network Security Incident Alert Mechanism – EU NSIAM », la cui costituzione è stata decisa dal Segretario Generale del Consiglio dell'UE, nelle more della creazione dei previsti organismi europei (incluso un CERT-UE) dedicati alla protezione delle infrastrutture critiche informatizzate;

- al processo in corso in ambito NATO – e segnatamente in seno al Working Group on Information Assurance del Comitato di Sicurezza dell'Alleanza Atlantica, cui pure partecipa l'UCSe – destinato verosimilmente a sollecitare gli Stati membri ad individuare un'Autorità nazionale di riferimento in materia.

Su entrambi i fronti, appare necessario raccomandare al Governo la pronta individuazione delle responsabilità nazionali di questi due processi multilaterali. Il DIS, che già partecipa sotto il profilo strategico e operativo al coordinamento delle attività di prevenzione e contrasto alla minaccia per la sicurezza nazionale, appare il riferimento istituzionale più idoneo.

Appare altresì prioritario, da parte degli apparati che compongono il sistema di informazione per la sicurezza della Repubblica, potenziare, nel rispetto delle previsioni della legge n. 124 del 2007, le attività legate alla cointroingerenza economica e finanziaria, all'intelligence economica (IE) e all'analisi delle fonti aperte (OSINT). I primi due aspetti sono cruciali per la tutela degli interessi del sistema economico-produttivo nazionale, reso più vulnerabile dalla interconnessione globale della rete e dalla dimensione internazionale delle sue attività. Il terzo aspetto è legato alla necessità di promuovere una specializzazione di analisi ed operativa circa la moltiplicazione di meccanismi e « luoghi » virtuali nei quali prendono forma le minacce.

Sotto il profilo tecnico, giuridico e normativo, al fine di rafforzare la capacità di contrasto alle minacce poste dall'utilizzo della rete da parte delle reti criminali transnazionali, si raccomanda alle istituzioni preposte di avviare una riflessione condivisa sulle pratiche emergenti di acquisizione e di conservazione dei dati telematici, con particolare riguardo a fenomeni quali il cloud computing o la proliferazione di server virtuali. È altresì importante che, tra autorità civili e organi giudiziari e inquirenti, vi sia una riflessione condivisa sui delicati profili legati alle operazioni di deep packet inspection (63), uno strumento che può essere utile in materia di tutela della sicurezza nazionale, ma che necessita di una adeguata disciplina di garanzia delle prerogative di privacy e riservatezza. Il delicato equilibrio tra tutela della privacy e capacità di garantire la sicurezza viene rapidamente compromesso dalla moltiplicazione delle fattispecie virtuali e dalla progressiva delocalizzazione degli asset informatici più rilevanti.

L'Italia presenta una base giuridica consistente e ampiamente efficace, che richiede però un costante aggiornamento, adeguatamente coordinato, da parte di chi opera a garanzia del diritto costituzionale della segretezza delle comunicazioni e di chi è chiamato a contrastare le minacce alla sicurezza nazionale o ai diritti individuali.

Sotto il profilo degli interventi, appaiono prioritarie le seguenti raccomandazioni:

– procedere al censimento delle banche dati di interesse nazionale, previa definizione del perimetro di interesse da parte dell'autorità politica; – favorire la cooperazione internazionale tra autorità di polizia e giudiziarie, al fine di garantire la piena tracciabilità delle reti criminali, la cui attività trovi origine fuori dai confini nazionali.

In via generale, come già invocato in precedenti occasioni da questo stesso Comitato parlamentare (64), si ritiene opportuno raccomandare al Governo il tempestivo avvio di un processo di analisi e valutazione delle priorità legate alla sicurezza della Repubblica.

L'assenza di una revisione strategica del perimetro di sicurezza nazionale comporta, direttamente e indirettamente, un investimento non ottimale in termini politici e di tutela degli interessi nazionali. Le caratteristiche, il rango e il posizionamento dell'Italia in uno scenario geopolitico e strategico in rapida e costante evoluzione richiedono l'elaborazione di una Strategia per la Sicurezza della Repubblica, che individui le priorità e le direttrici della politica estera, di sicurezza e difesa nazionale, rapportandone gli obiettivi alla consistenza delle risorse disponibili e avviando una pianificazione coerente con gli interessi di medio e lungo termine per il Paese.

Si tratta di una riflessione che dovrà trarre origine e impulso dalla Presidenza del Consiglio dei ministri, necessiterà della piena concertazione con le istituzioni e gli organi della Repubblica coinvolti nella tutela della sicurezza nazionale e dovrà trovare piena e compiuta elaborazione nella sede parlamentare. In tal senso, il ruolo dei nostri apparati di intelligence è assolutamente centrale e, come negli altri sistemi occidentali, deve essere valorizzato al massimo, perché si possa in tal modo allargare in maniera efficace lo spettro delle azioni di tutela della sicurezza e di contrasto alle nuove generazioni di minacce.

In un tale processo di revisione strategica delle priorità nazionali, il contrasto alle minacce alla sicurezza della Repubblica derivanti dallo spazio cibernetico dovrà occupare una priorità elevata, in linea con l'azione e la pianificazione degli alleati e dei partner transatlantici ed europei.

In tal senso, l'Italia dovrebbe farsi promotrice di un'azione di costruzione del consenso internazionale, volta a promuovere nelle più alte sedi multilaterali la redazione di un primo testo per un Trattato per il contrasto alle minacce cibernetiche statuali; uno strumento sovranazionale, cioè, in grado di contrastare la proliferazione dei centri e delle modalità offensive e, senza intaccarne la libertà di utilizzo e di accesso, la possibilità di utilizzare la rete quale strumento militare non convenzionale. Tale obiettivo potrebbe essere raggiunto anche attraverso la creazione di un Centro internazionale per la repressione e il controllo della proliferazione degli strumenti cibernetiche offensivi.

Pur nella certezza, come documentato dalla presente relazione, che buona parte delle attività criminali provenga da attori non statuali, una concreta disciplina delle relazioni tra governi, assieme ad una attività di monitoraggio e controllo sovranazionale, sarebbe un primo passo verso l'utilizzo cooperativo della rete, cui si sta contrapponendo lo scenario di una militarizzazione ad opera dei principali attori geopolitici. Una dinamica, quest'ultima, suscettibile di deteriorare le relazioni politiche e strategiche e di compromettere la ricerca di un ordine mondiale il più possibile improntato alla stabilità e alla cooperazione.

Un Trattato di disciplina dell'attività cibernetica di origine statale presuppone innanzitutto la consapevolezza piena della minaccia costituita dalla « guerra informatica », secondo le linee tracciate dal piano di revisione strategica promosso dalla NATO. In quest'ambito, l'Italia è chiamata a concorrere in sede politico-diplomatica al piano di azione congiunto per rispondere alla minaccia posta dal crimine cibernetico e dall'utilizzo militare della rete anche attraverso l'ampliamento del perimetro della « sicurezza collettiva » previsto dall'articolo 5 del Trattato sull'Alleanza Atlantica alle fattispecie di « attacco informatico ».

Note

(63) Tecnica di filtraggio dei pacchetti in transito sulla rete.

(64) Si veda la Relazione al Parlamento « La tratta di esseri umani e le sue implicazioni per la sicurezza della Repubblica », aprile 2009, www.parlamento.it