LE ESIGENZE AMERICANE IN MATERIA DI CYBER-TERRORISMO E CYBER-WARFARE

ANALISI STRATEGICA DELLE CONTROMISURE

STEFANO MELE

Le esigenze americane in materia di *cyber-terrorismo* e *cyber-warfare*.

Analisi strategica delle contromisure

Stefano Mele

Sommario

1.0 Introduzione

La continua ed ormai imprescindibile necessità di interconnessione di tutti i sistemi, informativi e non, impone ormai da alcuni anni una seria valutazione sulle minacce che da essa scaturiscono, a maggior ragione se poste sotto la lente della sicurezza nazionale e della solidità delle infrastrutture critiche.

Queste minacce, in continua evoluzione e crescita, possono essere non intenzionali o intenzionali, mirate e non mirate, nonché possono provenire da una varietà di fonti, come ad esempio i criminali, i terroristi, i Governi in conflitto, ma anche *hacker* e dipendenti interni "infedeli"[1].

Per la peculiarità del mezzo utilizzato, inoltre, questi potenziali aggressori hanno a disposizione una varietà strabiliante di tecniche, più o meno complesse, tali da rendere le loro azioni ancor più efficaci e di sicuro impatto (anche mediatico[2]). E' ormai nozione acquisita, infatti, che gli aggressori informatici non hanno quasi mai bisogno di essere fisicamente vicini ai loro obiettivi, così come i loro attacchi posso facilmente attraversare i confini nazionali. Il tutto con una inimmaginabile ed inusuale, almeno fino a pochissimi anni fa, probabilità di restare anonimi.

Per questi motivi, i rapporti inerenti gli incidenti relativi alla sicurezza informatica e delle informazioni da parte dei Governi di tutto il mondo sono in costante aumento, facendo registrare negli Stati Uniti d'America tra il 2006 ed il 2008 una crescita del 200%[3] e contribuendo a far percepire il "cyber-terrorismo" come una

---

[1] Per un'analisi approfondita sulla varietà delle minacce e delle fonti, nonché sulla loro "intenzionalità" o meno, si veda U.S. GOVERNMENT ACCOUNTABILITY OFFICE (GAO), "*Critical Infrastructure Protection: Multiple Efforts to Secure Control Systems Are Under Way, but Challenges Remain*", GAO-07-1036, september 2007.

[2] Un c.d. *defacement*, ad esempio, pone immediatamente sotto gli occhi di tutti i visitatori del sito la compromissione del sistema. Non solo, prendendo come esempio il terrorismo, ci possiamo accorgere facilmente come questo sia ormai diventato un vero e proprio "evento mediatico", per altro non più mediato dai mezzi di comunicazione. L'accessibilità delle tecnologie e l'incessante sviluppo di esse, infatti, ha fatto sì che terroristi e ribelli siano attualmente nella condizione di riprendere, modificare e caricare le loro azioni praticamente in tempo reale, senza bisogno della presenza di una "telecamera occidentale". Sull'argomento, si veda, STRATEGIC STUDIES INSTITUTE, "*Youtube war: fighting in a world of cameras in every cell phone and photoshop on every computer*", november 2009.

[3] PONEMON INSTITUTE, "*Cyber Security Mega Trends. Study of IT leaders in the U.S. federal government*", november 2009.

vera e propria minaccia per la sicurezza nazionale[4].

[4] Quest'esigenza, in verità, non è avvertita esclusivamente dagli Stati Uniti d'America. Numerosi Stati, infatti, si sono già dotati di uno o più documenti ufficiali di policy per il settore della cyber-sicurezza. In ordine cronologico, si prendano in considerazione: MINISTRY OF DEFENCE OF ESTONIA, "*Cyber Security Strategy*", 2008, in http://www.kmin.ee/files/kmin/img/files/Kuberjulgeoleku_strateegia_2008-2013_ENG.pdf; COMMISSION SUR LE LIVRE BLANC SUR LA DÉFENSE ET LA SÉCURITÉ NATIONALE, "*Le Livre blanc sur la défense et la sécurité nationale*", 2008, in http://www.livreblancdefenseetsecurite.gouv.fr/information/les_dossiers_actualites_19/livre_blanc_sur_defense_875/index.html. NATIONAL INFORMATION SECURITY POLICY COUNCIL, "*The Second National Strategy on Information Security. Aiming for Strong "Individual" and "Society" in IT Age*", 2009, in http://www.nisc.go.jp/eng/pdf/national_strategy_002_eng.pdf; SWEDISH EMERGENCY MANAGEMENT AGENCY, "*Information security in Sweden. Situational assessment 2009*", 2009, in http://www2.msb.se/Shopping/pdf//upload/Publikationsservice/MSB/0119_09_Information_security_in_Sweden.pdf AUSTRALIAN GOVERNMENT, "*Cyber Security Strategy*", 2009, in http://www.ag.gov.au/www/agd/agd.nsf/Page/CyberSecurity_CyberSecurity; U.S. GOVERNMENT, "*Cyberspace Policy Review. Assuring a Trusted and Resilient Information and Communications Infrastructure*", 2009, in http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf; CABINET OFFICE OF THE UNITED KINGDOM, "*Cyber Security Strategy of the United Kingdom. Safety, security and resilience in cyber space*", 2009, in http://www.cabinetoffice.gov.uk/media/216620/css0906.pdf; COMMISSION OF THE EUROPEAN COMMUNITIES, "*Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience*", 2009, in http://ec.europa.eu/information_society/policy/nis/docs/comm_ciip/comm_en.pdf; NATO PARLIAMENTARY ASSEMBLY, "*Committee Report 173 DSCFC 09 E bis - NATO and Cyber Defence*", 2009, in http://www.nato-pa.int/default.Asp?SHORTCUT=1782.

2.0 Le principali minacce cibernetiche dal 2006 ad oggi

Sebbene in Italia i recenti attacchi informatici ai siti dell'Aereonautica Militare e delle Poste Italiane possano certamente evidenziare una significativa *escalation*[5], anche nel nostro Paese, dei continui sforzi che le nazioni estere ed i gruppi criminali stanno profondendo nel colpire le reti governative ed alcune infrastrutture particolarmente sensibili del settore privato, è certamente agli Stati Uniti d'America che si deve volgere lo sguardo per comprendere a pieno l'evoluzione di questo *trend* e le possibili – ed ormai imprescindibili – contro-offensive.

Secondo il *Center for Strategic and International Studies* (CSIS), infatti, nel ristretto arco temporale di 3 anni (2006-2009), sono stati ben 44 i più significativi "*cyber-incidents*", il 30% dei quali avvenuti nel solo anno 2009[6], che hanno colpito con successo enti pubblici statali, della Difesa e società tecnologiche, ovvero crimini di natura economica con perdite per oltre 1 milione di dollari.

Citando, invece, i dati forniti dal *U.S. Strategic Command*, la *U.S.-China Economic and Security Review Commission* ha evidenziato come in tutto il 2008 ci siano stati ben 54.640 attacchi informatici registrati dai sistemi del *Department of Defense* americano, laddove, nella sola prima metà dello scorso anno, gli attacchi sono stati già 43.785[7]. Ciò significa che, in sintesi, il 2009 si è chiuso con un numero complessivo di cyber-attacchi in crescita di circa il 60% rispetto al 2008[8]. Sebbene la maggior parte di questi abbia origine da sistemi informatici collocati in Cina, in Corea del Nord e nei Paesi della *ex* Unione Sovietica, allo stato attuale della tecnica risulta spesso molto complesso per gli esperti di sicurezza capire se questi attacchi informatici provenienti da indirizzi IP asiatici o russi siano stati commessi effettivamente, ad esempio, dalla

---

[5] L'Italia, allo stato attuale, non si è ancora allineata agli Stati europei precedentemente menzionati, non producendo, almeno ufficialmente, un documento strategico specifico per questo settore. Ad ogni modo, da ultimo, in un recentissimo intervento pubblico presso la *Link Campus University* di Roma, il Direttore generale del DIS (Dipartimento delle Informazioni per la Sicurezza), Prefetto Giovanni De Gennaro, ha affermato che "*è ormai opinione condivisa che il principale campo di sfida per l'intelligence del terzo millennio sarà quello della cybersecurity; e sarà lì che si confronteranno gli organismi informativi delle Nazioni più sviluppate, nella piena consapevolezza della vulnerabilità dei rispettivi sistemi-paese, allorché il mondo del web avrà totalmente permeato costumi e modelli comportamentali dei loro cittadini, delle loro aziende, delle loro infrastrutture critiche, dei loro sistemi di comunicazione, dei loro assetti economici e finanziari. La cybersecurity avrà allora la stessa valenza della difesa dal "nucleare" e forse anche di più, se si considerano i danni incalcolabili di un attacco informatico su larga scala.*", sottolineando così l'attenzione che le nostre Istituzioni pongono sul tema.
Il testo integrale della lezione del Prefetto Giovanni De Gennaro può essere consultato sul sito istituzionale, raggiungibile all'URL: http://www.sicurezzanazionale.gov.it/web.nsf/pagine/lezione_direttore_generale_dis

[6] CENTER FOR STRATEGIC AND INTERNATIONAL STUDIES (CSIS), "*Significant Cyber Incidents Since 2006*", november 2009.

[7] Nel 2000, invece, gli incidenti informatici segnalati sono stati soltanto 1.415. Si deve necessariamente tener presente, però, che questo sconcertante incremento è in parte dovuto anche alle accresciute capacità del Governo americano di individuare i c.d. *cyber-threats* e alla crescente attenzione sul tema da parte dell'opinione pubblica mondiale.

[8] U.S.-CHINA ECONOMIC AND SECURITY REVIEW COMMISSION, "*2009 Report To Congress of the U.S.-China Economic And Security Review Commission*", november 2009.

Cina, ovvero se i sistemi informatici cinesi siano stati utilizzati solo come "ponte" finale per mascherarne la reale provenienza[9].

Per completezza e per comprendere a pieno la portata e la trasversalità della minaccia, tra gli attacchi più rilevanti avvenuti tra il 2009 ed i primi mesi del 2010, è opportuno segnalare nel:

- gennaio 2009 ignoti criminali informatici, presumibilmente un'organizzazione della *ex* Unione Sovietica finanziata da Hamas o Hezbollah, hanno attaccato l'infrastruttura Internet di Israele nel corso dell'offensiva militare nella Striscia di Gaza, paralizzando attraverso 500.000 computer i siti della pubblica amministrazione;

- febbraio 2009 ignoti criminali informatici hanno attaccato e violato i sistemi della *Federal Aviation Administration* (FAA);

- gennaio/febbraio 2009 ignoti criminali informatici pakistani hanno compromesso 600 *computer* del Ministero degli Affari Esteri indiano;

- marzo 2009 alcuni ricercatori canadesi hanno reso pubblica la scoperta di un sistema di spionaggio informatico con base in Cina, probabilmente installato sulle reti informatiche governative di 103 Paesi;

- aprile 2009, sulle pagine del *Wall Street Journal*, viene evidenziata non solo la fragilità ad un attacco informatico degli impianti nazionali di energia elettrica degli Stati Uniti d'America, quant'anche viene sottolineata e registrata la violazione ed il furto da parte di ignoti dei *database* inerenti l'aereo militare F-35;

- maggio 2009 la *Homeland Security Information Network* (HSIN) è stata violata da ignoti intrusi;

- giugno 2009 la *John Hopkins University Applied Physics Laboratory*, che svolge ricerche classificate per il Dipartimento della Difesa americano e per la Nasa, ha subìto una violazione dei propri sistemi informatici;

---

[9] L'*IP Bouncing* è una tecnica molto comune in tutti gli attacchi informatici, consistente nel mascherare l'indirizzo IP (*Internet Protocol*) facendo "rimbalzare" il proprio segnale e le proprie informazioni attraverso più sistemi "terzi", precedentemente violati e che non effettuino alcuna registrazione (*log*) degli accessi e delle operazioni compiute su di essi.

Per un'analisi approfondita sul funzionamento del protocollo di comunicazione TCP/IP si rinvia a W. RICHARD STEVENS, "*TCP/IP Illustrated, Volume 1: The Protocols*", Addison-Wesley, 1994; W. RICHARD STEVENS e GARY R. WRIGHT, "*TCP/IP Illustrated, Volume 2: The Implementation*", Addison-Wesley, 1995; W. RICHARD STEVENS, "*TCP/IP Illustrated, Volume 3: TCP for Transactions, HTTP, NNTP, and the UNIX Domain Protocols*", Addison-Wesley, 1996; ANDREW S. TANENBAUM, "*Computer Networks (4th edition)*", Prentice Hall PTR, 2002; CRAIG HUNT, "*TCP/IP Network Administration*", O'Reilly, 1998; DOUGLAS E. COMER, "*Internetworking with TCP/IP - Principles, Protocols and Architecture (4th edition)*", Prentice Hall PTR, 2000.

Per un'introduzione, invece, sulle metodologie informatiche per il rintraccio di attacchi informatici "mascherati", si prenda in considerazione R. STONE, "*CenterTrack: an IP overlay network for tracking DoS floods*" in *Proceeding of the 2000 USENIX Security Symposium*, pag. 199-212, Denver, CO, July 2000; S. SAVAGE, D. WETHERALL, A. KARLIN E T. ANDERSON, "*Pratical network support for IP traceback*" in *Proceedings of the 2000 ACM SIG-COMM Conference*, pag. 295-306, Stockholm, Sweden, August 2000; H. BURCH E B. CHESWICK, "*Tracing anonymous packets to their approximate source*" in *Proceedings of the 2000 USENIX LISA Conference*, pag. 319-327, New Orleans, December 2000; D. DEAN, M. FRANKLIN E A. STUBBLEFIELD, "*An algebraic approach to IP traceback*", in *Proceedings of the 2001 Network and Distributed System Security Symposium*, San Diego, CA, February 2001; D. SONG E A. PERRING, "*Advanced and authenticated marking schemes for IP traceback*" in *Proceeding of the 2001 IEEE INFOCOM Conference*, Anchorage, AK, April 2001.

- luglio 2009 numerosi attacchi informatici di tipo *Distribuited Denial of Service* sono stati perpetrati alle infrastrutture ed ai siti governativi degli Stati Uniti d'America e della Corea del Sud, presumibilmente, dalla Corea del Nord;

- agosto 2009 Albert Gonzalez è stato incriminato per aver rubato tra il 2006 ed il 2008, insieme ad alcuni ignoti complici russi o ucraini, circa 130 milioni di carte di credito e di debito attraverso sistematiche violazioni dei sistemi informatici di 5 grandi imprese americane, commettendo la più importante violazione di sistemi informatici ed il più grande furto di identità della storia degli Stati Uniti d'America;

- dicembre 2009 il quotidiano *The Wall Street journal* ha riportato la notizia che i sistemi informatici di una tra le maggiori banche americane sono stati violati da ignoti *hacker*, causando una perdita economica di circa 10 milioni di dollari;

- gennaio 2010 il colosso dei motori di ricerca Google ha denunciato una profonda violazione nella sicurezza dei propri sistemi informatici e di quelli di una trentina di altre rilevanti Società americane. Google ha attribuito la responsabilità degli attacchi alla Cina;

- gennaio 2010 un gruppo noto con il nome di "*Iranian Cyber Army*" ha violato i sistemi informatici ed interrotto i servizi del noto motore di ricerca cinese *Baidu*. Gli utenti in navigazione sono stati reindirizzati ad un'ulteriore pagina *web* contenente un messaggio a sfondo politico inneggiante all'Iran (messaggio sostanzialmente identico a quello lasciato nel dicembre 2009 sempre dallo stesso gruppo dopo aver violato i sistemi di *Twitter*, noto *social network*).

Anche solo questi accenni, peraltro senza alcuno scopo di completezza, ai più importanti e recenti attacchi perpetrati attraverso l'uso della rete Internet, pongono immediatamente in risalto non solo l'attenzione che questo tema si è guadagnato (e si guadagnerà sempre più) nel giro di pochissimo tempo, quanto, per di più, l'estrema capillarità e diffusione degli attacchi stessi, per contrastare i quali occorre una strategia di risposta multi-livello ben precisa e solida.

3.0 Le principali tipologie di attacchi informatici

Nell'ottica di inquadrare il problema delle minacce informatiche alle infrastrutture critiche degli Stati, occorre effettuare un seppur minimo – ed alquanto semplicistico – richiamo ai principali cyber-attacchi attualmente commessi sfruttando la rete Internet, precisando che la catalogazione è effettuata in ordine alfabetico e non per importanza e/o frequenza del singolo attacco, ovvero che la complessità di alcune azioni di pirateria informatica – nel pratico – comportano l'applicazione combinata e coordinata di una o più tecniche di seguito elencate:

Denial of service (o DoS)

E' un metodo di attacco, proveniente da una singola "sorgente", che ha come obiettivo quello di portare il funzionamento di un sistema informatico che fornisce un servizio (ad esempio un sito *web*) al limite delle prestazioni, lavorando su uno dei parametri d'ingresso, fino a renderlo non più in grado di erogare il servizio. Gli attacchi vengono abitualmente attuati inviando molti pacchetti di richieste – di solito ad un *server Web*, *FTP* o di posta elettronica – saturandone le risorse e rendendo tale sistema "instabile". Sfruttando i servizi disponibili sulla macchina bersaglio, qualsiasi sistema collegato ad Internet e che fornisca servizi di rete basati sul TCP è soggetto al rischio di attacchi di tipo *Denial of Service*.

Distributed denial of service (o DDoS)

E' la variante più comune del *DoS* visto in precedenza, che ne amplifica esponenzialmente gli effetti, poiché, per portare l'attacco, sfrutta un'intera "rete" coordinata e distribuita di sistemi informatici e non una singola "sorgente".

Exploit tools

Sono strumenti (*tools*), più o meno sofisticati e spesso liberamente disponibili al pubblico, sfruttati dai criminali informatici per scovare le vulnerabilità dei sistemi telematici e per guadagnarne indebitamente l'accesso.

Logic bombs

E' una forma di sabotaggio elettronico, che consiste nell'inserire una porzione di codice malevolo all'interno di un qualsiasi programma apparentemente innocuo. Il programmatore fa sì che il *software* esegua

un'azione distruttiva (modificare, cancellare *file*, bloccare il sistema o svolgere qualsiasi altra operazione dannosa) quando un evento, precedentemente previsto, si verifica all'interno del sistema.

Phishing

E' un'attività illecita che, sfruttando una tecnica di ingegneria sociale, ha come obiettivo quello di ottenere l'accesso alle informazioni personali o riservate degli utenti al fine di rubarne l'identità. Viene eseguita mediante l'utilizzo delle comunicazioni elettroniche, soprattutto messaggi di posta elettronica fasulli o messaggi istantanei, ma non per mezzo di contatti telefonici (per questo caso si veda, successivamente, il "*Vishing*"). Grazie ad *e-mail* che imitano perfettamente la grafica ed il logo dei siti istituzionali, l'utente è ingannato e portato a rivelare dati personali, come il numero di conto corrente, il numero di carta di credito, i suoi codici di autenticazione (*username* e *password*), ecc.

Sniffer

Contrazione di "*packet sniffer*", sono programmi volti all'intercettazione passiva e all'analisi dei dati che transitano su una rete telematica, al fine di acquisire fraudolentemente *password* o altre informazioni sensibili degli (ignari) utenti di quel medesimo segmento di rete (spesso una rete interna aziendale).

Trojan horse

Un *trojan* o *trojan horse*, in italiano "Cavallo di Troia", è un tipo di *malware*. Deve il suo nome al fatto che, come con il mitico stratagemma inventato da Ulisse, le sue funzionalità sono nascoste all'interno di un programma apparentemente utile. E' dunque l'utente stesso che, installando ed eseguendo un certo programma, inconsapevolmente installa ed esegue anche il codice malevole in esso nascosto.

Virus

E' un programma che è in grado, una volta eseguito, di infettare alcune tipologie di *file* in modo da riprodursi e fare più copie possibili di sé stesso, generalmente senza farsi rilevare dall'utente. Nell'uso comune, il termine *virus* viene frequentemente ed impropriamente usato come sinonimo di *malware*, indicando quindi di volta in volta anche categorie di programmi malevoli diversi, come ad esempio *worm* o *trojan*.

Vishing

E' un'evoluzione del *phishing*, effettuato però utilizzando i servizi di telefonia VoIP (*Voice over IP*), simulando, ad esempio, un *call center* di una banca ed invitando la vittima a fornire i propri dati

all'operatore. Questa pratica fa leva sempre sull'ingegneria sociale e sulla maggiore fiducia che si dà ad una persona che sembra essere autorizzata a richiedere tali informazioni.

War driving

E' un'attività volta ad individuare reti informatiche sfruttando la presenza di accessi *wireless* (senza fili). Consiste nell'intercettare reti *Wi-Fi* utilizzando un *laptop*, solitamente abbinato anche ad un ricevitore GPS per rilevare con precisione l'esatta posizione geografica della rete appena scoperta. Il *wardriving* in sé consiste esclusivamente nel trovare *Access Point* (AP) e registrarne la posizione. Alcune persone, però, infrangono le scarse misure di sicurezza tipiche di queste reti per accedere anche ai file personali degli utenti dei sistemi collegati a quella rete o per sfruttare la connessione ad Internet del sistema bersaglio per effettuare ulteriori attacchi esterni, garantendosi in questo modo il quasi totale anonimato.

Worm

E' un *software* indipendente che si riproduce e propaga da un sistema infetto all'altro attraverso una rete (come, ad esempio, Internet). A differenza dei virus informatici, un *worm* non richiede l'intervento dell'utente per propagarsi, essendo capace di sfruttare una o più vulnerabilità dei programmi o servizi presenti sul sistema bersaglio.

Zero-day exploit

Lo *zero-day* è un tipo di attacco informatico che inizia nel "giorno zero", ovvero nel momento in cui è scoperta una falla di sicurezza in un sistema. Questo tipo di attacco può mietere molte vittime, proprio perché è lanciato quando ancora non è stato distribuito alcun aggiornamento di sicurezza (*patch*) e quindi i sistemi sono completamente scoperti contro questo genere di minaccia telematica.

4.0 Analisi della strategia americana in materia di "cyber-security"

Nel febbraio 2009, il Direttore della *National Intelligence* (DNI) americana ha annunciato che alcune nazioni straniere e varie organizzazioni criminali internazionali hanno proclamato come obiettivo principale quello di colpire le reti informatiche del governo americano e di alcune realtà private di primissimo rilievo, al fine di ottenere un vantaggio competitivo attraverso la loro manomissione o distruzione, e inoltre che alcuni gruppi terroristici hanno espresso l'intenzione di avvalersi di attacchi informatici per colpire nuovamente al cuore gli Stati Uniti d'America[10].

Queste strategie di attacco, come abbiamo visto spesso non solo teoriche, possono essere imbastite anzitutto perché i sistemi informatici, anche quelli più critici, continuano a prestare il fianco a numerose debolezze nella gestione dei controlli più rilevanti. Negli ultimi anni, infatti, la maggior parte delle Agenzie non ha implementato le giuste procedure per prevenire, limitare ed identificare gli accessi non autorizzati alle reti di computer, ai sistemi e, più in generale, alle informazioni sensibili.

In altre parole, per quanto possa sembrare semplicistico, gli attacchi informatici sono (e saranno) possibili esclusivamente finché i sistemi presenteranno delle debolezze. E' proprio per questo che, finché i Governi baseranno la loro forza militare ed economica sulle reti di *computer* e finché queste reti potranno essere raggiunte (e le informazioni fruite) anche dall'esterno, queste saranno ipoteticamente sempre vulnerabili o comunque a rischio. I criminali informatici, infatti, non hanno solo la possibilità di rubare informazioni, ma anche di impartire falsi comandi per ottenere dei malfunzionamenti dei sistemi informatici ovvero di "iniettare" informazioni contraffatte per ottenere dai sistemi (e dai loro utilizzatori) conclusioni sbagliate e decisioni inopportune. In quest'ottica, estrema importanza deve assumere l'identificazione del grado e delle condizioni sulla cui base permettere l'accesso dall'esterno alle reti, onde evitare il paradosso che sia l'organizzazione stessa, con una cattiva gestione delle sue politiche di sicurezza, e non la bravura dei criminali a decidere "quanto" essere vulnerabili alle minacce informatiche.

Per far questo, già da tempo, la Casa Bianca e le altre Agenzie federali hanno intrapreso diverse iniziative volte a migliorare la sicurezza delle informazioni. Tra queste le più rilevanti, ai fini di quanto si sta analizzando, sono:

- *Comprehensive National Cybersecurity Initiative*[11]: nel gennaio 2008, l'*ex* Presidente Bush ha dato il via ad una serie di iniziative volte ad aumentare principalmente la sicurezza del *Department of Homeland Security* (DHS), concentrandosi sulla protezione dai tentativi di intrusione e sulle politiche volte ad anticipare le minacce informatiche future;

- *The Information Systems Security Line of Business*: obiettivo di questa iniziativa, capeggiata *dall'Office of Management and Budget* (OMB), è quello di migliorare il livello di sicurezza dei sistemi informativi tra enti

[10] DIRECTOR OF NATIONAL INTELLIGENCE, "*Annual Threat Assessment of the Intelligence Community for the Senate Select Committee on Intelligence, statement before the Senate Select Committee on Intelligence*", february 2009.

[11] THE WHITE HOUSE, "National Security Presidential Directive 54/ Homeland Security Presidential Directive 23", january 2008.

pubblici e ridurne contestualmente anche i costi, attraverso la condivisione dei processi e delle *policy* per la gestione della sicurezza delle informazioni;

- *Einstein*: un *intrusion detection system* specificatamente ideato per analizzare le informazioni provenienti dai flussi informativi di rete delle agenzie federali che fanno parte del *network*.

Allo stato attuale, però, non ci sono studi approfonditi pubblici che affrontano la pianificazione, l'attuazione, lo stato di avanzamento e gli sforzi messi in atto in questa direzione.

Quel che è certo, tuttavia, è che il DHS, a cui la legge americana e le *policy*[12] demandano il compito di proteggere i sistemi informatici delle infrastrutture critiche americane, è ancora molto lontano dal soddisfare le responsabilità specifiche[13] di questo delicatissimo compito. In particolar modo, il Dipartimento non ha ancora attuato una vera e propria politica volta a:

- rafforzare le capacità di analisi e di *warning* in materia di minacce informatiche;

- migliorare la sicurezza informatica per il controllo delle infrastrutture critiche;

- rafforzare le proprie capacità di intervenire e contribuire in caso di disfunzione nei servizi Internet;

- ridurre le inefficienze organizzative;

- riuscire nella realizzazione di una sistema capace di identificare la minaccia partendo dalle azioni poste in essere dai criminali informatici;

- sviluppare degli specifici piani di settore capaci di far fronte alle minacce informatiche;

- mettere in sicurezza i sistemi informativi interni;

---

[12] L'*Homeland Security Act* del 2002, l'*Homeland Security Presidential Directive-7* ed il "*National Strategy to Secure Cyberspace*".

[13] Dall'analisi dei documenti precedentemente richiamati, le responsabilità del DHS in materia di cyber-sicurezza si possono schematizzare e sintetizzare in:

- elaborare un piano nazionale per la protezione delle infrastrutture critiche che includa la cyber-sicurezza;
- sviluppare ed incentivare le collaborazioni tra Agenzie federali, statali e locali, nonché con i maggiori rappresentanti in materia di sicurezza del settore privato;
- migliorare e rafforzare la condivisione delle informazioni tra pubblico e privato in materia di attacchi, minacce e vulnerabilità informatiche;
- sviluppare e potenziare le capacità nazionali di analisi e *warning* in materia di cyber-sicurezza;
- fornire e coordinare gli sforzi per le attività di risposta agli incidenti informatici e per la pianificazione delle attività di recupero da essi;
- identificare e valutare tutte le minacce informatiche e le vulnerabilità;
- sostenere gli sforzi per ridurre le minacce informatiche e le vulnerabilità;
- promuovere e sostenere la ricerca e lo sviluppo per rafforzare la sicurezza nel "cyberspazio";
- promuovere la conoscenza e le attività di sensibilizzazione su questi argomenti;
- promuovere le attività di formazione e di certificazione in questo settore;
- accrescere la sicurezza informatica del governo federale, statale e locale;
- rafforzare la sicurezza internazionale nel "cyberspazio";
- integrare la cyber-sicurezza con la sicurezza nazionale.

riuscendo, così, a sviluppare ed attuare solo alcuni aspetti dei compiti ad esso delegati[14].

[14] U.S. GOVERNMENT ACCOUNTABILITY OFFICE (GAO), "*Cyber Analysis and Warning: DHS Faces Challenges in Establishing a Comprehensive National Capability*", GAO-08-588, july 2008. Si veda anche, U.S. GOVERNMENT ACCOUNTABILITY OFFICE (GAO), "*Critical Infrastructure Protection: DHS Needs To Fully Address Lessons Learned from Its First Cyber Storm Exercise*", GAO-08-825, september 2008.

4.1 Il mancato rafforzamento delle capacità di analisi e di *warning* in materia di cyber-sicurezza

Consolidare le capacità di analisi e di *warning* in materia di cyber-sicurezza significa, anzitutto, avere la giusta potenzialità – principalmente tecnica e di uomini – per monitorare le attività che avvengono nella Rete alla ricerca di eventuali anomalie, per analizzare e studiare quelle eventualmente evidenziate al fine di comprendere se siano reali minacce, per avvertire tempestivamente i funzionari preposti e, nel caso, per rispondere alla minaccia individuata[15].

Questi quattro inscindibili aspetti però, allo stato attuale, non sono stati fattivamente integrati dal lavoro dell'US-CERT. Anzitutto, dalle analisi svolte emerge come l'US-CERT, pur avendo la possibilità di ottenere informazioni da numerose fonti informative esterne, non abbia finora predisposto delle precise linee guida per la loro gestione.

Peraltro, nel mentre di un'indagine finalizzata a comprendere se un'anomalia sia o meno una minaccia, non è stata ancora prevista alcuna attività parallela volta ad integrare questo lavoro con un'analisi predittiva sulle eventuali implicazioni o sui possibili futuri attacchi informatici rivenienti da quella specifica attività "anomala", così come manca completamente, a monte, la possibilità tecnica e di analisi utile per far fronte ad eventuali (e sempre più probabili) incidenti multipli e simultanei.

Peraltro, seppure l'organizzazione avesse in sé la capacità di informare, attraverso numerose tipologie di *warning* ed *alert*, sugli attacchi e le minacce che di volta in volta si presentano, nella maggior parte dei casi queste informazioni non vengono poi trasmesse in maniera tempestiva, sicché viene a mancare il tempo utile per un'adeguata valutazione ed una conseguente assunzione delle azioni/reazioni più opportune, senza considerare che spesso, agendo a posteriori, risulta molto più complesso riuscire a perseguire (anche legalmente) gli attacchi medesimi.

Infine, nell'atto di mitigare o reagire ad un attacco foss'anche proveniente da un limitato numero di soggetti ovvero di recuperare i danni subìti e rimediare alle vulnerabilità sfruttate dai criminali informatici, va detto che l'organizzazione ha palesemente evidenziato nel tempo l'incapacità di disporre delle risorse necessarie per far fronte e gestire contemporaneamente più incidenti in essere sul suo suolo nazionale.

[15] U.S. GOVERNMENT ACCOUNTABILITY OFFICE (GAO), "*Cyber Analysis and Warning: DHS Faces Challenges in Establishing a Comprehensive National Capability*", GAO-08-588, july 2008.

4.2 L'incapacità di ridurre le inefficienze organizzative

Sin dal 2008 il DHS si è sforzato di adottare le raccomandazioni di una commissione interna di esperti volta ad istituire un centro unico ed integrato di gestione delle operazioni di pianificazione e monitoraggio per le interruzioni e i disservizi sulla rete voce e dati, prevedendo di incorporare il *National Communication System* con il *National Cyber Security Division*[16]. Seppure questo obiettivo sia stato prefissato ormai da quasi due anni, il Dipartimento non ha ancora predisposto né un piano strategico, né, tantomeno, le relative linee guida per la reale integrazione dei due centri, limitandosi semplicemente a collocarli in uno spazio territoriale adiacente.

Questo comporta anche che, fino al momento in cui i due centri non saranno completamente integrati, il DHS potrebbe non essere capace di gestire efficacemente le attività di pianificazione e di controffensiva in caso di attacchi o di danni alle infrastrutture deputate alle comunicazioni, nonché di proteggere i dati e le applicazioni che su di esse viaggiano, aumentando così la probabilità di malfunzionamenti in caso di un effettivo bisogno.

[16] U.S. GOVERNMENT ACCOUNTABILITY OFFICE (GAO), "*Critical Infrastructure Protection: Further Efforts Needed to Integrate Planning for and Response to Disruption on Converged Voice and Data Networks*", GAO-08-607, june 2008.

4.3 Il mancato sviluppo di specifici piani di settore volti a far fronte alle minacce informatiche

Come si è avuto modo di analizzare finora, il DHS ha più volte fallito nell'adattare le infrastrutture nazionali alle raccomandazioni che nel tempo esperti interni e, soprattutto, entità terze hanno sollevato nell'ottica della protezione del suolo americano dalle minacce informatiche.

Nel merito bisogna senza dubbio evidenziare anche il mancato adeguamento alle critiche, da più parti sollevate, ai progetti di pianificazione del CIP (*Critical Infrastructure Protection*) in materia di cyber-sicurezza[17]. In più della metà di questi, infatti, manca completamente un processo volto ad identificare le potenziali conseguenze dei vari attacchi informatici che possono essere perpetrati nei confronti delle infrastrutture americane, così come non c'è traccia di una politica di *risk assessment* (valutazione del rischio), impedendo così che le parti interessate nei settori deputati alla protezione delle infrastrutture possano adeguatamente identificare e proteggere con le giuste priorità i propri *asset* critici[18].

[17] Nel gennaio del 2009 il DHS ha aggiornato il suo *National Infrastructure Protection Plan* (NIPP), redatto per la prima volta nel giungo del 2006 a seguito dell'*Homeland Security Act* e dell'*Homeland Security Presidential Directory-7* (HSPD-7). Per un'analisi sui cambiamenti del NIPP rispetto alla precedente versione del 2006 e su come il DHS e le principali Agenzie specifiche del settore si siano sforzati di implementare e pianificare la "*resiliency*" dei loro sistemi, si veda U.S. GOVERNMENT ACCOUNTABILITY OFFICE (GAO), "*Update to National Infrastructure Protection Plan Includes Increased Emphasis on Risk Management and Resilience*", GAO-10-296, march 2010.

[18] U.S. GOVERNMENT ACCOUNTABILITY OFFICE (GAO), "*Critical Infrastructure Protection: Sector-Specific Plans' Coverage of Key Cyber Security Elements Varies*", GAO-08-64T, october 2007; ed anche U.S. GOVERNMENT ACCOUNTABILITY OFFICE (GAO), "*Critical Infrastructure Protection: Sector-Specific Plans' Coverage of Key Cyber Security Elements Varies*", GAO-08-113, october 2007.

4.4 L'inefficace messa in sicurezza dei sistemi di informazione interni e di controllo delle infrastrutture

Già dal 2007 le Agenzie federali hanno intensificato gli sforzi per migliorare la sicurezza dei sistemi di controllo delle infrastrutture critiche incaricati del monitoraggio dei processi sensibili e delle procedure fisiche[19]. Proprio il DHS si è fatto promotore di alcune iniziative volte ad intensificare le attività di controllo della sicurezza in questo delicatissimo settore, al fine di promuovere non solo tutte quelle azioni necessarie ad aumentare la solidità – in termini di sicurezza – di questi sistemi, soprattutto attraverso strumenti di valutazione delle vulnerabilità e di risposta alle minacce, quant'anche nell'intrecciare in prima persona dei veri e propri rapporti di fiducia con i fornitori di questi servizi e con gli *owner* di queste attività[20].

Tuttavia il Dipartimento ha omesso di predisporre una strategia volta a coordinare le varie attività di controllo tra le Agenzie federali ed i fornitori privati, nonché, cosa ben più grave, ha trascurato la predisposizione di una specifica pianificazione volta ad ovviare alle intrinseche debolezze nel processo di condivisione delle informazioni sulle vulnerabilità dei sistemi di controllo.

Ne consegue che, finché gli sforzi del pubblico e del privato saranno coordinati da una strategia generica e carente proprio sotto il profilo della condivisione di informazioni[21], soprattutto di quelle così sensibili, non è da escludere un aumento del rischio che numerose organizzazioni, in assenza del processo di condivisione, conducano contemporaneamente il medesimo lavoro, perdendo così l'opportunità di portare a termine in maniera più efficace ed in minor tempo le loro missioni critiche.

---

[19] In realtà, sin dal 2002, al fine di garantire la protezione dei sistemi informatici federali dalle minacce telematiche, il *Federal Information Security Management Act* (FISMA) ha previsto un *framework* globale per garantire l'efficacia dei controlli di sicurezza delle informazioni sulle risorse poste a supporto delle operazioni federali e dei suoi *asset*. Questo *framework* crea un ciclo di attività di gestione del rischio molto simile a quello normalmente implementato dal settore privato, in questo caso: valutazione dei rischi -> istituzione di un "*focal point*" per la gestione centralizzata -> attuazione di politiche e procedure appropriate -> promuovere la consapevolezza, il monitoraggio e la valutazioni delle *policy*, nonché il controllo della loro efficacia.
Nonostante ciò, a distanza di 8 anni, se da un lato la maggior parte delle Agenzie federali continuano a segnalare un deciso *trend* positivo rispetto alle attività volte ad incrementare la consapevolezza in materia di sicurezza, dall'altro evidenziano enormi carenze sui controlli predisposti (o che sarebbero dovuti essere predisposti) in materia di sicurezza delle informazioni.

[20] U.S. GOVERNMENT ACCOUNTABILITY OFFICE (GAO), "*Critical Infrastructure Protection: Multiple Efforts to Secure Control Systems Are Under Way, but Challenges Remain*", GAO-07-1036, september 2007.

[21] A mero titolo esemplificativo, ciascuno dei sistemi informatici interconnessi del Dipartimento della Difesa americano (DoD), prima di poter operare all'interno della rete della Difesa, deve necessariamente soddisfare le richieste di certificazione ed accredito in materia di sicurezza esplicitate nel DoD Instruction (DoDI) 8510.01, "*DoD Information Assurance Certification and Accreditation Process (DIACAP)*" del 2007. Un'efficiente analisi dei rischi e delle procedure in merito può essere ricavata dalla lettura di RAND CORPORATION, "*Implications of Aggregated DoD Information Systems for Information Assurance Certification and Accreditation*", 2010, in http://www.rand.org/pubs/monographs/MG951/

5.0 Conclusioni

Alla luce di quanto fin qui analizzato, non si può sottacere, comunque, che il potere esecutivo americano, prima con la *Comprehensive National Cybersecurity Initiative* e poi, sotto l'attuale amministrazione Obama, attraverso il *National Security Council* e l'*Homeland Security Council*, ha più volte provato ad effettuare una valutazione capillare delle *policy* in materia di cyber-sicurezza, ma con risultati attualmente poco soddisfacenti. Anche il recentissimo *report* "*Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure*", infatti, raccomanda ed auspica in maniera chiara la nomina di un funzionario della Casa Bianca come coordinatore delle politiche e delle attività in materia di cyber-sicurezza[22], nonché la scrittura di una nuova (e migliore) strategia nazionale[23] e lo sviluppo di un *framework* per la ricerca e lo sviluppo nel settore della sicurezza informatica, ben evidenziando ed avvalorando così, ancora una volta, le importanti lacune fin'ora emerse[24].

In conclusione, nel tentativo di contrastare le crescenti minacce informatiche alle infrastrutture critiche nazionali, il DHS ha certamente previsto una serie di processi e funzionalità di analisi e di *warning*, certamente efficaci, come il monitoraggio del traffico Internet sull'intero territorio e l'emissione periodica di avvisi in materia di sicurezza informatica per i *partner* nazionali e non.

Tuttavia, laddove il DHS, la Casa Bianca, l'OMB ed alcune Agenzie federali, con i progetti precedentemente analizzati, hanno posto le basi per sostenere il lavoro dell' US-CERT nell'assolvimento del compito che gli è stato attribuito, proprio questo, contestualmente, pare non riuscire ancora a supportare ottimamente, soprattutto da un punto di vista tecnico, le esigenze americane di sicurezza nazionale. Manca, infatti, una visione globale delle necessità (anche di base) utili a permettere una reale protezione delle informazioni e delle infrastrutture critiche degli Stati Uniti d'America, nonché risulta ampiamente insufficiente il controllo effettivo ed in tempo reale dei sistemi informatici di queste infrastrutture. Difetta, inoltre, delle capacità e delle procedure utili a permettere che i *warning* emessi siano tempestivi ed immediatamente "azionabili",

---

[22] Da ultimo, il Presidente Obama si è mosso in questa direzione, istituendo il *Cyber Command*, al cui vertice è stato incaricato il Direttore dell'NSA, Lt. Gen. Keith Alexander. Proprio in una sua recente audizione dinanzi al *Senate Armed Services Committee* americano, il Lt. Gen. Alexander, discutendo degli ipotetici scenari di *cyber-warfare* e dell'eventuale capacità di difesa delle infrastrutture USA, della complessità dei problemi connessi e su chi debba decadere la responsabilità oggettiva della suddetta difesa, ha confermato che giornalmente sono "centinaia di migliaia" i tentativi di scanning provenienti da ogni dove con l'obiettivo specifico di verificare la presenza di eventuali vulnerabilità da sfruttare per violare la sicurezza delle infrastrutture critiche americane. I documenti completi dell'audizione possono essere consultati su http://armed-services.senate.gov/testimony.cfm?wit_id=9315&id=4505

[23] Esigenza avvertita anche dal U.S. GOVERNMENT ACCOUNTABILITY OFFICE (GAO), "*National Cybersecurity Strategy: Key Improvements Are Needed to Strengthen the Nation's Posture*", GAO-09-432T, march 2009.

[24] THE WHITE HOUSE, "*Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure*", may 2009.

così come scarseggiano le risorse, tecniche e umane, per far fronte alle attività di mitigazione e ripristino dei sistemi in caso di incidenti informatici multipli e simultanei sul territorio nazionale[25].

Sul piano squisitamente tecnico occorre evidenziare con forza che i processi e le tecnologie esistenti non riescono attualmente a fare un buon lavoro nel settore dell'*intelligence* applicata alla cyber-sicurezza. Le applicazioni presenti sul mercato e gli sviluppatori di *software*, infatti, sono ancora troppo concentrati sulla protezione del perimetro di una specifica rete informatica. La maggior parte degli strumenti di sicurezza attualmente a disposizione, peraltro, si basano su un sistema di "firme" attraverso le quali riconoscere la minaccia in essere fallendo, però, nel riconoscimento e nell'individuazione delle minacce emergenti, derivate da quelle già conosciute ovvero identificabili nell'ottica di un sistema più complesso di interazione, come ad esempio quello discendente dagli equilibri internazionali tra Stati o dalle organizzazioni criminali strutturate. Tra l'altro, nel mondo interconnesso di oggi, può spesso risultare davvero impossibile stabilire con certezza quali siano i "perimetri" ed i confini di una determinata informazione o dove in un preciso momento uno specifico dato realmente si trovi. I sistemi informatici attuali di rilevamento delle intrusioni (*intrusion detection systems*), così come tutti gli altri *tools* basati su "firme", quindi, costringono gli operatori di sicurezza a lavorare, anche nel campo dell'*intelligence*, su ciò che già conoscono (ad esempio, una violazione della sicurezza già portata a segno) e non su quello che potrebbe accadere successivamente a quell'attacco ed in futuro.

In quest'ottica, occorre non soltanto ridisegnare la gestione della sicurezza in ambienti critici utilizzando schemi che non si limitino solo a "fotografare" ciò che già è avvenuto, ma che riescano a tracciare una "strada evolutiva" (se non un vero e proprio "*forecast*") della minaccia informatica, quanto, soprattutto, spingere urgentemente sulla condivisione sistematica delle informazioni tra personale addetto alle operazioni di sicurezza ed i *chief information officers* (CIO).

[25] Anche se, agli inizi del 2009, l'US-CERT ha pianificato di aumentare il proprio personale, ingaggiando altri 80 "*cyber-analysts*", e di incrementare la frequenza dei *test* e delle esercitazioni volte a migliorare l'efficienza della sua capacità di risposta agli attacchi informatici.

Note biografiche

Stefano Mele – Avvocato specializzato in Diritto delle Tecnologie Informatiche, Sicurezza ed Intelligence. Dottore di ricerca presso l'Università degli Studi di Foggia.

Vive e lavora a Milano dove svolge attività di consulenza per grandi aziende, anche multinazionali, sulle problematiche legali inerenti la Privacy e la protezione dei dati personali, Internet e i computer crimes. Per questi specifici settori ha redatto numerose pubblicazioni e approfondimenti per volumi, riviste e siti specializzati.

E' altresì esperto di sicurezza, cyber-terrorismo e cyber-warfare. E' senior researcher del Dipartimento di Studi d'Intelligence Strategica e Sicurezza della Link Campus University di Roma, nonché docente del loro "Master in Studi d'Intelligence e Sicurezza Nazionale" per i moduli relativi al cyber-terrorismo ed al cyber-warfare.

E' socio fondatore e vice presidente del Centro Studi Informatica Giuridica di Foggia (CSIG-Foggia) e Sector Director "Intelligence and Electronic Spying" dell'Istituto Italiano per la Privacy.