CAMERA DEI DEPUTATI **SENATO DELLA REPUBBLICA**

XVI LEGISLATURA

Doc. **XXXIV**
n. **4**

COMITATO PARLAMENTARE PER LA SICUREZZA DELLA REPUBBLICA

(istituito con la legge 3 agosto 2007, n. 124)

(composto dai deputati: *D'Alema,* Presidente; *Pastore,* segretario, *Briguglio, Cicchitto e Rosato* e dai senatori: *Esposito,* Vicepresidente*; Caforio, Passoni, Quagliariello* e *Rutelli*)

RELAZIONE

sulle possibili implicazioni e minacce per la sicurezza nazionale derivanti dallo spazio cibernetico

(Relatore: sen. Francesco RUTELLI)

Approvata nella seduta del 7 luglio 2010

Trasmessa alle Presidenze delle Camere il 15 luglio 2010

STABILIMENTI TIPOGRAFICI CARLO COLOMBO

Camera dei Deputati - Senato della Repubblica

COMITATO PARLAMENTARE
PER LA SICUREZZA DELLA REPUBBLICA

IL PRESIDENTE

Signor Presidente,

nella seduta del 7 luglio scorso il Comitato che presiedo ha approvato all'unanimità la "Relazione sulle possibili implicazioni per la sicurezza nazionale derivanti dall'utilizzo dello spazio cibernetico", a conclusione di un approfondito lavoro che si è sviluppato a partire dall'8 settembre 2009.

Nella medesima seduta il Comitato ha, altresì, deciso - ai sensi degli articoli 35 e 37, comma 2, della legge n. 124 del 2007 - di rendere pubblica la relazione, deliberandone la presentazione al Parlamento.

In adempimento del voto espresso dal Comitato mi onoro, pertanto, di trasmettere la relazione a Lei e al Presidente del Senato della Repubblica.

L'occasione mi è gradita per rinnovarLe i sensi della mia più alta considerazione.

On. Gianfranco FINI
Presidente della
Camera dei Deputati

Camera dei Deputati - Senato della Repubblica

COMITATO PARLAMENTARE
PER LA SICUREZZA DELLA REPUBBLICA

IL PRESIDENTE

Signor Presidente,

nella seduta del 7 luglio scorso il Comitato che presiedo ha approvato all'unanimità la "Relazione sulle possibili implicazioni per la sicurezza nazionale derivanti dall'utilizzo dello spazio cibernetico", a conclusione di un approfondito lavoro che si è sviluppato a partire dall'8 settembre 2009.

Nella medesima seduta il Comitato ha, altresì, deciso - ai sensi degli articoli 35 e 37, comma 2, della legge n. 124 del 2007 - di rendere pubblica la relazione, deliberandone la presentazione al Parlamento.

In adempimento del voto espresso dal Comitato mi onoro, pertanto, di trasmettere la relazione a Lei e al Presidente della Camera dei deputati.

L'occasione mi è gradita per rinnovarLe i sensi della mia più alta considerazione.

Sen. Renato SCHIFANI
Presidente del
Senato della Repubblica

PAGINA BIANCA

INDICE

PAGINA BIANCA

AVVERTENZA

Il Comitato parlamentare per la sicurezza della Repubblica ha svolto un'indagine approfondita su una delle questioni che più condizionerà lo scenario di sicurezza internazionale e nazionale nel prossimo futuro. La diffusione esponenziale dei sistemi e degli strumenti informatici e tecnologici porta con sé anche una maggiore vulnerabilità delle infrastrutture critiche nazionali, oltre che mettere a rischio le tutele della riservatezza e delle libertà dei cittadini, accrescere lo spazio di manovra delle organizzazioni criminali, creare un'area porosa nell'attività di salvaguardia della proprietà intellettuale, dei segreti industriali e delle informazioni che attengono la sicurezza nazionale.

La presente Relazione riferisce sugli esiti di tale indagine. Si articola in una premessa di sintesi delle nuove problematiche strategiche riferite ai compiti del Comitato; nella descrizione dell'attività svolta; nell'illustrazione delle caratteristiche del fenomeno a livello globale; nell'analisi delle ricadute per il nostro Paese; nella presentazione delle principali risultanze delle attività di intelligence*; nella 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.*

PAGINA BIANCA

1. Premessa.

Nelle relazioni internazionali e strategiche, la cifra di questo inizio di XXI secolo è l'interdipendenza. Sotto il termine generico di « globalizzazione » ricade una vasta serie di declinazioni che coinvolgono attori statuali e non, privati cittadini, imprese e istituzioni. Il compito di proteggere la sicurezza nazionale si fa, per questo, sempre più complesso, mentre si afferma il principio che vede la sicurezza emergere come un « bene » sempre più indivisibile, nella sua dimensione orizzontale e verticale.

La tutela collettiva della sicurezza ha come primo obiettivo la galassia delle minacce non-statuali, o asimmetriche, la cui pericolosità cresce proporzionalmente alla moltiplicazione dei possibili strumenti di offesa. È il caso del terrorismo di matrice integralista, il cui messaggio è meglio veicolato oggi anche grazie alla diffusione di internet e degli strumenti di comunicazione virtuale; o della minaccia posta dalla proliferazione di armi di distruzione di massa, stimolata dalla capacità di sofisticazione delle reti criminali transnazionali o del terrorismo nel garantirsi l'accesso a tecnologie sensibili e segreti industriali.

Se nella lunga parentesi della Guerra Fredda la tecnologia è stata un fattore di superiorità strategica nella competizione tra le due superpotenze, impegnate anche a militarizzare lo spazio e a sviluppare reti informatiche che potessero servire le rispettive strategie militari, oggi sempre più l'accento si sposta sulla virtualizzazione delle relazioni internazionali e quindi, potenzialmente, dei conflitti.

Lo spazio cibernetico è un nuovo fondamentale campo di battaglia e di competizione geopolitica nel XXI secolo. Lo Stato nazionale, la cui sovranità viene erosa proprio dal processo di globalizzazione, può proiettare i propri interessi e dispiegare le proprie strategie difensive sulla grande « autostrada virtuale » costituita dal *web*, dalle reti di comunicazione, dai circuiti telematici, dai sistemi e dalle reti computerizzate. Non sono poche le analisi strategiche che evidenziano come le prossime guerre tra Stati non verranno più iniziate dalle Forze Armate, ma saranno concentrate su un massiccio utilizzo di attacchi informatici per sabotare preventivamente la capacità di risposta o di offesa degli avversari e per arrecare pesanti danni, non virtuali ma materiali. Al tempo stesso, nello spazio cibernetico si concentrano attori asimmetrici che, da soli, costituiscono una seria minaccia alla sicurezza delle Nazioni. Il grande spazio telematico globale, di dimensioni virtualmente infinite, è solcato anche da reti criminali organizzate, il cui obiettivo è di sottrarre denaro, truffare o raggirare a scopo di lucro cittadini ed organizzazioni; da movimenti del terrorismo fondamentalista, impegnati a cementare consenso, attrarre nuovi adepti o diffondere messaggi attraverso la rete; agenzie di spionaggio non governative, in grado di sottrarre informazioni rilevanti alla *business community*, falsando in questo modo la leale concorrenza.

La comunità internazionale oggi accetta il fatto che la protezione dell'atmosfera, dell'idrosfera, della litosfera e della biosfera – considerati « beni universali » – sia responsabilità di tutti i Paesi. La stessa

considerazione deve applicarsi alla « *cyber*-sfera », che è fondamentale per la nostra vita quotidiana, il nostro benessere materiale e la nostra sicurezza. In un'era in cui gli attacchi informatici stanno crescendo in tutto il mondo, il segretario di Stato Usa Hillary Clinton ha avuto ragione nell'affermare che un attacco ad una rete di computer di una nazione « può essere un attacco a tutte quante ». Queste aggressioni non fanno che ricordarci che il *cyber*-spazio, nuovo elemento costitutivo dei beni comuni, è già minacciato. Esso deve essere considerato come proprietà comune per il bene di tutti, proprio come lo spazio esterno, le acque internazionali e gli spazi aerei internazionali. E come succede per la pirateria oceanica e il dirottamento di aerei, il crimine informatico non dovrebbe restare impunito se vogliamo salvaguardare i nostri interessi condivisi e collettivi.

Prima del latino *gubernare*, i greci usavano la parola *kybernan* per indicare il comando; e *kybernos* corrispondeva al nostro « capitano ». Una definizione di questa minaccia, i cui attori, mezzi, fini e bersagli mutano più velocemente delle loro contromisure, può estrapolarsi dal « *Cyberspace Policy Review* », pubblicato dalla Casa Bianca nel giugno 2009, che rappresenta lo stato dell'arte della dottrina della sicurezza cibernetica degli Stati Uniti, ovvero delle politiche dell'Amministrazione tese alla « sicurezza e stabilità dell'infrastruttura globale delle informazioni e comunicazioni » (1).

Pur non avendo pretese di completezza, questa descrizione sembrerebbe tradirne una minore concretezza; testimonianza del fatto che, anche per le maggiori potenze, la formulazione di una dottrina coerente e unificata per contrastare le nuove minacce rimane un compito estremamente complesso, oltre che per le esigenze di riservatezza, a causa delle sue mille variabili, accresciute dalla mancanza di una « dottrina » codificata e accettata dalle parti in causa.

La molteplicità dei possibili autori di un attacco informatico e dei loro fini fa sfumare il valore dei parametri necessari per tarare e impostare una strategia di difesa. L'assenza di barriere all'ingresso, l'anonimato, l'asimmetria nella vulnerabilità dei bersagli implica una capacità diffusa di esercitare il potere e determina il superamento del tradizionale confronto tra Stati-Nazione come attori centrali delle relazioni internazionali, tre secoli e mezzo dopo il Trattato di Westphalia, che ne sancì la primazia.

Il passaggio da una potenza dominante all'altra nell'arena politica internazionale è un evento storicamente comune e conosciuto. La vera novità di questo XXI secolo è, invece, la frammentazione del potere. La tecnologia, per molto tempo, è stata propensa a favorire il consolidamento delle gerarchie politiche. La moderna tecnologia, prevalentemente a causa dei suoi bassi costi, sembra favorire il decentramento politico attraverso l'universalizzazione virtuale dell'uso del potere. Nel 1993 esistevano circa 50 siti internet; alla fine di quel decennio ne esistevano oltre 5 milioni. Nel 2010 solo in Cina si sono registrati 400 milioni di utenti. Nel 1980 le telefonate trasmesse dai fili di rame potevano « trasportare » appena una pagina di informa-

---

(1) « *Cyberspace Policy Review* », su www.whitehouse.gov, 6/2009.

zioni al secondo; oggi la fibra ottica può trasmettere 90.000 volumi in un secondo. Nel 1980 un gigabyte di massa di archiviazione occupava lo spazio fisico di una stanza; oggi, 200 gigabyte di informazioni sono trasportabili in una tasca, attraverso una *pendrive*.

Le strategie e le modalità della competizione sul *web* sono difficilmente conoscibili, in virtù di un mutamento costante determinato dal salto tecnologico.

Se la Guerra Fredda è finita dal punto di vista geopolitico e militare, non si può affermare altrettanto per il dominio informatico. La politica di distensione avviata dal presidente americano Barack Obama riguarda anche il *web*, con l'obiettivo dichiarato di scongiurare il pericolo di una *cyber*-guerra tra grandi potenze.

Il confronto tra le diplomazie di USA e Russia riguarda anche un'ipotesi di versione digitale del recente Trattato Start-2, firmato nell'aprile 2010 a Praga e che prevede il taglio del 30% nel numero delle testate atomiche disponibili per i due Paesi.

Già durante l'Amministrazione di George W. Bush, la Russia aveva avanzato la proposta di un accordo, in ambito ONU, per il controllo e la limitazione della proliferazione di agenti virtuali di distruzione, dai virus malevoli ai *software* per le incursioni e il sabotaggio di reti strategiche su vasta scala. Gli USA, in quella circostanza, accettarono solo di circoscrivere il negoziato alle cosiddette minacce asimmetriche, ovvero all'utilizzo della rete da parte delle organizzazioni criminali transnazionali. Oggi le prospettive di un accordo più largo sembrano più concrete, soprattutto se rapportate all'urgenza di mettere in atto un sistema difensivo non spurio, alla luce delle ambizioni crescenti esercitate dalle potenze informatiche emergenti, a cominciare dalla Repubblica Popolare cinese, l'India o l'Iran.

In particolare, le implicazioni della militarizzazione dello spazio cibernetico condotta dalla Cina sono state analizzate da numerosi studi e rapporti internazionali (2). In un rapporto presentato al Congresso dal Dipartimento della Difesa americano si evidenzia come la Cina sia in procinto di espandere la capacità di offesa militare dai tradizionali domini di terra, mare, cielo allo spazio cibernetico, con lo scopo di rendere vulnerabili le infrastrutture critiche dei principali concorrenti strategici e ridurre così il *gap* militare e tecnologico.

Sotto il profilo prettamente dottrinale, la proiezione cibernetica di Pechino è persino antecedente a quella delle più rilevanti e note rivoluzioni negli affari militari, a cominciare da quella americana. In un noto testo del 1999, gli alti vertici dell'Esercito cinese (PLA – *People's Liberation Army)* teorizzavano una forma di conflitto in grado di trascendere le frontiere e le distanze fisiche, attraverso l'utilizzo della rete telematica (3).

---

(2) Tra gli altri, si veda Brian Mazanec, « *The art of (cyber)war* », The Journal of International Security Affairs, dicembre 2009.

(3) Qiao Liang, Wang Xiangsui, « *Unrestricted Warfare* », Pan American Publishing Company, 2002.

Secondo uno studio dell'*Institute for Security Technolgy Studies* (4) del 2008, la Cina è la sola potenza emergente che abbia già sviluppato capacità operative nei cinque domini relativi alla superiorità cibernetica: elaborazione di una dottrina operativa, capacità addestrative, capacità di simulazione, creazione di unità addestrate alla guerra cibernetica, sperimentazione di attacchi *hacker* su larga scala. Rispetto a quest'ultimo punto, significativa è stata la campagna conosciuta con il nome in codice « *Titan Rain* »: tra il 2003 ed il 2005, centinaia di computer di uffici dell'Amministrazione americana e di governi dell'Europa occidentale furono sistematicamente attaccati da *hacker* i cui *server* di accesso alla rete, venne poi verificato, si trovavano nella provincia cinese del Guandong.

Alla base della capacità di Pechino rispetto allo spazio cibernetico c'è l'opzione strategica della deterrenza: lo scopo dei vertici militari asiatici è di dissuadere altre potenze dall'assumere una politica troppo aggressiva nei confronti di Pechino. Si tratta di una autentica rivoluzione negli affari strategici, poiché, fino ad oggi, il concetto di deterrenza era stato utilizzato esclusivamente con riferimento all'arma atomica e alla mutua dissuasione che ha congelato le possibili prove di forza militare tra le due superpotenze della Guerra Fredda.

L'estensione di tale dottrina allo spazio cibernetico rappresenta un vantaggio ed un limite allo stesso tempo. Essa è un vantaggio nella misura in cui non presenta lo stesso potenziale distruttivo di un attacco atomico (benché una combinazione tra le due cose non si possa escludere): appare piuttosto improbabile, a titolo di esempio, che la Cina possa rispondere ad una eventuale *escalation* militare con gli USA nello Stretto di Taiwan con la minaccia nucleare; ma potrebbe benissimo attivare un esercito di *cyber*-combattenti per infliggere danni notevoli al sistema di sicurezza americano. Il limite di tale estensione del perimetro strategico della deterrenza risiede nella difficoltà di renderla una dottrina simmetrica, che risponda cioè a criteri di logica estrema. Un attacco attraverso la rete potrebbe risultare difficilmente identificabile, non facilmente arrestabile e dalle conseguenze non completamente prevedibili.

Di fronte a questi rapidi sviluppi, i principali attori della scena mondiale sono impegnati ad assumere iniziative di difesa il più possibile efficaci. Con un provvedimento senza precedenti, il Senato americano ha approvato una legge che autorizza la Casa Bianca ad assumere pieni poteri di emergenza in caso di *cyber*-attacco alle infrastrutture strategiche del Paese (5). Il Parlamento ha redatto, con il supporto degli uffici governativi, una lista di *provider* internet, siti, autostrade telematiche e telefoniche considerate strategiche per la sicurezza nazionale. A tali operatori privati, il Presidente degli Stati Uniti potrà imporre lo spegnimento in caso di minaccia impellente alla sicurezza nazionale o di possibile perdita di vite umane. Tale

---

(4) http://www.ists.dartmouth.edu.

(5) « *Protecting cyberspace as a national asset Act* », S. 3480, giugno 2010, http://www.opencongress.org/bill/111-s3480/show.

provvedimento fa seguito alla revisione della strategia nazionale di protezione dello spazio cibernetico richiesta dal Presidente americano, che ha evidenziato le principali vulnerabilità del sistema nazionale, suggerendo possibili rimedi (6).

Gli attori che possono avvalersi dello strumento informatico per azioni ostili vanno dall'*hacker* individuale che agisce a scopo di lucro, fino all'apparato governativo che persegue obiettivi geopolitici o propagandistici, come nel caso degli attacchi informatici verso l'Estonia nel 2007, passando per la criminalità organizzata e i gruppi terroristici (7). Questi ultimi, ad esempio, usano il *cyber*-spazio per tutto lo spettro delle loro attività, dal reclutamento al finanziamento, alla propaganda e, in misura sempre maggiore, anche all'attacco informatico vero e proprio (8) teso a procurare un danno all'avversario. In definitiva, un attacco informatico può provenire pressoché da chiunque, per qualunque fine.

Lo stesso discorso vale per il ventaglio dei possibili bersagli. Dai conti correnti dei singoli cittadini alla sicurezza delle strutture più sensibili dello Stato, la crescente dipendenza dalle infrastrutture telematiche che pervade tutte le sfere della società rende virtualmente infiniti i potenziali obiettivi della minaccia cibernetica, e quindi le strutture da difendere.

A titolo di esempio, va notato come, nel loro rapporto annuale, reso pubblico il 21 giugno 2010, i servizi di *intelligence* tedeschi abbiano avvertito che due sono i principali rischi per la democrazia della Germania e la sua stabilità: l'estremismo politico e lo spionaggio industriale. L'*intelligence* federale punta il dito in particolare contro Cina e Russia, due Paesi descritti alla frenetica ricerca di *know-how* tecnologico e industriale e che vedono nel composito panorama industriale tedesco un terreno fertile per possibili incursioni informatiche e per la sottrazione di creazioni, segreti e brevetti. Dalla Cina, l'interesse riguarda soprattutto i processi produttivi, le scoperte scientifiche e i nuovi prodotti. Dalla Russia, invece, l'interesse è rivolto al grande settore energetico tradizionale o alternativo.

Secondo l'associazione tedesca delle imprese, il danno provocato dal *cyber*-spionaggio in Germania è in crescita esponenziale (9).

2. L'attività del Comitato parlamentare per la sicurezza della Repubblica.

Il Comitato parlamentare per la sicurezza della Repubblica, nel mese di settembre 2009, ha deliberato su proposta del presidente *pro-tempore* e relatore del presente documento, senatore Francesco Rutelli, l'inizio di un'attività di indagine sulle possibili implicazioni e

---

(6) « *Cyberspace policy review* », su www.whitehouse.gov.

(7) Per un elenco delle diverse possibili fonti di minacce informatiche prese in considerazione dallo *United States Computer Emergency Security Program* (US-CERT) si veda www.us-cert.gov.

(8) Vds. ad esempio: Directorate General External Policies of the EU, « *Cyber Security and Politically, Socially and Religiously Motivated Cyber Attacks* », 2/2009.

(9) Si veda: B. Romano, « *La Germania attacca le spie industriali* », Il Sole 24 Ore, 23 giugno 2010.

minacce per la sicurezza nazionale derivanti dall'utilizzo dello spazio cibernetico. È stato altresì stabilito di acquisire la consulenza di esperti per supportare utilmente il Comitato nella redazione di una completa Relazione al Parlamento sul tema.

Sono stati quindi affidati incarichi di consulenza alla società *Rand Europe Corporation*, per inquadrare il tema dal punto di vista strategico, tecnologico e normativo; al dottor Andrea Margelletti, presidente del Centro studi internazionale (CESI) con il compito di analizzare i rischi per la sicurezza nazionale del *cyber-crime* negli ambiti governativi e militari, e al dottor Alessandro Politi, analista OSINT, per l'analisi delle eventuali ricadute del *cyber-crime* sui settori civili ed economici, tra cui energia e servizi, telecomunicazioni, finanza e trasporti. Ha partecipato, inoltre, alla fase di elaborazione dei testi il dottor Gianluca Ansalone.

Il Comitato ha svolto le audizioni:

– il 2 dicembre 2009 del colonnello Umberto RAPETTO, comandante del Nucleo speciale frodi telematiche della Guardia di Finanza;

– il 16 marzo 2010 del prefetto Giovanni DE GENNARO, direttore generale del DIS;

– il 14 aprile 2010 del dottor Domenico VULPIANI, Consigliere per la sicurezza informatica e la protezione delle infrastrutture critiche della Polizia di Stato;

– il 28 aprile 2010 dei rappresentanti delle società Telecom (dottor Damiano TOSELLI), Vodafone (dottor Gaetano COSCIA), Wind (dottor Vincenzo FOLINO) e H3G (dottor Roberto COSA);

– il 18 maggio 2010 del dottor Raoul CHIESA, consulente dell'UNICRI;

– il 20 maggio 2010 dell'ambasciatore Giancarlo ARAGONA, nella sua qualità di membro del Gruppo di Riflessione Strategica della NATO, impegnato nella definizione del nuovo concetto strategico dell'Alleanza;

– il 1° luglio 2010 di un alto rappresentante del sistema di sicurezza di un governo europeo, con l'obiettivo di valutare le politiche di contrasto alla minaccia adottate in quel Paese.

Inoltre, in data 6 maggio 2010, il presidente del Comitato, onorevole Massimo D'Alema, d'intesa con il relatore, senatore Francesco Rutelli, ha inviato a soggetti istituzionali e società, individuati per la loro particolare e specifica competenza nel settore, una richiesta volta a conoscere le loro valutazioni « *sull'evoluzione della minaccia e le tendenze prevedibili; sulle strategie di prevenzione adottate sotto il profilo aziendale, sul contributo alla tutela delle infrastrutture critiche nazionali, nonché sulla qualità della collaborazione con le istituzioni preposte* ».

Tutti coloro che sono stati interpellati hanno fornito il loro contributo trasmettendo al Comitato un documento che è stato acquisito agli atti dell'indagine. In particolare:

• la Terna SpA ha trasmesso un elaborato dal titolo « Nota sui rischi alla sicurezza nazionale derivanti dal *cyber-crime* »;

• la Sogei ha trasmesso una « Nota riguardante il *cyber-crime*: strategie di prevenzione della minaccia »;

• la Finmeccanica ha inviato un elaborato dal titolo « *Cyber-security – Cyber warfare*. Definizioni, descrizione »;

• la RFI – Rete Ferroviaria Italiana ha inviato una relazione su « Strategie di Rete Ferroviaria Italiana per il contrasto al *cyber-crime* »;

• l'ENI ha trasmesso una « Nota di approfondimento sui rischi per la sicurezza nazionale derivanti dal *cyber-crime* »;

• l'ABI – Associazione bancaria italiana – ha inviato un elaborato dal titolo « Valutazioni in merito al fenomeno del *cyber-crime* nel settore bancario italiano »;

• Poste italiane ha inviato una relazione dal titolo « *Cybercrime* e *cybersecurity* »;

• il Garante per la protezione dei dati personali, professor Francesco Pizzetti, ha trasmesso il documento « Rischi derivanti dal *cyber-crime*: quadro nazionale e ruolo dell'Autorità ».

3. Sicurezza globale ed utilizzo dello spazio cibernetico: definire il fenomeno.

Il *cyber*-spazio non è più solo lo spazio di diffusione per i mezzi di comunicazione di massa, da quelli tradizionali a quelli a più elevate vocazioni innovative. Esso è piuttosto un nuovo continente, ricco di risorse ma anche di insidie. Di fronte alla crescente militarizzazione di questo spazio, i governi del pianeta – ed in particolare le grandi potenze – sono impegnati in una accelerata competizione. La Russia ha ereditato dall'URSS un sistema, noto con l'acronimo di Sorm-2, in grado di copiare in *backup* ed in tempo reale qualsiasi singolo *bit* (10) che transita nello spazio sovrano russo. La Cina ha attrezzato una rete difensiva nazionale, una sorta di enorme filtro in grado di scremare le informazioni di navigazione su internet considerate dannose, sgradite al governo centrale.

Negli anni '60 dello scorso secolo il primato strategico tra USA e URSS si affermava con le missioni spaziali e i satelliti spia; oggi la competizione per la sicurezza si sta spostando rapidamente sulle reti tecnologiche. Non a caso, la relazione annuale presentata nel 2010 al Comitato parlamentare per i servizi di informazione da Dennis Blair,

---

(10) *Binary digit* (cifra binaria): Unità di misura elementare di informazioni dei calcolatori.

allora direttore della *National Intelligence* americana pone la minaccia cibernetica al primo posto, per la crescita esponenziale della capacità di « rubare, corrompere, danneggiare o distruggere gli *asset* pubblici e privati essenziali per la nazione americana ».

Tocca a ciascun Paese, e anche all'Italia, occuparsi di queste minacce che incidono in maniera profonda su qualsiasi attività economica, sociale e istituzionale delle nostre comunità.

Chi ha una responsabilità pubblica nei sistemi democratici occidentali dovrà cercare di conciliare in maniera efficace la prevenzione delle minacce con il pieno godimento dei diritti di ciascun cittadino, tra cui rientrano quelli alla riservatezza delle comunicazioni e alla libertà di espressione e di pensiero.

I tre elementi costitutivi dello Stato nazionale sono direttamente coinvolti dal potenziale utilizzo per fini criminali delle reti informatiche: l'individuo, il sistema economico e le istituzioni.

Nel primo caso, possiamo considerare il criminale virtuale come una versione contemporanea del truffatore *d'antan* e la frode telematica come una diversificazione di portafoglio per i *network* criminali transnazionali, la cui capacità finanziaria è alimentata anche da questi circuiti.

Gli internauti e gli operatori economici sono i bersagli privilegiati di una congerie di criminali dal profilo molto diverso: dai variopinti *hacker*, eroi o anti-eroi della pubblicistica, fino a strutture ben organizzate e aggressive, che originano dalle mafie transnazionali, dalle reti di criminalità finanziaria e anche dalle reti terroristiche.

Ma è sul terreno della competizione strategica tra Stati che si gioca la posta più alta, che influirà sui nuovi equilibri internazionali.

Concettualmente, occorre acquisire un elemento importante: quei Paesi che definiscono pubblicamente strategie e meccanismi difensivi rispetto alle minacce cibernetiche sono in grado di organizzare in parallelo capacità offensive. Si stanno formando, cioè, dottrine di impiego che sono basate sulla capacità di attaccare un potenziale nemico, di azzerarne le difese e colpirne obiettivi strategici, anche come parte di pianificazioni di attacchi militari, senza che esistano definizioni condivise di questo nuovo spazio di competizione e potenziale contrapposizione strategica.

A sua volta, la sicurezza delle infrastrutture informatiche che assicurano il funzionamento delle linee critiche è divenuta una priorità nella ridefinizione della sicurezza nazionale: infrastrutture logistiche e di viabilità, reti elettriche e telefoniche, *pipeline* per il trasporto di idrocarburi, circuiti finanziari sono reti di sensibilità strategica per la vita di un Paese. Non meno sensibili dei comandi satellitari e dei sistemi di controllo del traffico aereo sono le reti e i dialoghi tra macchine che muovono generatori, dighe, ascensori, pompe, treni, piattaforme petrolifere. I *network* informatici e telematici ne rappresentano una metastruttura, una « rete delle reti », il cui danneggiamento può provocare il *black-out* delle operazioni, dalle più elementari a quelle vitali. Un attacco ai nodi sensibili di connessione tra questi *network* può « accecare » parti importanti dei sistemi esistenti. La novità delle minacce legate al *cyber*-spazio è che

esse rappresentano un'arma non convenzionale in grado di produrre effetti convenzionali (11).

La minaccia cibernetica ha conosciuto una graduale trasformazione che le ha conferito una dimensione propriamente strategica: ai singoli *hacker* si affiancano da tempo gruppi terroristici e criminali, mentre è più recente la crescente aggressività di attori statuali, i quali combinano posizioni meramente « difensive » – di reazione e contrasto agli attacchi – con quelle che annoverano anche misure controffensive.

Per semplificazione analitica ed interpretativa, è possibile suddividere la minaccia derivante dal *cyber*-spazio in quattro principali tipologie:

1) *cyber-crime*: ovvero l'insieme delle minacce poste da organizzazioni criminali nazionali o transnazionali, le quali sfruttano lo spazio cibernetico per reati quali la truffa, il furto d'identità, la sottrazione indebita di informazioni o di creazioni e proprietà intellettuali;

2) *cyber terrorism*: ovvero l'utilizzo della rete da parte delle organizzazioni terroristiche, a fini di propaganda, denigrazione o affiliazione. Particolarmente significativo è il caso della *cyber*-propaganda, ovvero della manipolazione delle informazioni veicolate nella rete a fini di denigrazione e delegittimazione politica, discriminazione sociale o personale. Nei casi estremi, si intende ipotizzare l'utilizzo sofisticato della rete internet o dei controlli telematici per mettere fuori uso, da parte di organizzazioni terroristiche, i gangli di trasmissione critica delle strutture o dei processi che attengono alla sicurezza nazionale;

3) *cyber espionage*: ovvero l'insieme delle attività volte a sfruttare le potenzialità della rete per sottrarre segreti industriali a fini di concorrenza sleale (se consumati nel mercato dei brevetti civili) o di superiorità strategica (nel caso di sottrazione di disegni e apparecchiature militari o *dual-use)*;

4) *cyber war*: ovvero lo scenario relativo ad un vero e proprio conflitto tra Nazioni, combattuto attraverso il sistematico abbattimento delle barriere di protezione critica della sicurezza dell'avversario, ovvero attraverso il disturbo o lo « spegnimento » delle reti di comunicazione strategica, e l'integrazione di queste attività con quelle propriamente belliche.

La difficile tracciabilità degli attacchi rende molto complessa la prevenzione della minaccia, se non attraverso adeguati scudi di

---

(11) Nel suo libro « *Cyber War* », Richard A. Clarke – che ha collaborato alla Casa Bianca con gli ultimi Presidenti USA – osserva: « Organizzazioni militari e di *intelligence* stanno preparando il campo di *cyber*-battaglia con strumenti chiamati « *logic bombs* » e « *trapdoors* », piazzando esplosivi virtuali in altri Paesi in tempo di pace. Data la natura unica della *cyber war*, ci possono essere incentivi ad attaccare per primi. I più probabili bersagli sono di natura civile. La velocità con cui possono essere colpiti, a migliaia, quasi ovunque nel mondo, definisce la prospettiva di crisi altamente volatili. La forza che ha prevenuto la guerra nucleare, la deterrenza, non funziona bene con la *cyber war* ».

protezione. Molto spesso, l'offensiva giunge da migliaia di chilometri di distanza ed il *server* che ne scatena il potenziale ha raramente una precisa identità.

Vi sono evidenze consolidate dell'interesse di *al-Qaeda* per il *cyber*-terrorismo. Alcuni computer sequestrati alla rete terroristica hanno fatto trapelare dettagli riguardanti i sistemi di Supervisione e Acquisizione Dati (SCADA) negli Stati Uniti, che controllano l'infrastruttura strategica del Paese, comprese reti elettriche, centrali nucleari, cavi a fibre ottiche, oleodotti e gasdotti, dighe, ferrovie e depositi di acqua. I sistemi SCADA non sono stati creati per essere accessibili da reti esterne, ma molti attualmente sono controllati via internet, cosa che li rende vulnerabili alle intrusioni e agli attacchi informatici. I computer sequestrati ad alcuni appartenenti ad *al-Qaeda* contenevano addirittura gli schemi di una diga negli Stati Uniti, insieme al *software* di ingegneria che abilita gli operatori a simulare un guasto virtuale di dimensioni catastrofiche, con relativa inondazione di aree densamente popolate.

Lo sviluppo relativamente recente delle reti digitali globalmente collegate ha inaugurato anche una nuova stagione di spionaggio. Ogni giorno il Dipartimento della Difesa americano rintraccia circa tre milioni di sonde non autorizzate nei suoi *network*, mentre il Dipartimento di Stato deve fronteggiarne due milioni. Il Dipartimento di polizia di New York registra 70.000 tentativi giornalieri di intrusioni elettroniche. Nel 2007 il Comitato per la Sorveglianza e la Riforma della Pubblica Amministrazione USA ha assegnato al Dipartimento di Stato, a quello della Difesa, a quello del Tesoro e alla Commissione per la Regolamentazione Nucleare un *rating* pari a « F » nella Pagella Federale di sicurezza dei sistemi informatici. Si tratta di uno dei voti più bassi attribuibili. Poche settimane prima, infatti, il sistema informatico della segreteria e del gabinetto del Ministro alla Difesa Robert Gates era stato ripetutamente violato da *hacker* che, secondo le indagini dei servizi di sicurezza, avrebbero avuto supporto logistico e finanziario del governo cinese.

Da quella indagine ebbe altresì inizio una analisi più estesa delle minacce legate al *cyber*-spazio provenienti dall'Estremo Oriente. Il risultato è contenuto in un'articolata pubblicazione promossa dallo *US-China Economic and Security Review Commission* (12), nella quale si individua esplicitamente la crescente competizione tra USA e Cina nella conquista del *cyber*-spazio ed il possibile utilizzo di strumenti informatici per operazioni mirate di sabotaggio o di intromissione nei sistemi americani. La Cina, si afferma, seguirà la strada del *cyber*-spionaggio con particolare determinazione, sia attraverso agenzie governative sia sponsorizzando altre organizzazioni che si stanno impegnando in questo tipo di « pirateria » internazionale. Il Pentagono ritiene che gli *hacker* militari cinesi abbiano compilato piani dettagliati per il sabotaggio delle infrastrutture di comunicazione militare USA; nella primavera del 2009 il *Wall Street Journal* ha riportato la notizia

---

(12) « *Capability of the People's Republic of China to conduct cyber warfare and computer network exploitation* », ottobre 2009.

secondo cui parti del programma militare *Joint Strike Fighter* (JSF), il più costoso programma della storia per la creazione di un nuovo caccia, per un valore complessivo di più di 40 miliardi di dollari, erano state intaccate da *hacker*-spia cinesi.

Nel 2007 l'Amministrazione Bush ha investito 17 miliardi di dollari nella *Comprehensive initiative on cybersecurity*, che ha identificato e segnalato le vulnerabilità esistenti. Poco dopo l'inizio del suo mandato, il presidente Obama ha dichiarato che la sicurezza cibernetica sarebbe stata considerata elemento strategico di sicurezza nazionale, procedendo poi alla nomina di un Coordinatore nazionale delle attività *(cyber-zar)*, che opera alla Casa Bianca in raccordo con il *National Security Council*.

Il Segretario Generale della *International Telecommunications Unit* dell'ONU, Hamadoun Toure, ha invocato l'urgenza di un accordo internazionale per prevenire la possibilità di una guerra informatica tra grandi potenze, i cui effetti sono stati definiti « più devastanti di uno *tsunami* » (13); contemporaneamente, sulla base di uno studio commissionato dal *World Economic Forum* di Ginevra, è emerso come almeno 20 Paesi del mondo abbiano già sviluppato capacità sofisticate per avviare un conflitto su larga scala utilizzando gli strumenti informatici.

Nell'enfatizzare la capillarità della rete informatica mondiale – di cui internet è solo l'espressione più nota –, non possono essere sottovalutate le possibili implicazioni derivanti dall'utilizzo distorto e dalla manipolazione dei contenuti informativi a fini di propaganda politica, discriminazione o denigrazione personale e professionale, creazione di consenso attraverso la distruzione della reputazione dell'avversario. La rete come « arma politica » ed evoluzione dei più tradizionali strumenti di propaganda richiede una particolare attenzione da parte di chi è chiamato a regolare, negli spazi di discussione, confronto e dibattito *online*, messaggi e contenuti che richiedono, innanzitutto, la piena assunzione di responsabilità da parte degli utenti.

* * *

Queste variabili producono, a loro volta, una serie di criticità nell'elaborazione di strategie difensive:

• rendendo indispensabile un approccio sistemico (14). Una politica di difesa cibernetica comprensiva, riguardando tutti i settori della società, presuppone necessariamente uno stretto coordinamento fra i diversi soggetti, dalle agenzie governative competenti alle imprese che gestiscono infrastrutture critiche, fino ai singoli cittadini, in termini di « educazione » alla sicurezza informatica. Uno fra i problemi di un simile coordinamento « pubblico-privato », al di là dei pur significativi aspetti tecnici e logistici, consiste nell'imporre al settore privato la subordinazione degli interessi particolari a quelli

(13) Febbraio 2010, http://rawstory.com/2010/01/agency-calls-global-cyberwarfare-treaty-drivers-license-web-users.

(14) « *Cyberspace and the National Security of the UK* », Chatham House, 3/2009.

generali (15). Ad esempio, in un rapporto del *Congressional Research Service* statunitense, ci si interroga circa l'opportunità di obbligare le compagnie informatiche a dare immediata notizia al *Department of Homeland Security* (DHS) di eventuali vulnerabilità riscontrate nei propri prodotti (16);

• rendendo necessario il superamento, sul piano metodologico, della divaricazione fra ambito militare e civile (17). Il linguaggio utilizzato per descriverne i concetti chiave è spesso derivato dal settore della difesa (« aggressione », « minaccia », « attacco », ecc.), ma le minacce informatiche riguardano in egual misura anche le infrastrutture civili. Inoltre, alcune tipologie di attacchi informatici toccano necessariamente le competenze di organismi civili di sicurezza e di polizia, come avviene, ad esempio, per le truffe elettroniche e il furto d'identità; altre, quali l'intrusione dall'estero in una banca dati governativa classificata, attengono evidentemente agli organi preposti alla difesa del Paese. Questo aspetto ostacola notevolmente un efficace coordinamento internazionale a difesa delle infrastrutture informatiche poiché influenza la definizione stessa di minaccia cibernetica, sempre fortemente modellata dalle specifiche sensibilità di ogni singolo Paese ed attore. Così, ad esempio, la « *Cyber Security Strategy* », recentemente pubblicata dal Governo australiano, pone un forte accento sull'aspetto « micro » della minaccia (truffe informatiche, *privacy*, furti d'identità) (18), mentre dalla documentazione statunitense traspare l'ormai consolidata tendenza di Washington a mettere in primo piano la dimensione strategico – militare e quella terroristica (19);

• generando un dibattito giuridico-istituzionale, in particolare negli USA, sulla suddivisione delle responsabilità della difesa informatica, a livello statale, fra Esecutivo e Legislativo (20). La discussione chiama fortemente in causa la funzione regolatoria dell'organo legiferante, specialmente a causa dei dilemmi che solleva in materia di rispetto della *privacy* delle comunicazioni. Tuttavia, essa risente di un interrogativo più profondo circa l'importanza della dimensione operativa della minaccia cibernetica. L'istituzione di un *Cyber Command* presso il Pentagono, forte di quasi 90.000 uomini e con capacità tecnologiche all'avanguardia (21), è l'eloquente conferma della decisione di considerare il *cyber*-spazio un nuovo fronte militare. Oltre a interrogarsi sulla possibilità di un futuro *cyber*-attacco terroristico catastrofico (22), il dibattito sulla materia negli USA ha toccato anche l'applicabilità di una dottrina di deterrenza all'ambito della *cyber- war* (23). Si tratta, come è evidente, di uno sforzo teorico audace,

---

(15) V. supra.
(16) « *Terrorist capabilities for cyberattack: overview and policy issues* », CRS, 22/1/2009.
(17) V. supra.
(18) « *Cyber Security Strategy* », Governo dell'Australia, 2009.
(19) V. nota 9.
(20) « *Comprehensive National Cybersecurity Initiative: legal authorities and policy considerations* », Congressional Research Service, 10/3/2009.
(21) A dirigere il Comando è il generale Keith Alexander, veterano di numerose operazioni militari e strategiche.
(22) « *Cyberdeterrence and war* », Rand Corporation, 2009.
(23) V. supra.

considerato che il principale beneficio di cui gode l'autore di un attacco informatico è l'alto tasso di anonimato e protezione fisica garantitagli dalla rete. La medesima copertura che, ad oggi, sembra confinare qualunque strategia di difesa a una dimensione esclusivamente di prevenzione e di « *damage control* » eliminando, o quasi, credibili prospettive di misure di ritorsione. In ogni caso, appare evidente che quanto maggiore è la percezione della minaccia come « operativa » e immediata, tanto più operativa deve essere la risposta, che diviene quindi in misura maggiore compito del Governo;

• rendendo ardua la quantificazione della minaccia. La scarsità di elementi circa l'ubicazione fisica dell'attaccante e delle sue risorse rende estremamente complessa la valutazione del danno che egli è potenzialmente in grado di infliggere. L'unico elemento tangibile di valutazione è il danno che l'attaccante è già stato in grado di fare. Questo complica enormemente la definizione generale del rischio e di conseguenza il calcolo e la ripartizione delle risorse da allocare per proteggersi. Gli unici dati certi sull'entità della minaccia cibernetica è che essa è in aumento, a un ritmo tale da farla assurgere al rango di questione urgente e prioritaria nelle agende di sicurezza e difesa delle maggiori Nazioni occidentali. Secondo un sondaggio, citato dal presidente Obama il 5 giugno 2009, « negli ultimi due anni il crimine informatico è costato agli USA più di 8 miliardi di dollari » (24). Inoltre, mentre nel 2006 il CERT (25) del DHS (26) ha riportato 5.503 « incidenti » relativi alla sicurezza dell'infrastruttura informatica del governo, la cifra è salita a 16.843 nel 2008, pari a un aumento del 206% (27). Ancora, la società di sicurezza informatica McAfee ha affermato, nel suo rapporto annuale del 2007, che « circa 120 Paesi stanno sviluppando la capacità di usare Internet come un'arma offensiva da sfruttare sui mercati finanziari, sui sistemi informatici governativi e sulle infrastrutture critiche » (28). Un *trend*, quello descritto, che ha portato il Direttore dell'Unione Internazionale delle Telecomunicazioni (ITU) a dichiarare che « la prossima guerra mondiale potrebbe essere combattuta nel *cyber*-spazio » (29).

* * *

Sulla base dei dati presentati dal già citato *World Economic Forum* di Ginevra, l'Italia risulta al decimo posto tra i Paesi più esposti al mondo in termini di produzione di *software* malevolo, di *spam* ovvero posta elettronica « spazzatura », di siti di *phishing* per frodi finanziarie *online* e di attacchi verso altri Paesi. Ai primi posti ci sono gli Stati Uniti, il Brasile, la Repubblica Popolare di Cina e la

---

(24) V. supra.
(25) CERT: *Computer Emergency Readiness Team*.
(26) DHS: *Department of Homeland Security*.
(27) V. nota 7.
(28) « *Cyber crime*: a 24/7 *global battle* », McAfee, 2007.
(29) « *ITU, Head warns next world war could take place in cyberspace* », AFP, 6 ottobre 2009.

Repubblica Federale di Germania (30). Tale contesto sembra essere confermato dai dati pubblicati dal Ministero dell'interno nel suo *Bilancio del contrasto alla criminalità* del 4 agosto 2009, dove si rileva che in Italia sono state registrate 102.127 truffe e frodi informatiche, un numero in linea con la situazione dell'anno precedente (31). Tuttavia, l'interpretazione di questi dati richiede l'applicazione di due ordini di considerazioni. In primo luogo, come evidenziato nel rapporto citato, bisogna considerare la natura globale di internet e la facilità tecnologica con la quale è possibile confondere la provenienza geografica di un'attività illegale compiuta via internet. Un secondo elemento di attenzione nell'analisi è anche la complessità dei comportamenti di rilevanza penale in ambito *cyber-crime* e la loro registrazione statistica. Per esempio, in Italia, come in altri paesi europei, il furto di identità elettronica via *phishing* non ha una sua specifica norma penale indicata all'interno della legge n. 48 del 2008 per la ratifica della Convenzione sul *Cybercrime*. Esso richiede l'applicazione di diverse norme che vanno dal delitto di abuso di attività di mediazione finanziaria alla falsificazione di comunicazioni informatiche (articolo 671-*sexies* del codice penale) e all'utilizzo indebito di carte di credito (32), di cui all'articolo 12 della legge n. 197 del 5 luglio 1991.

Sulla base di questi due *caveat* interpretativi, identificare i potenziali rischi per la sicurezza nazionale derivanti dal *cyber-crime* richiede una mappatura delle fattispecie tecnologiche alla base delle condotte criminali, quali, per esempio, l'accesso non autorizzato ad un sistema informatico, la detenzione e la diffusione abusive di codici di accesso come *password* oppure il danneggiamento di sistemi informatici di pubblica utilità (33).

Le attività delittuose di *cyber-crime* sono facilitate in generale dalla crescente presenza di vulnerabilità nei sistemi e nelle infrastrutture informatiche da cui vengono erogati servizi di *e-government* e di *e-commerce* oppure sono gestite infrastrutture critiche tra loro interdipendenti. Sulla base del rapporto *Force 2008 Trend and Risk Report* dell'IBM, altro primario fornitore globale di servizi informatici, nel 2008 vi è stata una crescita del 15.3% nel numero di vulnerabilità altamente critiche a livello di sistema operativo e del 67.3% per quelle di media criticità. Inoltre, di tutte le vulnerabilità identificate, solo per il 47% sono state fornite le necessarie soluzioni correttive (dette nel linguaggio tecnico *patches)* da parte del fornitore (34). L'importanza

---

(30) Si veda *Symantec Intelligence Quarterly*, July-September 2009, pubblicato in October 2009 e disponibile su http://www.symantec.com.

(31) Ministero dell'interno, Bilancio del contrasto alla criminalità-Dati sulla Criminalità e Attività in Corso 2008, presentati il 4 agosto 2009; disponibili su http://www.interno.it nella sezione Documenti.

(32) Si veda Roberto Flor, Phishing Misto, Attività abusiva di mediazione finanziaria e profili penali dell'attività di c.d. « *financial manager* », nota a sentenza del Tribunale di Milano, 29 ottobre 2008 in *Rivista di Giurisprudenza ed Economia d'Azienda*, n. 5, 2009.

(33) La terminologia « danneggiamento di sistemi informatici di pubblica utilità » è mutuata dagli articoli 635-*ter* e 635-*quinquies* del codice penale come modificati dalla legge n. 48 del 18 marzo 2008.

(34) IBM Global Technology Services, Internet Security Systems, *X-Force(r) 2008 Trend & Risk Report*, Gennaio 2009 disponibile su http://www.ibm.com.

di questo ultimo dato sta nel fatto che individui o organizzazioni criminali possono utilizzare queste vulnerabilità per compromettere la disponibilità dei sistemi informatici e l'integrità e la riservatezza dei dati ivi contenuti a seguito di una loro estrazione non autorizzata.

I rischi associati alla presenza di vulnerabilità nei sistemi non sono collegati esclusivamente alla mancanza della necessaria *patch*. Esiste spesso un intervallo di tempo tra la scoperta di una vulnerabilità e il rilascio della relativa soluzione tecnologica. Tale spazio temporale può essere sfruttato liberamente dall'attore criminale. Negli ultimi due anni è importante sottolineare notevoli miglioramenti visto che la soluzione correttiva viene individuata per l'87% dei casi nelle ventiquattro ore successive all'identificazione della relativa vulnerabilità. Questo risultato è stato conseguito grazie alla crescente tendenza del produttore di pubblicizzare *online* una vulnerabilità per coinvolgere la comunità di esperti per la soluzione. Tuttavia esiste anche un « mercato nero telematico » per la vendita e per lo scambio di informazioni su tali vulnerabilità oppure, come vedremo in seguito, di metodologie di attacco digitale. Il prezzo può variare da tre USD per quelle meno impegnative (e anche meno efficaci) a importi molto significativi per informazioni su vulnerabilità che possono portare ad un consistente ritorno economico e/o politico se sfruttate (35). Infine, non bisogna sottovalutare il fatto che la disponibilità di una soluzione correttiva ad una vulnerabilità non comporta l'immediata soluzione al problema. Soprattutto nel caso di organizzazioni con infrastrutture tecnologiche complesse, l'installazione di un *patch* può richiedere del tempo, necessario ad eseguire rigidi *test*, al fine di evitare che il suo inserimento possa creare « falle digitali ». Esiste quindi sempre un intervallo temporale che può essere sfruttato. Quello che cambia è il livello di esperienza richiesta all'attore criminale per entrare e per compiere i propri delitti informatici.

Insieme alle vulnerabilità a livello di sistema operativo, sono da segnalare quelle sempre più crescenti per l'ambiente *web* da dove è possibile montare attacchi multipli sfruttando ignari utenti individuali diventati *botnets*. Sebbene il numero delle vulnerabilità in questo specifico contesto sia calato nel 2008, esiste tutta una serie di nuove applicazioni *web* che creano delle nuove « falle digitali » anche in quei sistemi dove sono state applicate tutte le necessarie contromisure. Esempi in questo senso sono l'installazione di nuove soluzioni di comunicazione *Voice over IP* all'interno di *browser* oppure di soluzioni per la visione interattiva di documenti elettronici o di contenuti multimediali.

Le vulnerabilità di cui si è parlato precedentemente sono associate, in particolare, a errori nella programmazione o nell'integrazione di complessi sistemi e soluzioni *software*. Possono anche

---

(35) Vedi nota precedente, Symantec, ottobre 2009. Inoltre, in un *reportage* pubblicato dal quotidiano « Il Sole 24 Ore », il 14 giugno 2010, vengono descritti i passaggi per una semplice acquisizione di un *software*, reperibile via internet ad un costo estremamente modesto, in grado di favorire violazioni di *personal computer* anche da parte di utenti principianti.

essere causate dall'errata implementazione di regole di sicurezza informatica da parte degli utenti. Queste vulnerabilità, tuttavia, sono anche causate da codici malevoli meglio conosciuti con i termini *virus, worm o trojan*. Essendo ognuno di essi un'opera di ingegno, le loro funzionalità variano sulla base degli obiettivi o delle esigenze del suo programmatore, sebbene alla fine vi sia una certa somiglianza funzionale tra tutti loro. Esistono, per esempio, codici malevoli che, una volta installati, disattivano le funzionalità di sicurezza informatica di una postazione di lavoro o di una rete aziendale, facilitando il successivo scarico di altri codici malevoli oppure l'ingresso abusivo. Esistono altri *software* che hanno invece l'obiettivo di facilitare il furto di dati commercialmente sensibili. Sebbene siano adesso sul mercato soluzioni di sicurezza informatica dai prezzi contenuti, esistono su internet programmi simili ma totalmente « modificati » in modo tale da dare un falso senso di sicurezza all'operatore che invece si ritrova uno strumento informatico completamente vulnerabile. Come nel caso delle vulnerabilità, anche per questi *software* esiste « un mercato nero digitale » dove la domanda e l'offerta criminale si incontrano.

La diffusione massiva di vulnerabilità e di codici malevoli è anche facilitata dal crescente fenomeno della posta elettronica spazzatura meglio conosciuta come *spam*. Sulla base di dati offerti dai principali produttori di *software* alla Commissione Europea, circa il 28% dello *spam* mondiale ha origine in Europa, mentre il 20% proviene dal Nord America. Il poco invidiabile primato spetta alla Polonia, seguita da Romania, Russia e Italia. Tuttavia, come precedentemente indicato, l'identificazione della provenienza di tali messaggi non è sempre certa per la facilità con la quale è possibile nascondere la propria residenza geografica su internet.

Di per sé lo *spam* non crea particolari problemi agli utenti se non quello di ricevere messaggi elettronici dai contenuti indesiderati. Il problema è che, come anticipato precedentemente, lo *spam* può essere veicolo per altri rischi.

Collegato al problema dello *spam* esiste quello del furto dell'identità elettronica attraverso attività di *phishing*. Con questo termine si intende principalmente la richiesta via posta elettronica ad un ignaro utente delle credenziali di accesso ai propri conti bancari tramite *link* ad una pagina surrettizia di un istituto bancario presente *online*. Che tale truffa possa avere un buon ritorno economico è dimostrato dal fatto che il 72% dei messaggi di *phishing* hanno una connotazione finanziaria, mentre gli altri presentano offerte per servizi internet, per giochi d'azzardo o per l'acquisto di materiale elettronico. Come altri fenomeni di *cyber-crime*, anche il *phishing* finanziario presenta una spiccata trans-nazionalità, in quanto gli artefici delle truffe sovente appartengono a Paesi diversi da quelli delle vittime. In Italia, come in altri Paesi, è stato registrato un significativo aumento di tali truffe. Secondo la Centrale Rischi Finanziari (CRIF), principale agenzia italiana di *consumer credit information*, nel 2008 è stata registrata una crescita dell'11% e del 16%, rispettivamente, nel numero e nel volume medio delle frodi elettroniche via *phishing* rispetto all'anno precedente.

Tutte queste forme di *cyber-crime* di per sé hanno un impatto indiretto sulla sicurezza nazionale del Paese. Infatti, possono incidere

sulla propensione ad utilizzare internet e i suoi strumenti durante le attività quotidiane e nei rapporti con altre strutture governative o commerciali frenando, di conseguenza, lo sviluppo della società dell'informazione nel Paese. Secondo lo studio *Euroflash barometer* della Commissione Europea sulla percezione che i cittadini hanno della propria *privacy* in Europa, solo il 16% degli italiani ritiene sicura la trasmissione di dati personali via internet. Inoltre, solo il 40% degli utenti italiani di internet conosce gli strumenti a disposizione per proteggersi dai rischi precedentemente descritti. È interessante sottolineare come queste percentuali siano in linea con quanto rilevato negli altri Paesi europei, con l'eccezione dei Paesi scandinavi dove si nota un *trend* molto più positivo (36).

Il *cyber-crime* ha un impatto diretto sulla sicurezza nazionale nel momento in cui vengono compromesse le cosiddette infrastrutture critiche di un Paese. Sulla base del decreto del Ministero dell'interno del 9 gennaio 2008, sono da considerarsi infrastrutture informatizzate critiche di interesse nazionale quei sistemi e quei servizi informatici di supporto dei ministeri, di agenzie e di enti operanti in settori strategici anche nei rapporti internazionali quali, ad esempio, giustizia, difesa, finanza, ambiente, Banca d'Italia, oppure società partecipate dallo Stato che forniscono servizi essenziali in comuni con oltre 500.000 abitanti. La sospensione totale o parziale delle funzionalità di queste strutture a valle di attacchi informatici coordinati può avere effetti diretti sulla capacità del Paese di operare in linea con le sue esigenze socio-politiche ed economiche. Sebbene un'analisi dettagliata della letteratura *open source* disponibile non abbia permesso l'identificazione di tali attività nei confronti dell'Italia, è possibile comprendere le conseguenze di un simile scenario dall'attacco che ha visto coinvolta l'Estonia nella primavera del 2007 (37).

A seguito di una diatriba interna circa la rimozione di un simbolo sovietico nel Paese, l'Estonia ha subito quella che è stata classificata come « *Web War I* », parafrasando l'acronimo anglosassone per Prima Guerra Mondiale (*World War I*), ovvero una serie di attacchi diretti a rendere non operativi alcuni elementi delle infrastrutture critiche. In parallelo, tra i principali attivisti informatici russi sono circolati inviti ad attaccare infrastrutture critiche estoni attraverso il « bombardamento » digitale oppure l'uso di codici malevoli. Per prima cosa, fu sospeso il servizio di posta elettronica del parlamento nazionale, mentre i *provider* di servizi internet e telecomunicazione si trovarono a sospendere l'erogazione di loro servizi per un breve periodo. La situazione peggiorò nel tempo, quando un cosiddetto « attacco coordinato » attraverso l'utilizzo di *botnets* fu lanciato contro gli istituti finanziari, costretti a sospendere tutte le proprie attività per un certo

---

(36) Commissione Europea « *Euroflash barometer: data protection in the European Union-Citizens' perceptions survey conducted by the Gallup Organization Hungary upon the request of Directorate-General Justice, Freedom and Security* », Febbraio 2008, disponibile su http://ec.europa.eu/public_opinion/flash/fl_225_en.pdf (visitato, 12 dicembre 2009).

(37) Per una descrizione di dettaglio: Swedish Emergency Medical Association (SEMA), *Large scale internet attacks: the internet attacks on Estonia-Sweden's emergency preparedness for internet attacks*, SEMA Educational Series n. 2, 2008.

intervallo di tempo. L'esempio più eclatante rimane quello della Georgia, oggetto, nell'agosto 2008, di un attacco informatico su larga scala nel corso della guerra dell'Ossezia meridionale. Poche settimane prima della deflagrazione del conflitto, i principali *server* georgiani vennero messi fuori uso da una serie di interruzioni mirate (in gergo DoS – *Denial of Service*). Contemporaneamente all'avvio delle operazioni militari, qualsiasi tentativo di connessione a siti *internet* georgiani veniva reindirizzato in automatico verso siti in lingua russa, caratterizzati da una propaganda politica estremamente aggressiva. Sebbene le specifiche conseguenze socio-economiche siano state alla fine limitate, i casi estone e georgiano dimostrano la potenziale facilità con cui si può montare un attacco digitale contro le infrastrutture informatiche di un Paese. È difficile dimostrare, tuttavia, che tali comportamenti siano da equipararsi ad un attacco « armato » che giustifichi un'eventuale azione di auto-difesa (38).

In primis, è necessario dimostrare in modo inequivocabile che tale attacco sia originato in un Paese sovrano e che sia stato ordinato da strutture governative e non da gruppi di *hacker* che si sono coordinati *online*. Tutto ciò richiede « prove » informatiche inconfutabili, una condizione questa molto improbabile da soddisfare visto che eventuali tracce digitali sono probabilmente sparse su *server* in giro per il mondo e probabilmente non producibili in alcun contesto giuridico. Su quest'ultimo punto è interessante il caso dell'attacco contro *Google*. Infatti, dal punto di vista strettamente tecnologico, sembra che questa azione sia stata implementata sfruttando una vulnerabilità presente in un programma per documenti PDF che, una volta attivato, ha creato una « falla » da sfruttare successivamente per accedere ai sistemi di *Google*. La letteratura *open source,* inoltre, evidenzia come questo attacco abbia richiesto l'utilizzo di numeri IP utilizzati in precedenza per simili attività contro società private e commerciali presenti in Cina (39).

Nei precedenti paragrafi è stata fornita una panoramica delle principali minacce e dei rischi derivanti dalla crescente dipendenza del tessuto socio-economico e finanziario da infrastrutture e tecnologie informatiche. Sono state anche introdotte delle considerazioni circa la complessità di classificare un attacco informatico contro infrastrutture critiche come un'azione offensiva. Nel prosieguo del documento si presenterà una panoramica dell'approccio alla gestione di questi rischi *online,* analizzando il caso comunitario e quelli degli Stati Uniti e del Regno Unito. Il primo è di particolare interesse, laddove lo stesso presidente della Commissione Barroso ha indicato

---

(38) Lo studio degli aspetti di diritto internazionale e cosiddetta « *information warfare* » non è molto sviluppato. Un esempio è Goodman, S., « *Cyber-attacks and international law* » Survival, Volume 42, Number 3, 2000, pp. 89-104.

(39) In ogni caso, uno degli aspetti più interessanti di questo caso è la richiesta di assistenza da parte di *Google* alla *National Security Agency*, l'organizzazione governativa USA di *signal intelligence*, ancorché non siano stati resi pubblici i dettagli di questa eventuale collaborazione. Per maggiore informazione si veda Marc Rotemberg, *Executive Director, Electronic Privacy Information Centre* (EPIC), Audizione presso la Commissione affari esteri del Congresso, 10 febbraio 2010, disponibile su http://www.epic.org.

la sicurezza informatica e la lotta contro il crimine informatico come obiettivi strategici del suo nuovo mandato (40).

4. La prevenzione della minaccia: panorama internazionale.

***a)* L'Unione Europea.**

Le istituzioni comunitarie hanno cominciato ad affrontare il problema del *cyber-crime* e della protezione delle infrastrutture critiche nei primi anni '90, quando era diventato evidente che internet e le sue applicazioni avrebbero avuto un impatto diretto sul tessuto socio-economico e finanziario dell'Europa. Tenendo conto dei limiti imposti dai tre Pilastri del Trattato di Maastricht, la Commissione affrontava questa problematica come un possibile impedimento allo sviluppo di una cultura della fiducia *(trust)* verso internet e, di conseguenza, al suo utilizzo per servizi di *e-commerce* e *e-government* (41). Sulla base dei risultati di attività di ricerca dell'allora Direzione Generale per la Società dell'Informazione e Media, la Commissione invitava alla ricerca di un approccio coordinato europeo. Primo risultato di questa riflessione è stato un regolamento del 2005 in cui si confermava l'urgenza di coordinare a livello europeo iniziative relative alla sicurezza informatica. A questo è seguita nel 2006 una comunicazione della Commissione che delineava una *roadmap* strategica incentrata sui seguenti elementi:

a) lo scambio di informazioni sui rischi e vulnerabilità *online* via *Computer Emergency Response Teams* (CERTs);

b) la sensibilizzazione dell'utente sui rischi *online*;

c) la definizione di parametri per l'identificazione di infrastrutture critiche;

d) le attività di ricerca in nuove aree quali la simulazione degli effetti economici di attacchi informatici (42).

Sempre in questo periodo è da segnalare nel 2004 la nascita dell'ENISA, *European Network and Information Security Agency*, come il centro di eccellenza strategico e operativo dell'Unione Europea in ambito di sicurezza informatica (43). Dopo un inizio complesso, ENISA ha trovato una sua collocazione operativa, il suo mandato è stato esteso per altri quattro anni nel 2008 e si pensa già ad una sua estensione definitiva.

Nel 2008 il Consiglio e il Parlamento europei hanno invitato la Commissione e gli Stati membri a valutare l'ENISA e le altre attività europee per la promozione di cultura della sicurezza informatica e

---

(40) Si veda Commissione Europea, *Political guidelines for the next Commission*, p. 30, disponibile su http://ec.europa.eu/commission_barroso/president/pdf/press_20090903_EN.pdf (visitato il 12 dicembre 2009).

(41) Per una breve analisi della materia, si veda Lorenzo Valeri, « Sicurezza Informatica » Rivista di *Intelligence*, n. 2, novembre 2009, pp. 84-94.

(42) Commissione Europea « *A strategy for a secure information society – "Dialogue, partnership and empowerment"* » disponibile su http://eur-lex.europa.eu/LexUriServ/site/en/com/2006/com2006_0251en01.pdf (visitato il 12 dicembre 2009).

(43) Per maggiori dettagli sull'ENISA e la sua struttura legale e operativa si veda il sito dell'organizzazione a http://www.enisa.eu.int.

per la protezione delle infrastrutture critiche (44). Questa riflessione ha avuto come primo risultato la comunicazione della Commissione del 30 marzo 2009, la quale indica iniziative per consolidare la preparazione, la sicurezza e la resilienza delle infrastrutture informatiche europee (45). Prima di analizzare in dettaglio tali iniziative, è importante indicare che, in parallelo, la Commissione ha lavorato per impostare anche un programma per la protezione delle infrastrutture critiche (EPCIP) (46), comprese quelle di natura informatica.

Nel giugno 2004, infatti, il Consiglio ha richiesto alla Commissione, in particolare alla Direzione Giustizia, Libertà e Sicurezza, la predisposizione di una strategia per la protezione delle infrastrutture critiche. Nell'ottobre dello stesso anno, tale comunicazione fu adottata dalla Commissione facendo partire delle iniziative operative.

In primis, fu definito il programma europeo per la protezione delle infrastrutture critiche con l'obiettivo di identificare soluzioni organizzative, tecnologiche e operative. Il secondo risultato è stata una direttiva nel 2008 per l'individuazione e per la designazione di infrastrutture critiche europee e per la creazione di un « *Critical Warning and Information Network* », al fine di facilitare lo scambio di informazioni su eventuali rischi o minacce (47). La stessa direttiva ha classificato come « infrastrutture critiche » quelle di natura informatica. Quest'ultima direttiva integra le misure già presenti per la cooperazione nella lotta al *cyber-crime* indicate nella decisione quadro del 2005 relativa ad attacchi contro sistemi informatici, il cui aggiornamento è previsto nei prossimi mesi, a seguito dell'entrata in vigore del Trattato di Lisbona.

La problematica della sicurezza delle infrastrutture critiche informatiche potrebbe, inoltre, ricevere un indiretto impulso dal recente parere favorevole del Parlamento europeo alle direttive per la riforma del quadro regolamentare per i servizi di telecomunicazione.

Nella prima direttiva sull'accesso, sull'interconnessione e sull'autorizzazione per le reti e per i servizi di comunicazione elettronica (48), si afferma espressamente che il trasporto sicuro delle informazioni attraverso le reti di comunicazione elettronica è elemento centrale per il tessuto socio-economico europeo. Si invitano, quindi, le autorità regolamentari nazionali ed ENISA a contribuire alla

---

(44) Si veda al riguardo il risultato della fase consultiva pubblica disponibile presso http:// ec.euro pa.eu/information_society/policy/nis/nis_public_consultation/index_en.htm (visitato il 12 dicembre 2009).

(45) European Commission Communication « *Critical Information Infrastructure Protection – Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience* » disponibile su http://eur-lex.europa.eu /Notice.do?checktexts=checkbox&val=493232:cs&pos=1&page=1&lang=en&pgs=10& nbl=1&list=493232:cs&hwords=&acti- on=GO&visu= (visitato il 12 dicembre 2009).

(46) Il sito del programma è disponibile su http://ec.europa.eu/justice_home/funding/ 2004_2007/epcip/funding_epcip–en.htm (visitato il 12 dicembre 2009).

(47) Commissione Europea *Protection des infrastructures critiques dans le cadre de la lutte contre le terrorisme* * COM/2004/0702 final */ disponibile su http://eur -lex.europa.eu/LexUriServ.do ?uri=CELEX:52004DC0702:FR:NOT (visitato il 12 dicembre 2009).

(48) Direttiva 2002/20/CE del Parlamento europeo e del Consiglio, del 7 marzo 2002, relativa alle autorizzazioni per le reti e i servizi di comunicazione elettronica.

crescita del livello di sicurezza attraverso lo scambio di *best practices*. Le stesse organizzazioni sono invitate ad indicare ai fornitori di servizi di comunicazione elettronica misure per la tutela della riservatezza e dell'integrità dei dati e della loro disponibilità. La direttiva conferisce alla Commissione la possibilità di adottare misure tecniche per conseguire un adeguato livello di sicurezza delle reti e dei servizi di comunicazione elettronica. Le autorità regolamentari nazionali hanno la facoltà di svolgere indagini in caso di attestata mancata conformità e, ove necessario, di imporre sanzioni.

Sempre in questo contesto di revisione del quadro regolamentare relativo alle telecomunicazioni e ai servizi elettronici, è importante considerare il potenziale impatto della direttiva sul servizio universale, i diritti degli utenti e il corretto trattamento dei dati personali. Oltre a richiedere agli operatori l'applicazione delle misure minime di sicurezza per la protezione di dati personali, la direttiva indica la necessità per gli operatori di fornire dettagli circa potenziali incidenti di sicurezza che hanno coinvolto singoli abbonati. Quest'ultimo aspetto non fa che confermare come l'implementazione delle normative nazionali ed internazionali in ambito di protezione dei dati personali sia un passo essenziale per la creazione di una cultura della sicurezza informatica e, di conseguenza, per la protezione delle infrastrutture critiche.

Sulla base dell'*excursus* dei precedenti paragrafi, allo stato attuale è possibile anticipare future iniziative comunitarie in questo settore. Tenendo conto dell'entrata in vigore del Trattato di Lisbona, l'intervento normativo riguarderà, in particolare, la creazione di un approccio integrato che porti valore aggiunto ai vari programmi nazionali oppure alle attività bilaterali già in corso. Come stabilito nella sua comunicazione del 31 marzo 2009, la Commissione vuole in primo luogo rafforzare le capacità operative dei CERTs di reazione a incidenti e a potenziali minacce informatiche. Si vogliono anche predisporre le basi per lo sviluppo e per l'implementazione di un sistema europeo di scambio di informazioni e di potenziali allarmi a vantaggio degli utenti individuali e delle piccole e medie imprese. La Commissione vuole anche facilitare uno scambio di idee sulle priorità tecniche relative alla sicurezza di internet a livello europeo e globale, nonché la promozione di accordi tra strutture governative e mondo privato per favorire il dialogo e lo scambio di informazioni e *best practices*.

L'aspetto più interessante è la proposta che gli Stati membri facciano almeno un'esercitazione nazionale per testare l'efficienza di piani di emergenza per la gestione di attacchi informatici o di disastri naturali o accidentali contro infrastrutture informatiche. La Commissione contribuirà inoltre alla realizzazione di esercitazioni paneuropee come base per una loro successiva estensione anche su scala globale. Anche nel 2010 ENISA continuerà le sue attività di valutazione del livello europeo di « *prepardness* » (49) e di facilitazione del

(49) In termini tecnici, il livello di preparazione di una risposta adeguata alla possibile minaccia e di eventuale ripristino a seguito di un attacco catastrofico.

dialogo tra mondo pubblico e privato per la gestione dei disastri con impatti sul sistema delle telecomunicazioni, come indicato dalla Comunicazione della Commissione « *Reinforcing the Union's disaster response capacity* » del 2008 (50).

A tutte queste attività sono da aggiungersi le iniziative del Programma di Stoccolma dell'Unione licenziato dal Consiglio europeo nel dicembre 2009 volto a promuovere la sicurezza, la giustizia e le libertà dei cittadini europei. Per quanto concerne il *cyber-crime*, il Consiglio invita tutti gli Stati membri a ratificare la convenzione del 2001 del Consiglio d'Europa, al fine di potenziare la cooperazione transfrontaliera per compiere le necessarie indagini e per raccogliere prove eventualmente ammissibili in sede processuale. Europol viene inoltre indicato come il punto di riferimento per la creazione di una piattaforma europea per l'identificazione delle fattispecie penali, oltre che per il potenziamento delle attività di analisi strategica delle molteplici espressioni di questo fenomeno (51).

b) Gli Stati Uniti d'America.

A poche settimane dalla sua elezione, il presidente Barack Obama ha richiesto al suo intero *staff* e agli organismi competenti una rapida ricognizione dello *status quo* in materia di sicurezza informatica (52). Il documento finale, firmato dalla Casa Bianca e redatto dal *team* di Sicurezza Nazionale del Presidente, ha ribadito l'importanza della protezione delle infrastrutture informatiche critiche per la sicurezza del Paese. Molti dei provvedimenti già assunti dalle precedenti Amministrazioni venivano, in quella stessa occasione, ripresi ed ampliati. Già nel maggio 1998 era stata creata all'interno dell'*Executive Office* del Presidente una struttura di coordinamento per prevenire e per gestire eventuali attacchi contro le infrastrutture critiche informatiche del Paese. Nel 2003 questo approccio è stato aggiornato con la pubblicazione della *The national strategy to secure cyberspace* e della Direttiva n. 7 del 2007 che assegnava al *Department of Homeland Security* il coordinamento delle attività volte a proteggere le infrastrutture critiche del Paese, incluse quelle di natura informatica, in cooperazione con i singoli dipartimenti di riferimento all'interno dell'*Executive Office*. Si parlava, in particolare, di facilitare lo scambio di informazioni tra pubblico e privato attraverso gli *Information Security and Advisory Centres*, di potenziare i *Computer Emergency Response Teams* (CERTs) e di sviluppare nuove soluzioni tecnologiche e gestionali attraverso iniziative di ricerca e sviluppo. Sempre nel 2007, fu lanciata la *Comprehensive National Cybersecurity Initiative* (CNCI) come ponte operativo tra gli aspetti « civili » della

---

(50) Per maggiori informazioni su queste attività si veda il programma annuale per il 2010 dell'ENISA, disponibile al http://www.enisa.eu.int.

(51) Il testo del Programma di Stoccolma è disponibile su http://ec.europa.eu/justice_home/news/intro/doc/stockholm_program−en.pdf.

(52) Si veda *White House*, *Cyberspace Policy Review* disponibile presso http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review−final.pdf (visitato il 12 dicembre 2009).

protezione delle infrastrutture informatiche critiche e quelli relativi al *cyber-crime*, con un'attenzione precipua alle reti governative.

La revisione da parte del Presidente USA di questo impianto operativo ha indirettamente confermato la sua validità iniziale evidenziandone, tuttavia, delle chiare limitazioni. Innanzitutto, si chiedeva la nomina di un coordinatore di tutte queste attività per mantenere una certa coerenza operativa e per identificare eventuali interventi correttivi e migliorativi. Veniva anche prevista la nomina di un coordinatore degli aspetti di protezione dei dati personali, una richiesta questa in netto stacco rispetto alla precedente amministrazione.

Tra gli aspetti più interessanti delle proposte al nuovo Presidente, sono da segnalare un più forte coinvolgimento internazionale, la proposta di organizzare altre simulazioni di incidenti dopo quelle di *Cyberstorm* I e II (53) e l'incremento degli investimenti in ricerca e sviluppo. Infine, si confermava la centralità dello scambio di informazioni tra pubblico e privato per l'*early warning* di possibili attacchi. Come detto precedentemente, le nuove proposte non sono di per sé nuove. L'innovazione più autentica risiede piuttosto nell'approccio multilaterale, incentrato sulla forte collaborazione con altri Paesi e all'interno dei principali fori internazionali come, per esempio, l'OCSE oppure le Nazioni Unite, nella sede dell'*Internet Governance Forum*.

La continuità con le precedenti amministrazioni è confermata dalla recente nomina di Howard Schmidt a *Cybersecurity Coordinator*. Schmidt non è nuovo a tali ruoli istituzionali, visto che aveva già rivestito l'incarico di consigliere per gli aspetti di sicurezza informatica e di protezione delle infrastrutture critiche durante l'amministrazione Bush. La differenza, tuttavia, risiede nella sua collocazione gerarchica, all'interno del *National Security Council*, la struttura di supporto al Presidente USA per gli aspetti di sicurezza nazionale. Da tale collocazione, il nuovo responsabile può coordinare tutte le attività federali che assegnano al *Department of Homeland Security* un ruolo determinante con riferimento alle attività di analisi, di raccolta e di catalogazione delle vulnerabilità e di scambio di informazioni tra pubblico e privato. Per gli aspetti di lotta contro il *cyber-crime*, invece, il *Federal Bureau of Investigation* (FBI) continua a mantenere la sua *leadership* operativa sia a livello nazionale che internazionale.

Oltre che a questi aspetti prettamente civili, è da segnalare anche il forte coinvolgimento delle organizzazioni militari, come confermato dalla recente *Quadriennal Defence Review*, il documento strategico di politica di difesa degli Stati Uniti dove si invita il Dipartimento della Difesa ad adoperarsi per la protezione dei suoi *network* informatici, al fine di preservare le capacità di comando, controllo e di *intelligence* di

---

(53) Si tratta di due esercitazioni condotte tra il 2006 ed il 2008, coordinate dal *Department of Homeland Security* e che hanno coinvolto l'intera comunità di attori federali e governativi coinvolti nella politica di protezione delle infrastrutture critiche e informatiche nazionali. Sono stati simulati gli effetti di un attacco informatico su larga scala, alla rete idrica e a quella elettrica, nonché l'effetto di penetrazione da parte di *hacker* sui sistemi di sicurezza delle principali agenzie federali.

tutto l'apparato militare statunitense (54). Di recente (55), su impulso della revisione della strategia di sicurezza nazionale promossa dalla Casa Bianca, queste strutture, assieme ai comandi operativi in materia di sicurezza cibernetica e guerra elettronica delle quattro Forze Armate USA (Aeronautica, Esercito, Marina e Marines), sono confluite in un unico *Cyber Command*, all'interno del Dipartimento della Difesa, forte di 90.000 operativi sotto la guida di un Generale di Corpo d'Armata (il primo Direttore è il generale Keith Alexander, Direttore della *National Security Agency* – NSA). Qui confluiranno anche, a partire dall'ottobre 2010, la *Joint Task Force for Global Network Operations* e la *Joint Functional Component Command for Network Warfare*, mentre il supporto tecnico e scientifico arriverà dalla *Defence Information System Agency*.

Dall'analisi dell'approccio statunitense è evidente l'accentramento funzionale e gerarchico delle attività per la protezione delle infrastrutture critiche e della lotta contro il *cyber-crime* nell'ambito dell'*Executive Office* del Presidente per quanto concerne gli aspetti civili e all'interno del US *Cyber Command* per gli aspetti militari. Alcuni commentatori hanno interpretato queste iniziative come una militarizzazione del *cyber*-spazio. Questo giudizio non sembra, tuttavia, appropriato, in quanto contrasta con la natura globale e prevalentemente civile delle infrastrutture e con i nuovi compiti di monitoraggio, raccolta e scambio di informazioni in ambito di protezione dei dati personali. È anche da segnalare l'accresciuto interesse del governo e del legislatore statunitense a muoversi verso una cornice normativa federale, volta alla protezione dei dati personali nel rispetto delle esigenze di *law enforcement*, nonché di quelle della comunità *intelligence* e della difesa. Questo interessamento non ha ancora dato segnali tangibili, se non con dichiarazioni di massima da parte del presidente Obama e di altri esponenti della sua squadra di governo.

c) Il Regno Unito.

Spostando l'analisi sul Regno Unito, la politica per la sicurezza informatica e per la protezione delle infrastrutture critiche è in evoluzione, anche se tendente verso un coordinamento più accentrato. Attualmente, questo *dossier* vede il coinvolgimento di differenti istituzioni per i propri ambiti di competenza. Il *Computer and Electronics Security Group* (CESG), che fa parte del GCHQ *(Government Communications Headquarter* (56)*)*, coordina l'implementazione della strategia nazionale per la sicurezza informatica e gestisce il CERT governativo (57). Per quanto concerne i rapporti con il mondo privato e, in particolare, con i fornitori di servizi di comunicazione,

---

(54) Si veda US Department of Defence, *Quadriennal Defence Review-Final Report,* Febbraio 2010 disponibile su http://www.defense.gov.

(55) Maggio 2010.

(56) Si tratta dell'Agenzia governativa che si occupa di sicurezza delle comunicazioni.

(57) Per maggiori informazioni sul CESG e GCHQ si veda http://www.cesg.gov.uk e www.gchq.gov.uk.

la gestione è affidata al *Centre for Protection of National Infrastructure* (CPNI). Questa struttura lavora in stretto contatto con tutti i ministeri di riferimento, con il mondo privato e con il *National Counter Terrorism Security Office*, una struttura creata con il supporto dell'AICPO, l'associazione nazionale dei capi delle singole forze di polizia a livello regionale. Per quanto concerne gli aspetti di *cyber-crime*, le attività sono svolte dall'*Home Office* e dalla *Serious Organised Crime Agency* (SOCA) per le proprie aree di competenza.

Vista la complessità della materia, anche nel Regno Unito si sta definendo una struttura centrale di coordinamento. A valle della pubblicazione della *Cybersecurity Strategy of the United Kingdom* (58), nel giugno 2009 è stato creato all'interno dello *staff* del Primo Ministro l'*Office of Cybersecurity* per coordinare tutte le iniziative. Per gli aspetti più operativi invece è stato predisposto un *Cybersecurity Operations Office* che, dalla sua base all'interno di GCHQ, controlla la situazione e fornisce informazioni e dettagli di eventuali attacchi o minacce alle infrastrutture critiche del Paese.

Con il cambio nella guida del governo del Regno Unito, questo modello organizzativo è stato posto sotto esame; dai primi atti dell'amministrazione Cameron-Clegg non emergono mutamenti sostanziali.

d) **Francia.**

Nel 2008 il governo di Parigi ha varato la prima strategia di sicurezza nazionale, il « *Livre Blanc sur la Défense et la Sécurité Nationale* », nella quale la sicurezza del *cyber*-spazio viene esplicitamente indicata come una priorità di sicurezza nazionale.

L'approccio francese alla sicurezza cibernetica si caratterizza per la particolare attenzione riservata alle minacce provenienti (direttamente o indirettamente) da attori statuali e per il ricorso alla cosiddetta « difesa attiva ».

L'implementazione di tale linea strategica ha richiesto un adeguamento delle strutture governative. Nel luglio 2009 il governo ha realizzato quanto previsto dal documento di sicurezza nazionale, istituendo l'*Agence Nationale de la Sécurité des Systèmes d'Information* (Agenzia Nazionale per la Sicurezza dei Sistemi Informativi – ANSSI), evoluzione della *Direction centrale de la sécurité des systèmes d'information*.

Alle dipendenze del Primo Ministro, l'Agenzia è pienamente integrata all'interno del vertice decisionale politico-strategico e costituisce, per esplicita menzione di legge, l'autorità nazionale in materia di sicurezza dei sistemi informativi.

L'ANSSI è stata pensata come una struttura complessa e completa, attraverso la quale la « funzione *cybersecurity* » viene razionalizzata, centralizzata e collegata stabilmente all'organo responsabile della pianificazione strategica integrata in materia di sicurezza nazionale, il *Secrétaire Général de la Défense et de la Sécurité Nationale*

---

(58) Cabinet Office, *Cybersecurity Strategy of the United Kingdom*, giugno 2009 disponibile su http://www.cabinetoffice.gov.uk/media/216620/css0906.pdf (visitato il 12 dicembre 2009).

(SGDSN). A conferma ulteriore della rilevanza attribuita a questo aspetto della sicurezza, la legge istitutiva dell'Agenzia ha disposto la creazione, presso l'SGDSN, di un comitato strategico con compiti di orientamento e verifica, cui partecipano anche i vertici dei servizi di *intelligence*.

***e)* La cooperazione in ambito NATO.**

Chiamata a ridefinire il proprio concetto strategico, grazie al lavoro svolto da un gruppo internazionale di esperti cui ha preso parte anche l'Italia, l'Alleanza Atlantica concentrerà in maniera crescente i propri sforzi di analisi e prevenzione del rischio legato alla sicurezza informatica e all'utilizzo delle reti telematiche come strumento offensivo per la sicurezza dello spazio euro-atlantico. Tra le priorità che la NATO dovrà affrontare, emerge la messa in sicurezza dei sistemi di Comando e Controllo dell'Alleanza, autentica spina dorsale delle comunicazioni tra vertici militari e operativi dei singoli Stati membri. Un attacco cibernetico ai sistemi che controllano l'attività operativa metterebbe in ginocchio la NATO e la sua capacità di garantire la sicurezza collettiva.

Quale foro privilegiato di cooperazione, l'Alleanza dovrà fornire altresì supporto tecnico alla protezione delle infrastrutture critiche delle singole Nazioni, equiparate spesso al rango di infrastrutture strategiche per la piena operatività dell'Alleanza. Infine, essa dovrà attrezzarsi con adeguate misure difensive e di dissuasione rispetto alle minacce esterne. Verranno rafforzate le prerogative del Centro di eccellenza per la difesa informatica, creato a Tallinn, in Estonia, proprio a seguito degli attacchi subiti dal Paese nel 2007.

È in corso di realizzazione un'Autorità per la difesa del settore informatico dell'Alleanza, oltre ad una rete di reazione immediata a potenziali attacchi cibernetici.

Appare senz'altro interessante, in questa prospettiva, il dibattito relativo alla possibile estensione delle implicazioni dei contenuti degli articoli 4 e 5 del Trattato istitutivo della NATO: essi disciplinano i meccanismi di consultazione e il principio della « difesa collettiva » in caso di attacco a uno dei Paesi membri. Fino ad oggi, tali strumenti sono stati invocati e adottati in caso di attacco militare tradizionale (salvo l'attacco terroristico alle Torri Gemelle).

In tal senso, il gruppo di lavoro chiamato a ridefinire il concetto strategico della NATO, coordinato dall'*ex* Segretario di Stato USA Madeleine Albright, ha formulato cinque raccomandazioni al Segretario Generale in tema di protezione delle infrastrutture informatiche:

a) il rafforzamento della sorveglianza delle reti e, quindi, la possibilità di individuare tempestivamente le debolezze e le criticità;

b) il rafforzamento del centro di formazione di eccellenza con sede a Tallinn;

c) il rafforzamento delle capacità nazionali di allerta precoce (*early warning*) in caso di attacco informatico o intrusione in sistemi di sicurezza nazionale;

d) la creazione di un gruppo di esperti da inviare a sostegno del Paese eventualmente oggetto di attacco;

e) la dotazione di strumenti e di strutture adatte a scongiurare un attacco asimmetrico all'Alleanza e ai suoi *network*.

* * *

Dalle esperienze in ambito multilaterale e in quelle degli Stati Uniti, della Francia e del Regno Unito si possono evincere degli esempi di *best practices* sulle politiche pubbliche di contrasto alle minacce per la sicurezza nazionale derivanti dalle diverse forme di *cyber-crime*. Seppure nel rispetto delle rispettive competenze definite dal loro ordinamento costituzionale, queste esperienze evidenziano la necessità di creare un coordinamento centrale delle attività, con l'obiettivo di raccordo delle iniziative di prevenzione e di gestione nei casi di attività di *cyber-crime* con impatti diretti sulla sicurezza nazionale di un Paese. Estremamente importante è che questo coordinamento centrale non vada a sostituirsi alle iniziative e attività operative già in corso. Per esempio, negli Stati Uniti la lotta operativa per le attività di rilevanza penale in ambito *cyber-crime* continua ad essere affidata al FBI. La stessa cosa può essere detta per le attività del *Serious Organised Criminal Agency* nel Regno Unito.

Il secondo aspetto che si evince da questa analisi comparativa è la necessità di creare una forte sinergia tra mondo pubblico e privato al fine di favorire lo scambio di informazioni e *best practices* per la prevenzione e per la gestione dei rischi. Negli Stati Uniti, questa *partnership* si esprime prevalentemente negli *Information Sharing and Analysis Centres* settoriali, attraverso cui organizzazioni private e mondo pubblico si scambiano informazioni su eventuali minacce o attacchi contro i propri sistemi informativi in via anonima. Un simile approccio è anche stato implementato dal Regno Unito nell'ambito del CNPI, mentre la Commissione Europea e la *European Network and Information Security Agency* ne hanno parlato molto apertamente all'interno della direttiva sulle infrastrutture critiche del marzo 2009 e dei loro programmi operativi e di ricerca.

Il terzo elemento comune è la convinzione che tutte queste iniziative non possano dare il risultato sperato senza iniziative di sensibilizzazione di tutti gli attori, compresi gli utenti individuali, circa i rischi di operare su internet e sugli altri strumenti *online* a disposizione senza le necessarie difese tecnologiche e organizzative.

Alcuni punti cardine, di carattere molto generale, sembrano trasversalmente condivisi. Fra questi:

– l'assurgere della sfida cibernetica allo *status* di minaccia strategica;

– il dovere per il Governo di guidare il contrasto alla minaccia informatica;

– la necessità di un coordinamento « *top-down* » fra Stato e settore privato;

– la necessità di una maggiore « *cyber*-consapevolezza » presso i singoli cittadini;

– la natura eminentemente difensiva e preventiva di una strategia di « *cybersecurity* ».

A fronte di ciò, i dubbi e i nodi irrisolti rimangono significativi. Nonostante i notevoli sforzi compiuti, lo stato del dibattito sembra infatti tradire un ritardo nel processo di adattamento dei sistemi-Paese a una minaccia nuova, in costante evoluzione, e al contempo già reale. Nei citati documenti governativi sono talvolta visibili chiari sintomi di un eccessivo « generalismo », come se, a livello di scelte politiche, non fosse ancora conclusa la fase della descrizione del problema. Ad esempio, la *Cybersecurity Policy Review* statunitense soffre in molti punti di un tono che la rende non molto più di una dichiarazione di intenti, un tentativo di tracciare linee guida concettuali che attendono di essere riempite da provvedimenti operativi o dalla loro esecuzione. Inoltre, la distribuzione delle competenze in materia di minaccia cibernetica appare tuttora uno dei dilemmi dottrinali più spinosi e suscettibili di assestamento nel medio periodo.

Questi ostacoli divengono ancora più evidenti nell'esaminare i tentativi in atto di elaborare strategie di sicurezza cibernetica internazionali. La proposta formulata nello studio della Direzione per gli Affari Esterni e la Politica di Vicinato dell'UE appare troppo generica rispetto alle reali esigenze. Nella pubblicazione si prevede che, benché l'UE sia « attivamente impegnata nella sicurezza cibernetica, non si può affermare che possieda un approccio organico al problema » (59). Per poi proporre una politica di « *Comprehensiveness in diversity* », fondata in sostanza su un evanescente concetto di coordinamento, molto simile ad una candida ammissione delle enormi difficoltà nella creazione di una strategia di sicurezza comunitaria.

5. L'attività di contrasto alla minaccia in Italia.

La lotta al crimine informatico in Italia è stata condotta con una strategia articolata secondo cinque direttrici:

- un adeguamento normativo alle condotte criminose emergenti;
- il potenziamento del ruolo dell'*intelligence* in termini di contrasto e prevenzione della minaccia e la predisposizione di reti tecnologiche di comunicazione sicure per le forze armate, le forze di polizia e gli apparati di sicurezza;
- l'affidamento ad una branca altamente specializzata della Polizia di Stato, il Servizio di Polizia postale e delle comunicazioni, dei principali compiti di contrasto operativo;
- la sottoscrizione di accordi di *partnership* pubblico-privato, in base al modello di « sicurezza partecipata », adottato dal Dipartimento di Pubblica Sicurezza, tra le istituzioni preposte alla sicurezza e le potenziali vittime del crimine;

---

(59) « *Cyber security and politically, socially and religiously motivated cyber attacks* », Directorate General External Policies of the Union, 2/2009.

• lo sviluppo della collaborazione internazionale di Polizia, in ragione della natura transnazionale e della delocalizzazione dei *computer crimes*;

• la promozione di campagne di informazione, finalizzate a segnalare i rischi relativi a un uso improprio o imprudente delle nuove tecnologie e per diffondere cultura della legalità.

L'adeguamento normativo è stato consequenziale all'evoluzione e alla sofisticazione del crimine informatico. L'Italia, a partire dal 1993, con la legge n. 547 recante « Modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica », si è dotata di un quadro normativo più efficace ed aggiornato.

Il legislatore è altresì intervenuto due volte in materia di pedofilia *online*. Con la legge 3 agosto 1998 n. 269, recante « Norme contro lo sfruttamento della prostituzione, della pornografia, del turismo sessuale in danno dei minori, quali nuove forme di schiavitù », ha introdotto nel codice penale le fattispecie volte a sancire le condotte criminali circa lo sfruttamento sessuale dei minori attraverso la pornografia in rete, affidando ad un'unica branca della Polizia di Stato particolari e incisivi strumenti investigativi (attività sotto copertura e acquisti simulati).

Tale legge è stata poi modificata dalla legge 6 febbraio 2006, n. 38, recante « Disposizioni in materia di lotta contro lo sfruttamento sessuale dei bambini e la pedopornografia anche a mezzo internet », per renderla più rispondente alle esigenze di contrasto di alcuni aspetti della pedopornografia *online* particolarmente subdoli e che si erano rivelati impermeabili all'azione di polizia.

Con la direttiva del Ministro per le innovazioni e tecnologie del 16 gennaio 2002 (« Sicurezza informatica e delle telecomunicazioni nelle pubbliche amministrazioni ») è stato stabilito per la prima volta che le informazioni gestite dai sistemi pubblici diventano una risorsa di valore strategico per il governo del Paese e la sua sicurezza.

In materia di tutela del *copyright* vi è stata una serie di interventi legislativi, da ultimo con la legge 21 maggio 2004, n. 128: « Conversione in legge con modificazioni del decreto-legge 22 marzo 2004, n.72, recante interventi per contrastare la diffusione telematica abusiva di materiale audiovisivo, nonché a sostegno delle attività cinematografiche e dello spettacolo », che ha profondamente modificato la precedente normativa, rivelatasi inadeguata a fronteggiare la violazione del diritto d'autore in rete.

Con l'entrata in vigore del codice della *privacy* (decreto legislativo 30 giugno 2003, n. 196) è stato disciplinato in modo particolarmente efficace il diritto alla riservatezza dei dati personali delle persone, messo fortemente in pericolo dalle nuove tecnologie e dal proliferare di banche dati (e anche di apparati di sorveglianza elettronica; si pensi, ad esempio, al recente esperimento di adozione dei *body scanner* negli aeroporti).

Le norme in vigore, in generale, impongono ai titolari di qualsiasi banca dati l'adozione di stringenti misure di sicurezza, sia fisiche sia

logiche, soprattutto quando contengono informazioni sensibili pertinenti alla persona. A ciò si aggiungono i provvedimenti emanati in questi anni dal Garante per la *privacy*, che costituiscono il più importante baluardo posto a difesa della riservatezza dell'utente e dei dati che transitano sulla rete. Accanto alle tutele per i cittadini e gli utenti, l'estensione del perimetro della disciplina da parte dell'Autorità garante alle aziende, enti ed istituzioni e qualsiasi altro soggetto della vita pubblica e privata rappresenta uno strumento essenziale per favorire la ricerca del delicato equilibrio tra due beni essenziali quali sono la *privacy* e la sicurezza.

All'indomani degli attentati terroristici di Madrid e Londra, nell'agosto 2005, il Parlamento approvò la legge 31 luglio 2005, n. 155, avente ad oggetto « Conversione in legge, con modificazioni, del decreto-legge 27 luglio 2005, n. 144, recante misure urgenti per il contrasto del terrorismo internazionale », destinata a rendere più incisiva e coordinata l'attività degli organi antiterrorismo delle forze di polizia e dei servizi di *intelligence*. In tale provvedimento, all'articolo 7-*bis* (sicurezza telematica), per la prima volta si fornisce una base normativa finalizzata a preservare da eventuali attacchi cibernetici le cosiddette « infrastrutture critiche nazionali ». In particolare, sono individuate come infrastrutture critiche quelle risorse, quei processi, la cui distruzione, interruzione o anche parziale indisponibilità, ha l'effetto di indebolire in maniera rilevante l'efficienza e il funzionamento dei servizi vitali di una nazione, ed in particolare:

- la produzione e distribuzione di energia (elettrica, del gas, dei carburanti);
- le comunicazioni (postali, telefoniche, telematiche);
- i trasporti (stradale, ferroviario, aereo, navale);
- la gestione delle risorse idriche;
- la produzione e distribuzione di derrate alimentari;
- la sanità (ospedali, reti di servizi e interconnessione);
- le banche e i sistemi finanziari;
- la sicurezza e protezione civile (forze dell'ordine, forze armate);
- le reti a supporto delle istituzioni e degli organi costituzionali;
- servizi particolari forniti da alcuni enti e aziende strategiche.

Un'altra tappa importante di questo percorso di adeguamento normativo è stata la ratifica della Convenzione del Consiglio d'Europa sul *Cybercrime*, sottoscritta a Budapest il 23 novembre 2001, e ratificata dall'Italia con la legge 18 marzo 2008, n. 48.

Negli anni successivi alla sottoscrizione, hanno aderito anche Paesi non appartenenti al Consiglio d'Europa, tra i quali gli USA, per un totale, ad oggi, di ventinove Stati.

La legge di ratifica ha modificato, allineandole con quelle degli altri Paesi che hanno aderito alla Convenzione, le norme esistenti

nell'ordinamento italiano sia sostanziali sia di rito, attinenti il *cyber-crime*. Sul piano della collaborazione giudiziaria, per velocizzare lo scambio di dati investigativi durante le indagini sui crimini informatici, la Convenzione prevede tra l'altro, su richiesta dello Stato che procede all'indagine, il « congelamento », per un periodo di tre mesi, dei dati informatici eventualmente in possesso di altri Stati. Le richieste in questione dovranno transitare attraverso il *network* dei rispettivi « punti di contatto » nazionali. A questo fine, con decreto interministeriale dei Ministri dell'interno e della giustizia, in data 24 novembre 2009, il Servizio Polizia postale e delle comunicazioni è stato designato punto di contatto nazionale all'interno della rete di cooperazione dei Paesi che hanno ratificato la Convenzione sul *Cybercrime* del Consiglio d'Europa.

Il quadro di riferimento per il *cyber-crime* si sta arricchendo di norme che sanzionano comportamenti illeciti alla soglia della punibilità penale o nella fase del tentativo di reato – è il caso del *grooming* – o addirittura alla fase preparatoria di un ipotetico crimine più grave, come nello *stalking*.

5.1. La protezione delle infrastrutture critiche in Italia.

L'organo primario nella lotta contro il *cyber-crime* è la Polizia postale, sebbene la natura complessa del fenomeno possa creare delle sovrapposizioni operative nei casi in cui sia richiesto il coinvolgimento di altre strutture. Alla Polizia postale è stata demandata la sicurezza delle infrastrutture informatiche, incluse quelle identificate come critiche, oltre che la prevenzione e il contrasto degli attacchi di livello informatico, la regolarità dei servizi di telecomunicazione e il contrasto della pedopornografia *online*. La Polizia postale è anche attiva nella lotta agli illeciti concernenti i mezzi di pagamento attraverso le attività di commercio elettronico e il diritto d'autore svolti via internet o altri strumenti informatici in raccordo con la Guardia di Finanza (prevalentemente con il suo Nucleo Speciale Frodi Telematiche), cui competono le attività per la tutela dei marchi, dei brevetti e della proprietà intellettuale, nonché per la tutela dei mezzi di pagamento.

Sin dalla sua costituzione, questo reparto specializzato della Polizia di Stato si è distinto a livello nazionale e internazionale per le capacità tecnologiche ed operative. A livello nazionale, la sua presenza capillare sul territorio, attraverso i 19 comparti regionali e con quasi 2000 addetti, permette una diretta interazione con una moltitudine di attori locali per la soluzione di situazioni critiche e per lo svolgimento di mirate attività di sensibilizzazione. A livello internazionale, questo reparto è demandato ad essere il punto di raccordo e di contatto per richieste che arrivano da altri paesi e partecipa alle attività di studio e scambio di *best practices* nei consessi specifici quali il *Rome/Lyon Group* del G8, Europol, Interpol, oltre che a contesti quali l'ufficioso *Meridian Conference (v. infra)*.

Nel panorama della lotta al *cyber-crime* e della protezione delle infrastrutture critiche, è da segnalare nel giugno 2009 l'attivazione del Centro nazionale anticrimine informatico per la protezione delle

infrastrutture critiche (CNAIPIC), che era stato previsto dal decreto del Capo della Polizia del 7 agosto 2008. Questa struttura, che era stata indicata già all'interno della direttiva europea sulla protezione delle infrastrutture critiche del 2008, raccoglie al suo interno personale altamente specializzato con funzioni operative e tecniche della Polizia postale e si raccorda con gli operatori di infrastrutture critiche di natura informatizzata identificati nel decreto del Ministero dell'interno del 9 gennaio 2008. Al fine di facilitare il dialogo con gli operatori privati, la Polizia di Stato ha sottoscritto una serie di convenzioni triennali di cooperazione e di scambi di informazioni attraverso collegamenti dedicati con Consob, RAI, ACI, Ferrovie dello Stato, Vodafone, Telecom e Unicredit.

Di recente è stata istituita una segreteria tecnica dipendente funzionalmente dal consigliere militare del Presidente del Consiglio per favorire il coordinamento interministeriale delle attività nazionali, anche in consessi internazionali, sulle problematiche relative alle infrastrutture critiche comprese quelle di natura informatica. Questa segreteria tecnica è stata distaccata presso il Nucleo di Difesa Civile/NRBC del Dipartimento della Protezione Civile.

Il Paese si è dunque dotato nel corso degli anni di strumenti operativi per la lotta al *cyber-crime* e, su impulso di iniziative internazionali e comunitarie, sta definendo un approccio coordinato alla problematica della protezione delle infrastrutture critiche, comprese quelle di natura informatica. In un contesto in cui le infrastrutture informatiche sono sempre più interdipendenti, oltre alla gestione e repressione nei casi di attacchi informatici, è tuttavia necessario che gli attori che da esse dipendono siano dotati anche di idonei strumenti per la prevenzione. Benché in maniera che è stata giudicata ancora troppo prudente, l'Italia inizia a implementare strategie e strumenti operativi, prevedendo:

- il « Commissariato *online* »: è il portale dedicato a tutti gli utenti per denunciare, segnalare reati o comportamenti anomali, rilevati durante la navigazione, ovvero per chiedere informazioni;

- il « Centro Nazionale per il Contrasto alla Pedopornografia *online* » – CNCPO: è stato istituito con la citata legge n. 38 del 2006 e inaugurato il 1º febbraio 2008. Il Centro è destinato a coordinare le complesse attività di contrasto a questo crescente fenomeno criminale, in collaborazione con gli ISP (*Internet Service Provider)* e con le Onlus che si occupano del problema sotto l'aspetto sociale. Il Centro ha inoltre il compito di coordinare le attività investigative degli uffici periferici della Polizia postale. Si occupa della collaborazione operativa internazionale con gli uffici di Polizia di altri Paesi che hanno funzioni analoghe. I *network underground* di pedofili in rete hanno ormai dimensioni che travalicano i confini nazionali e le indagini sempre più spesso coinvolgono contemporaneamente più Paesi;

- il « Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche » (CNAIPIC), istituito in attuazione dell'articolo 7-*bis* della legge 155 del 2005 e inau-

gurato il 23 giugno 2009. Si tratta in sostanza di una sala operativa, disponibile 24 ore al giorno, 7 giorni su 7. È un servizio dedicato alle infrastrutture critiche informatizzate, che sono collegate telematicamente al Centro per la reciproca e immediata trasmissione di informazioni e dati utili alla prevenzione e alla repressione di eventuali minacce criminali o terroristiche condotte in modo informatico, all'integrità delle stesse. Il CNAIPIC agisce solo in presenza di reato o di tentativo di reato e quindi sotto il controllo e d'intesa con l'Autorità giudiziaria competente;

- il « Nucleo Speciale Frodi Telematiche » della Guardia di Finanza: istituito nel 2001, è specializzato nel contrasto alle frodi informatiche.

La collaborazione tra pubblico e privato nel campo della sicurezza cibernetica è parte integrante della strategia nazionale. Con la società Poste Italiane è stata, ad esempio, sottoscritta dal Capo della Polizia nel 2002 una Convenzione volta a stabilire servizi mirati della Polizia postale in cambio di servizi da parte della società.

L'attività di *computer forensic* (60) è uno dei principali strumenti investigativi nel contrasto del *cyber-crime* e attualmente costituisce un impegno rilevante per la Polizia delle comunicazioni. In questi anni, sono stati siglati « Protocolli d'Intesa » con le maggiori università italiane per la formazione del personale di polizia addetto al settore, ma anche per trasmettere agli studenti dei *master* universitari in materia di sicurezza informatica esperienze qualificate della sezione specializzata della Polizia di Stato.

Da ultimo, per fronteggiare in maniera più incisiva la minaccia ai servizi finanziari in rete, è stata costituita, nel giugno 2009, una struttura composta dal Servizio Polizia postale e delle comunicazioni, *Secret Service* – la nota agenzia di *law enforcement* statunitense – e Poste Italiane. Il gruppo denominato « *European Electronic Crime Task Force* » ha l'obiettivo di porsi come centro di eccellenza europeo per il contrasto al *cyber-crime*, e sarà aperto all'adesione anche di altri soggetti pubblici e privati con interessi comuni.

Tra i gestori di reti critiche nazionali, Poste Italiane ha, tra l'altro, avviato una collaborazione con l'università statale di Milano per implementare il sistema denominato « *Phishing Forensic Analyzer* », uno strumento di supporto alla clientela e alle vittime di *phishing* tramite posta elettronica. Poste Italiane ha altresì avviato la costituzione di un « Centro di Eccellenza Nazionale » sulla *cybersecurity* (CENSec), con gli obiettivi di fungere da acceleratore della conoscenza e cultura nazionale sulle problematiche relative alla sicurezza informatica; identificare e diffondere le soluzioni di contrasto alla minaccia; contribuire allo sviluppo di nuove soluzioni organizzative, procedurali, tecnologiche e di regolamentazione.

Nel 2003 è stato elaborato un progetto di collaborazione per la prevenzione e il contrasto agli accessi illeciti e ai tentativi di accesso ai sistemi di gestione della sicurezza della circolazione ferroviaria

---

(60) L'insieme delle tecniche investigative sviluppate attraverso la rete o che abbiano ad oggetto i crimini commessi attraverso la rete.

utilizzati dalla RFI Spa, che ha portato, in data 15 luglio 2003, alla stipula di una « *Convenzione per la prevenzione dei crimini informatici sui sistemi di gestione della sicurezza della circolazione ferroviaria utilizzati dalla Rete Ferroviaria Italiana Spa* ». La Convenzione ha recepito la direttiva del Ministro dell'interno che prevedeva, tra gli obiettivi operativi della politica dell'ordine e della sicurezza pubblica, il contrasto alla criminalità informatica, nonché l'implementazione della messa in sicurezza delle infrastrutture critiche. A seguito della costituzione del CNAIPIC, la Convenzione consente la condivisione e l'analisi di informazioni utili alla prevenzione della minaccia; la segnalazione di emergenze relative a vulnerabilità, minacce e incidenti; l'identificazione dell'origine tecnica degli attacchi contro l'infrastruttura ferroviaria e le altre infrastrutture critiche; la realizzazione e la gestione di attività di comunicazione per fronteggiare situazioni di crisi o di emergenza. È in corso di realizzazione, da parte delle Ferrovie dello Stato, l'adeguamento dei sistemi di automazione del controllo del traffico e del segnalamento ferroviario.

Per affrontare le emergenze di criminalità informatica – tipicamente a carattere transnazionale – la Polizia postale e delle comunicazioni è entrata a far parte di diverse reti di cooperazione internazionale, per meglio integrare gli ordinari canali di cooperazione giudiziaria e investigativa. Partecipando al sottogruppo *High Tech Crime* del G8, i rappresentanti della Polizia delle comunicazioni, già nel 1999, hanno dato vita alla rete dei punti di contatto che, ad oggi, conta sulla partecipazione di uffici specializzati nel contrasto ai crimini informatici di 56 Paesi.

La Polizia italiana, nel 2003 e nel 2006, ha organizzato conferenze internazionali di addestramento tecnico-operativo dei funzionari addetti dei Paesi aderenti. La rete costituisce un mezzo per trasmettere fra gli specialisti le richieste di « congelamento » dei dati informatici che, indispensabili nelle investigazioni internazionali, potrebbero andare dispersi per vari motivi. Questa rete di agenzie di *law enforcement*, nata in ambito G8, è più ampia di quella costituita dai punti di contatto dei Paesi che hanno ratificato la Convenzione di Budapest sul *Cybercrime*, cui si è fatto cenno.

Con specifico riferimento al tema della protezione delle infrastrutture critiche nazionali, il Servizio Polizia postale e delle comunicazioni partecipa anche alla *International Watch and Warning Network* (IWWN), finalizzata alla tempestiva circolazione delle notizie di minacce e vulnerabilità, che potrebbero andare ad incidere sulle funzionalità dei sistemi informatici che presiedono l'erogazione di servizi pubblici essenziali di un determinato Paese.

Sempre sullo stesso tema, il servizio di Polizia partecipa con propri rappresentanti alla *Meridian Conference*, un gruppo di lavoro internazionale permanente, nato in ambito G8, composto da esperti di 32 Paesi che si occupano a vario titolo di protezione delle infrastrutture critiche.

La Polizia postale e delle comunicazioni ha contribuito alla costituzione, nel novembre 2008, di un *pool* di uffici investigativi internazionali specializzati nella lotta allo sfruttamento dei minori a

fini sessuali *online*, dando vita alla *Virtual Global Taskforce*, di cui fanno parte anche i governi di Australia, Canada, Regno Unito e USA, oltre al Segretario Generale dell'Interpol.

La sicurezza informatica rientra altresì all'interno del piano di *e-government* 2012. Tra le varie iniziative, è da segnalare l'obiettivo 24 (« Sicurezza dei sistemi informativi e delle reti »), che prevede la stabilizzazione e il potenziamento dell'Unità di prevenzione degli incidenti informatici in ambito servizio pubblico di connettività (SPC) istituita presso il CNIPA in ottemperanza all'articolo 21, comma 51.a del Decreto del Presidente del Consiglio dei Ministri del 1º aprile 2008, denominata *Computer Emergency Response Team* (CERT) SPC. In questo contesto particolare attenzione viene data alla necessità di consolidare l'integrazione tra la componente centrale (CERT-SPC) e le strutture delle PA distribuite a livello locale (le Unità Locali Sicurezza – ULS), cui è attribuito il compito di dare attuazione alle azioni di prevenzione e gestione degli incidenti che si dovessero verificare sui sistemi interni al rispettivo dominio, anche a seguito delle indicazioni e del supporto fornito dal CERT-SPC. Infatti, le regole tecniche per il funzionamento e per la sicurezza del sistema pubblico di connettività (SPC) prevedono che ogni amministrazione centrale aderente all'SPC si doti di una Unità Locale di Sicurezza, cui è affidata sia la responsabilità di porre in atto tutte le fasi di prevenzione degli incidenti di sicurezza informatica, sia la gestione operativa degli eventuali incidenti informatici.

Il consolidamento del CERT-SPC conferisce al governo centrale la capacità di:

- disporre di una rete informativa, focalizzata principalmente sulla raccolta di dati e informazioni necessari al coordinamento nel proprio contesto di riferimento;
- utilizzare strumenti evoluti per il monitoraggio delle vulnerabilità e l'osservazione dei comportamenti ostili registrati in Rete;
- predisporre un sistema articolato di comunicazione mediante avvisi e segnalazioni delle emergenze, da destinare al personale e alle strutture impegnate nella gestione operativa dei sistemi informatici governativi;
- impiegare procedure standardizzate di reazione e coordinamento in occasione del verificarsi di incidenti informatici;
- interagire con una pluralità di interlocutori esterni al proprio dominio ma omologhi per funzioni, tali da consentire un'idonea attività di verifica e correlazione delle indicazioni e dei dati ottenuti;
- migliorare i meccanismi e le misure di protezione sulla base dell'analisi degli incidenti avvenuti.

In linea con quanto indicato dalla Banca Centrale Europea, nel 2007 la Banca d'Italia ha emanato le disposizioni per la continuità operativa degli operatori finanziari, definiti « processi a rilevanza sistemica », anche in caso di attacco informatico. I nuovi requisiti sono

stati applicati con gradualità con l'obiettivo di raggiungere la completa conformità entro 5 anni.

I processi ad alta criticità nel sistema finanziario italiano, se intaccati o manipolati, possono provocare blocchi nei sistemi di pagamento e nelle procedure per l'accesso ai mercati finanziari, sino a colpire l'operatività dell'intera piazza finanziaria nazionale. Si tratta di un complesso strutturato di attività finalizzate all'erogazione dei servizi connessi con i sistemi di regolamento interbancario, compensazione, garanzia e liquidazione degli strumenti finanziari, servizi per l'accesso ai mercati, fino alla erogazione di denaro agli utenti.

Le disposizioni della Banca d'Italia richiedono che le banche o gli istituti finanziari nominino un responsabile per la gestione dei piani di continuità operativa e definiscano gli scenari di rischio rilevanti per la continuità operativa dei processi a rilevanza sistemica, inclusi quelli di attacco informatico, che devono essere documentati e costantemente aggiornati. Le stesse disposizioni richiedono che gli istituti finanziari si dotino di siti di *recovery* per la gestione di questi processi di rilevanza sistemica, situati a congrua distanza dai siti primari in modo da assicurare un elevato grado di indipendenza tra i due insediamenti. Sono stati anche previsti dei tempi di ripristino in caso di incidente contenuti nelle quattro ore, in modo da ridurre al minimo la perdita di informazioni. Si richiede infine che gli istituti finanziari coinvolti svolgano delle verifiche con frequenza almeno annuale e che partecipino attivamente ai test di sistema promossi dalle autorità, dai mercati e dalle principali infrastrutture finanziarie.

È da segnalare l'attività dell'ABI LAB, una struttura all'interno dell'Associazione Bancaria Italiana, attiva per la definizione e lo sviluppo di *best practices* in ambito di sicurezza informatica e continuità operativa.

Il canale dell'*internet banking* in Italia è ad oggi abilitato per un numero di clienti che supera i 13 milioni e che si proietta in crescita costante. Particolarmente allarmante è risultato, negli ultimi anni, il fenomeno del furto d'identità, sotto forma di due strumenti: il *phishing* e il *crimeware* (61).

La Centrale d'Allarme ABI LAB effettua una rilevazione annuale del fenomeno delle frodi informatiche nel settore bancario. Nei primi mesi del 2010 sono state raccolte le evidenze relative alla diffusione del fenomeno nell'anno 2009, aggregando un campione di 162 istituti di credito, rappresentativi del 75% del sistema bancario italiano, del 78% in termini di dipendenti e dell'81,6% dei clienti *online* abilitati.

L'89% delle banche del campione ha dichiarato di aver riscontrato tentativi fraudolenti mirati al furto delle credenziali di autenticazione all'*home banking*. A fronte di una sostanziale riduzione dell'incidenza

---

(61) Il *phishing* consiste nella creazione e nell'uso di messaggi *e-mail* o SMS che invitano a consultare siti *web* realizzati da truffatori per carpire informazioni personali e riservate. Con il termine *crimeware* si fa invece riferimento a una specifica classe di codici malevoli (*malware*), che si diffondono attraverso internet e che sono in grado di installarsi automaticamente sul PC del cliente, rendendo disponibili informazioni personali e codici di accesso a aree riservate.

percentuale delle frodi informatiche perpetrate tramite *phishing* (le falle nel sistema hanno concesso lo 0,6% di casi di smarrimento di identità informatica), si assiste per contro ad un aumento degli attacchi di *crimeware*. Nel corso del 2009, infatti, il 37,9% degli attacchi subiti dalle banche del campione sono riferibili al fenomeno del *phishing*, mentre nel 47,5% dei casi essi sono riconducibili a *crimeware*; nel 14,6% dei casi non è stato possibile determinare la causa primaria di perdita delle credenziali da parte dei clienti.

Nella consapevolezza che quello bancario sia tra i *network* più sensibili rispetto alle possibili infiltrazioni delle reti criminali informatiche, vanno richiamate alcune sedi di cooperazione internazionale. L'ABI partecipa ai seguenti *forum* di coordinamento:

- *IT Fraud Working Group* (Federazione Bancaria Europea): gruppo di lavoro della Federazione bancaria europea per lo scambio di informazioni sul fenomeno delle frodi informatiche e il confronto sulle iniziative di prevenzione e contrasto avviate dalle associazioni bancarie nazionali nei propri domini di riferimento;
- FI-ISAC: gruppo di lavoro promosso dall'Agenzia europea ENISA per la costituzione di un centro dedicato alle istituzioni finanziarie. Vi partecipano rappresentanti delle istituzioni bancarie di riferimento di 19 Paesi, i rappresentanti dei CERT nazionali e i rappresentanti delle Forze dell'ordine;
- CISEG (*Cybercrime Information Sharing Expert Group)*: *task force* in *staff* al Gruppo di Supporto sulla Sicurezza Informatica (ISSG) attivato dallo *European Payment Council*, che ha l'obiettivo di favorire lo scambio di informazioni rilevanti per il fenomeno del crimine informatico.

Esistono inoltre numerosi gruppi tecnici di lavoro nelle sedi internazionali preposte alla vigilanza del sistema bancario e finanziario.

Dal 2004 la Banca d'Italia ha emanato la Normativa di Vigilanza « Continuità operativa in casi di emergenza », che impone alle 800 banche italiane di dotarsi di un Piano di Continuità Operativa (*Business Continuity Plan)*. Nel 2007, la stessa Banca d'Italia ha emanato una Normativa di Vigilanza (« Requisiti particolari per la continuità operativa dei processi a rilevanza sistemica »), volta ad accrescere gli obblighi a carico degli operatori che gestiscono processi a rilevanza strategica nel sistema finanziario italiano, con particolare riferimento al sistema dei pagamenti e alle procedure per l'accesso ai mercati finanziari. Il tavolo CODISE (Continuità Di Servizio), che riunisce gli operatori e le tre banche a rilevanza sistemica ed è coordinato dalla Banca d'Italia d'intesa con la CONSOB, rappresenta il principale punto di incontro istituzionale per la definizione di iniziative per la protezione delle infrastrutture di rete di interesse nazionale.

Un'altra organizzazione di riferimento è l'Associazione Italiana Esperti Infrastrutture Critiche, un *forum* che coinvolge esperti

multidisciplinari in tematiche connesse con la protezione delle infrastrutture critiche. Un ruolo primario viene svolto dal CLUSIT, il club italiano per la sicurezza informatica che riunisce oltre 100 organizzazioni private, statali e fornitrici di servizi di *IT security*.

Particolarmente significativa è l'attività svolta dall'Autorità Garante per la protezione dei dati personali. Essa è chiamata a vigilare e verificare presso privati, enti pubblici o imprese, l'attuazione delle misure tecnico-organizzative prescritte dal Codice per la protezione dei dati personali e ad impartire prescrizioni aggiuntive nel caso lo ritenesse necessario, attraverso l'emanazione di specifici provvedimenti. Il Codice, oltre ad indicare (Titolo II) le regole generali per il trattamento dei dati e a stabilire (Titolo IV) specifiche responsabilità per i soggetti titolari, responsabili e incaricati del trattamento, disciplina (Titolo V) gli obblighi di sicurezza (62).

L'attività svolta dal Garante presso le infrastrutture critiche si concretizza negli accertamenti ispettivi svolti in applicazione degli articoli 157 e 158 del Codice; nell'emanazione di provvedimenti per adeguare o migliorare le misure di sicurezza e protezione dei dati e dei sistemi fisici o logici che li custodiscono o li trattano; nell'emanazione di provvedimenti di carattere generale applicabili ai sistemi informativi delle infrastrutture critiche.

Le tutele sancite dal Garante vanno oltre l'attività di messa in sicurezza delle infrastrutture critiche, attraverso un'adeguata protezione dei dati personali e la disciplina delle necessarie regole di riservatezza. Di fronte a minacce che evolvono rapidamente e a sistemi che progrediscono con crescente sofisticazione, l'obiettivo dell'Autorità è quello di anticipare le possibili implicazioni dell'innovazione a servizio della sicurezza della collettività, anche rispetto a dinamiche di largo interesse e coinvolgimento. È il caso, ad esempio, delle reti di comunicazione internet cosiddette *wi-fi*; la moltiplicazione dei punti « *hot spots* », ovvero delle porte di accesso alla rete virtuale, divenute ormai di utilizzo corrente e gratuito per una larga fetta di popolazione. Tutto ciò implica la necessità del ricorso a strumenti di protezione e di crittografia che sono l'unica barriera contro il pericolo di sottrazione illecita di dati personali o aziendali, così come del registro di navigazione.

All'estremo opposto, l'attività di implementazione di provvedimenti a carattere generale si orienta anche verso la frontiera dell'innovazione. Vale la pena citare il caso del trattamento dei dati genetici e biometrici, che in maniera crescente saranno la cifra dell'identificazione personale a largo spettro. Con l'approvazione da parte del Parlamento italiano della legge 30 giugno 2009, n. 85 (adesione dell'Italia al Trattato di Prum e istituzione della banca dati

---

(62) In particolare all'articolo 31: « i dati personali oggetto di trattamento sono custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alla finalità della raccolta ».

nazionale del DNA), il nostro Paese si avvia a creare, presso il Ministero dell'interno, una banca dati biometrici e, presso il Ministero della giustizia, un Laboratorio centrale per la gestione dei campioni biologici. Due strutture che a pieno titolo dovranno rientrare nel sistema nazionale delle infrastrutture critiche e di sicurezza della Repubblica e la cui organizzazione dovrà rispettare i parametri di classificazione e di conservazione di dati personali completi, utili però allo svolgimento di indagini giudiziarie delicate o alla garanzia dell'inconfutabile riconoscimento di diritti.

Rispetto all'opinione pubblica e ai cittadini, con particolare riguardo alle classi di età più vulnerabili, va sottolineato che un'adeguata politica di sensibilizzazione al rischio contribuisce a scongiurare numerosi pericoli. La Polizia di Stato ha da qualche tempo avviato, insieme con altri soggetti pubblici e privati, campagne d'informazione sui rischi nell'utilizzo di nuovi mezzi di comunicazione. In rete, infatti, si può essere vittime di frodi e raggiri, anche se, con la stessa facilità, si può diventare inconsapevolmente autori degli stessi atti illegali: è proprio la rete a fornire, spesso attraverso *forum* di discussione tematici – impiantati dagli utenti stessi e talvolta improntati ad un errato senso di impunità – tutte le informazioni tecniche necessarie per eventuali azioni illegali. La disinvoltura con cui molti utenti si calano nella rete, fornendo informazioni sulla propria vita privata, sulla propria identità e su quella dei propri familiari, apre delle falle negli apparati di sicurezza nelle quali si insinuano pervasivi *network* criminali o semplici criminali solitari, per gli scopi delittuosi più diversi.

Le sfide, in ogni caso, sono in costante evoluzione. I problemi di sicurezza della rete diventeranno ancora più impellenti nei prossimi anni, con l'avvento del *cloud computing*. Si tratta di un'architettura di sistemi informatici in forte espansione, sulla quale stanno investendo molte grandi aziende. Con il *cloud computing*, i *software* applicativi non saranno più residenti nei computer degli utenti, ma saranno posti su *server* remoti; gli utenti, in tal modo, potranno collegarsi ai *server* remoti per lavorare i propri dati in qualsiasi luogo e con qualunque computer, anche di basse prestazioni. Non avranno bisogno nemmeno del *backup* dei dati, che sarà a carico del *server* remoto. Ma i dati risulteranno, per questo, non più fisicamente nella disponibilità dell'utente. Se si perde il collegamento a internet, essi non saranno più accessibili. La tutela della riservatezza dei dati degli utenti sarà compito del gestore del *server* che li ospita, con il rischio che se per qualsiasi ragione le difese del *server* fossero violate, i dati, le credenziali digitali degli utenti potrebbero essere sottratti.

5.2. L'attività dei servizi di *intelligence* italiani.

Pur nella consapevolezza che non esistono un'architettura e un modello ottimali di prevenzione della minaccia, l'Italia ha, sulla base anche delle esperienze internazionali, rafforzato di recente il ruolo e l'attività dei suoi servizi di informazione e sicurezza, quali attori

centrali di qualsiasi politica volta a scongiurare le minacce informatiche e telematiche. Ciò vale per:

– la Divisione INFOSEC dell'AISE, responsabile dell'individuazione e neutralizzazione degli attacchi alle risorse informative dell'Agenzia e del Paese, attuati attraverso strumenti informatici. L'AISE partecipa a numerosi consessi NATO e internazionali, in modo da mantenere costantemente aggiornate le proprie capacità nel settore della difesa cibernetica e da assicurare lo scambio tempestivo di informazioni in materia di *cyber-intelligence*, al fine di ridurre la vulnerabilità e incrementare la capacità di discriminare la tipologia e la provenienza degli aggressori;

– la Sezione controingerenza telematica dell'AISI. Nel quadro del nuovo ordinamento previsto dalla legge n. 124 del 2007, l'Agenzia ha di recente istituito, all'interno del Reparto di Controingerenza, una Sezione Controingerenza Telematica, con un'attività basata sulla stretta cooperazione tra l'Agenzia interna ed i soggetti pubblici e privati di valenza strategica nazionale, e con i comparti di specialità delle Forze di Polizia. La minaccia è stata seguita dall'Agenzia attraverso la partecipazione della sua componente tecnica in consessi multilaterali nell'ambito dei quali vengono affrontate le problematiche degli attacchi elettronici. L'Agenzia ha curato, in seno al MEDINT, l'organizzazione di seminari sulle tecniche di *hacking* e ha provveduto all'addestramento tecnico del personale operativo;

– il DIS, attraverso l'Ufficio Centrale per la Segretezza (UCSe), con competenze sulla sicurezza delle comunicazioni classificate (COMSEC) e sull'attività per la sicurezza materiale delle infrastrutture che gestiscono informazioni classificate. L'UCSe, in particolare, cura gli adempimenti istruttori per l'esercizio delle funzioni del Presidente del Consiglio quale Autorità nazionale per la Sicurezza responsabile della protezione delle informazioni classificate. Esso, inoltre, prende parte ai lavori del Gruppo di Esperti Governativi (GGE) costituito in ambito ONU per lo studio delle conseguenze di attacchi informatici e la valutazione di possibili contromisure per la protezione dei sistemi informativi critici.

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 e 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 controingerenza 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 e 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.

---

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

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 cibernetici 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

---

(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.

ricerca di un ordine mondiale il più possibile improntato alla stabilità e alla cooperazione.

Un Trattato di disciplina dell'attività cibernetica di origine statuale 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 ».

Allegato 1

LE PRINCIPALI CATEGORIE DA FONTI DI ATTACCO CIBERNETICO SECONDO IL COMPUTER EMERGENCY READINESS TEAM DEL DHS *(Department of Homeland Security USA)*

Minaccia	***Descrizione***
Bot-network operator	I *Bot-network operators* (Botnet) sono *hacker* che si avvalgono di sistemi multipli per coordinare attacchi di *phishing*, *spam* e *malware*.
Gruppi criminali	I gruppi criminali attaccano i sistemi informatici per profitto finanziario. In particolare, i gruppi organizzati criminali usano *spam*, *phishing* e *spyware/malware* per commettere furti di identità e frodi *online*. Le spie industriali internazionali e le organizzazioni criminali organizzate, rappresentano una minaccia per la loro capacità di condurre attività di spionaggio industriale e furti di denaro di grossa entità, ma anche per la loro abilità nell'assumere o sviluppare talenti *hacker*.
Servizi di *intelligence* stranieri	I servizi di *intelligence* stranieri usano strumenti informatici come parte delle loro attività di raccolta informazioni e di spionaggio. Inoltre, molte nazioni stanno lavorando con impegno per sviluppare dottrine, piani e capacità nell'ambito della guerra informatica. Tali capacità consentono ad una singola entità di avere un impatto serio e significativo, danneggiando le infrastrutture economiche, di fornitura, e di comunicazione che sostengono la potenza militare e provocando potenzialmente conseguenze sulla vita dei cittadini in tutto il Paese.
Hacker	Gli *hacker* si introducono nelle reti per il gusto della sfida o per acquisire fama nella comunità *hacker*. Mentre un tempo il *cracking* a distanza richiedeva una consistente dose di abilità e conoscenza, oggi gli *hacker* possono scaricare codici e protocolli di attacco da internet e lanciarli contro i siti presi di mira. Così, se gli strumenti di attacco sono diventati più sofisticati, essi sono anche più facili da usare. Secondo la CIA, la grande maggioranza degli *hacker* non possiede le competenze per minacciare obiettivi difficili come le reti critiche degli Stati Uniti. Tuttavia, la popolazione mondiale degli *hacker* pone una minaccia relativamente alta di un danno breve o isolato che potrebbe causare un danno ingente.

Minaccia	***Descrizione***
Insider	Il lavoratore insoddisfatto interno ad un'organizzazione è una delle principali fonti di crimini informatici. Gli *insider* non hanno bisogno di una grande conoscenza delle intrusioni elettroniche, perché la loro conoscenza del bersaglio permette loro di acquisire un accesso illimitato per infliggere danni o sottrarre dati. La minaccia degli interni include anche i fornitori di servizi *in outsourcing* e gli impiegati che accidentalmente introducono *malware* nei sistemi.
Phisher	Individui, o piccoli gruppi, che eseguono schemi di *phishing* nel tentativo di appropriarsi di identità o informazioni a fini di lucro. I *phisher* possono anche usare *spam* e *spyware*/*malware* per raggiungere i loro obiettivi.
Spammers	Individui e organizzazioni che diffondono *e-mails* non richieste con informazioni false o nascoste per vendere prodotti, eseguire schemi di *phishing*, distribuire *spyware*/*malware* o attaccare sistemi.
Autori di *spyware/malware*	Individui e organizzazioni che compiono attacchi contro gli utenti producendo e distribuendo *spyware* e *malware*.
Terroristi	Individui che cercano di distruggere, danneggiare o sfruttare le infrastrutture critiche per minacciare la sicurezza nazionale, causare vittime su larga scala, indebolire l'economia e abbattere il morale e la fiducia del pubblico. I terroristi possono usare schemi di *phishing* o *spyware*/*malware* per acquisire fondi o informazioni sensibili.

Allegato 2

ELENCO ESEMPLIFICATIVO DELLE PRINCIPALI TIPOLOGIE DI MINACCIA INFORMATICA

Minaccia	***Descrizione***
***Cyber*-spionaggio**	Il *cyber*-spionaggio è l'attività di raccolta di informazioni sensibili, proprietarie o classificate utilizzando strumenti di ricerca telematici e sfruttando internet, reti telematiche, *software* e computer.
Vandalismo	Appartengono a questa categoria gli attacchi diretti a compromettere il funzionamento dei siti *web*, fra cui la diffusa tipologia DoS (*Denial of Service*). Salvo eccezioni, si tratta di attacchi riparabili rapidamente e non in grado di infliggere danni gravi.
Propaganda	L'estensione di messaggi politici attraverso internet o qualunque mezzo che riceva trasmissioni digitali dalla rete, quali telefoni cellulari, palmari, ecc.
Attacchi *Distributed Denial of Service Attacks*	Aggressioni nelle quali un numero rilevante di computer, controllati dal medesimo attore, lanciano attacchi DoS coordinati contro un sistema-obiettivo, per comprometterne il funzionamento.
Sabotaggio di equipaggiamento e strumentazione	Rientrano in questa categoria, ad esempio, l'intercettazione o contraffazione di ordini militari trasmessi attraverso strumenti telematici. Inoltre, le attività militari che sfruttano computer e satelliti per il loro coordinamento sono il principale bersaglio di questo tipo di attacchi.
Attacchi a infrastrutture critiche	Ad esempio, attacchi telematici ai sistemi di controllo di infrastrutture energetiche, idriche, del trasporto e della comunicazione.
Compromised Counterfeit Hardware	Componenti *hardware* che presentano una preventiva installazione di *software* malevolo nascosto, anche all'interno del microprocessore.

Allegato 3

ALCUNI DEI PRINCIPALI CASI CONCRETI DI *CYBERCRIME*

a) *A scopo di frode finanziaria.*

Operazione *Phish Phry*. (65)

La mattina del 7 ottobre 2009 l'FBI, insieme a squadre specializzate della polizia di Los Angeles, del *Secret Service*, della DEA, delle Dogane, degli uffici della procura nazionale USA, di altri enti locali e nazionali e di forze della polizia egiziana, effettua il primo arresto di massa nazionale e multinazionale di 100 persone (47 in Egitto), smantellando un sofisticato sistema di *phishing* ai danni di migliaia di vittime titolari di conti presso numerose banche statunitensi.

L'operazione inizia nel 2007 con un lavoro congiunto fra FBI e banche, in modo da identificare e scompaginare attivamente reti che lavoravano ai danni del sistema finanziario USA. Dopo due anni, si arriva alla decisione di effettuare un'indagine congiunta egizio-americana. Le accuse sono di frode, frode bancaria, furto aggravato d'identità, associazione a delinquere per frode informatica, trasferimenti bancari fraudolenti e riciclaggio internazionale.

Un gruppo di *hacker* egiziani aveva raccolto un numero imprecisato di dati riservati da clienti americani usando tecniche di *phishing*. Sulla base di questi dati sono stati violati i conti correnti di due banche e, in collegamento telefonico ed elettronico, complici americani effettuavano trasferimenti finanziari informatici illegali su conti civetta. Una parte del denaro depredato serviva a pagare i complici egiziani, effettuando una condivisione internazionale di competenze, abilità e tattiche.

Le persone danneggiate sono nell'ordine di centinaia, quelle coinvolte circa 5.000 per un danno imprecisato (con pene massime previste di 20 anni, salvo aggravanti).

Caso Heartland Payment Systems.

Il caso scoppia il 20 gennaio 2009 quando, una delle più importanti società americane per il processamento di carte di debito, credito e strumenti elettronici di pagamento, ammette una penetrazione nel proprio sistema con il furto di migliaia di file riservati. L'azienda di carte di credito Visa aveva segnalato attività sospette a partire dal 28 ottobre 2008.

Nel febbraio 2009, non solo l'FBI ed il Dipartimento del Tesoro, ma anche la SEC (*US Security and Exchange Commission)* e la FTC (*US Federal Trade Commission)*, avevano iniziato indagini sul caso.

Infatti un gruppo di *hacker* era riuscito a superare le difese dei sistemi della Heartland ed a raccogliere dati non cifrati di transazioni di carte di credito gestiti dalla società per conto dei suoi clienti nel settore del

---

(65) Gioco di parole da *Fish Fry* (frittura di pesce) con l'assonanza gergale del termine *phishing* (inganno informatico per carpire dati riservati, « abbocco ») dove questa volta sono i *phishers* ad essere fritti.

commercio. Il danno all'epoca non era quantificabile, ma i commercianti in 250.000 località americane usano i servizi di Heartland. Nello stesso periodo furono attaccati anche altri due gestori di carte di credito: RBS WorldPay (1,5 milioni di clienti compromessi) ed uno non divulgato.

Se venisse individuata della negligenza da parte della Heartland, la FTC ha il potere non solo d'investigare, ma di costringere ad indennizzare i clienti, come successe nel 2006 a ChoicePoint che dovette versare un indennizzo di $15 milioni per aver permesso che criminali accedessero alle schede di 163.000 consumatori.

Nell'agosto 2009 la giustizia ha incriminato il ventottenne Albert Gonzalez (alias segvec, soupnazi, j4jaguar17) per associazione per delinquere informatica e per aver sottratto i dati relativi a più di 130 milioni di carte di credito e debito con la tecnica dell'SQL *injection*, che prevedeva anche l'elusione dei *software* antivirus delle vittime e la cancellazione delle tracce informatiche sia durante la penetrazione dei sistemi presi di mira, sia nella trasmissione dei dati carpiti verso altri *server* (66). Una volta raccolti i dati delle vittime, essi venivano inviati a *server* controllati dai criminali negli Stati Uniti (California, Illinois) e in altri paesi come Lettonia, Paesi Bassi ed Ucraina. In Europa Orientale si trovavano anche i complici per decifrare i PIN da usare con nuove carte false. Nel frattempo Gonzalez continuava ad essere un informatore del *Secret Service* statunitense.

I dati spesso venivano venduti al grande trafficante di carte di credito Maksym « Maksik » Yastremski, che si faceva pagare in moneta virtuale E-Gold e Web Money, oppure con bonifici su banche dell'Europa Orientale. A loro volta gli acquirenti criminali riportavano i dati rubati su nuove carte contraffatte.

Dopo aver guadagnato $11 milioni, Yastremski fu arrestato nel 2007 in Turchia e condannato due anni dopo a 30 anni.

Lo stesso Gonzalez è stato incriminato nell'agosto 2008 in un procedimento differente per il furto di dati ai danni di circa 40 milioni di proprietari di carte di credito o debito di otto grandi ditte di distribuzione. Gonzalez aveva iniziato la sua carriera criminale con un attacco alla catena nazionale di ristorazione Dave & Busters, per il quale è stato incriminato nel 2008. I danni complessivi sono stati stimati a $200 milioni.

I danni maggiori erano stati subiti da Heartland Payment System; 7-Eleven Inc., un noto supermercato texano, Hannaford Brothers Co., una catena di supermercati basata nel Maine, oltre che dalle ditte TJX, Office Max e Barnes & Noble.

Il *phishing* mirato: un caso particolare.

Una variante molto più moderna di questo caso, perché condotta in ambiente totalmente virtuale e con tecniche d'ingegneria sociale, è quella dello *spear-phishing* o del *wale-phishing*. Mentre il *phishing* è come una pesca a strascico, lo *spear-phishing* equivale all'arpionamento di uno specifico impiegato della società prescelta, usando le credenziali *e-mail* di una persona autorevole all'interno dell'impresa, sempre allo scopo di ottenere dati

(66) Un modo di aggirare le difese di un *firewall*. Gonzalez viene condannato a 20 anni nel marzo del 2010.

confidenziali. Lo *whale-phishing* è una variante molto più ambiziosa, perché punta direttamente a persone del calibro dell'amministratore delegato. Un tentativo consiste nell'inviare una citazione a comparire in tribunale come testimone con l'invito a cliccare su un *link* per scaricare la documentazione del caso.

Il fallito attacco britannico alla Sumitomo Bank.

Nell'ottobre 2004 due *hacker* ed un funzionario infedele insieme ad altri complici provarono a sottrarre $423 milioni dai conti aziendali controllati dagli uffici di Londra della banca Sumitomo Mitsui.

Il sistema usato fu l'installazione di un *software* commerciale di cattura della digitazione dei dati (*keystroke-logging)* in modo da sottrarre identità e parole d'ordine necessari per effettuare dei trasferimenti SWIFT. Bastarono due gruppi di credenziali SWIFT (un gruppo ordinario ed uno con privilegi da supervisore) per cominciare l'operazione di frode, dopo aver sperimentato le credenziali su una terza macchina.

L'errore fatale consistette nell'errata compilazione di uno dei campi richiesti per il trasferimento: le operazioni richieste ai danni di conti delle Toshiba International, Nomura Asset Management, Mitsui OSK Lines e della Sumitomo Chemical non ebbero buon fine, e quindi lo storno non comparì sui conti dei criminali in Dubai, Hong Kong e Spagna. Questo era però anche un ostacolo all'indagine, in assenza di una traccia finanziaria da seguire.

L'uso di un programma commerciale non illecito (un classico è il programma di sorveglianza dei genitori sui *computer* in uso a minorenni, impiegato anche per la sorveglianza a distanza di reti di *computer*) permetteva di non farlo identificare come sospetto dai programmi antivirus della rete. Il fatto che non vi fossero trasmissioni di dati riservati al di fuori della rete riduceva ulteriormente i rischi di scoperta. Un'ulteriore precauzione consistette nel formattare le macchine compromesse in modo da distruggere le tracce di manomissione: misura insufficiente perché le tecniche di analisi forense sono in grado di ricostruire anche gruppi di dati assai danneggiati.

Mentre la collaborazione con le polizie belga e francese risultò efficace, le rogatorie nei confronti di Abu Dhabi non ebbero nessun esito. La fattiva collaborazione della banca risparmiò mesi di lavoro e permise d'identificare rapidamente il complice interno, nonostante vi fosse il rischio di una pubblicità negativa.

b) *Attacco ad alcune Infrastrutture critiche nazionali.*

Il caso dell'Indian Eastern Railway.

Il 24 dicembre 2008 un gruppo autodefinitosi Wackerz Pakistan penetra il sito dell'Indian Eastern Railway, danneggiandolo in vario modo. Analisi specialistiche indiane sottolineano che almeno 3 membri di questo gruppo di 6 persone hanno un alto livello d'istruzione professionale e che almeno 2 sono attivi nel settore tecnologico. Un membro del gruppo potrebbe essere un impiegato infedele di una società americana di telecomunicazioni globali.

La società ebbe bisogno di almeno due ore e mezzo per ripristinare il sito (la cui prima linea d'attacco fu rintracciata a Toronto in Canada), ma i visitatori continuarono ancora per diverso tempo ad essere infettati da virus *trojan*. Il metodo più probabile d'attacco era stato l'SQL *injection* con cui gli attaccanti prendono controllo delle basi dati del sito dopo aver manipolato pagine *web* con contenuti attivi.

Apparentemente si potrebbe trattare di un caso di *cyberwarfare*, dichiarato dagli stessi *hacker*. Le conseguenze dell'attacco non permettono, tuttavia, di classificarlo come tale se confrontato con casi analoghi di maggior portata.

I casi d'attacco a biglietti elettronici.

Situazioni più serie riguardano invece le tessere magnetiche usate come biglietti e abbonamenti elettronici.

Il primo caso è del 26 giugno 2008 e concerne le *Oyster Card* usate dalla metropolitana londinese come biglietti per i pendolari. Basate sul *chip* Mifare e presenti sul *Tube* londinese in 17 milioni di copie, esse presentano delle vulnerabilità che sono state sfruttate da operatori olandesi che hanno clonato carte durante un normale viaggio in metropolitana, servendosi di un *laptop*.

Il problema è che lo stesso *chip* è impiegato anche nelle tessere d'accesso per centinaia di uffici e luoghi protetti del governo britannico. Avuta notizia dell'esperimento, il governo olandese ha pianificato la sostituzione di 120.000 *badge* d'accesso per i funzionari del governo centrale.

La stessa ditta Mifare, avuta notizia di pubbliche violazioni compiute con successo tra il 2007 ed il 2008 (Karsten Nohl e Henryk Ploetz con tecniche di *reverse engineering*; gli specialisti della Radboud University di Nijmegen con la pubblicazione dell'algoritmo e di alcune tecniche d'attacco; Nicolas T. Courtois dell'University College di Londra) ha avvisato tempestivamente i clienti, diffondendo in modo riservato tecniche di scoperta degli attacchi e di miglioramento delle procedure di sicurezza nell'architettura generale del *chip* all'indirizzo degli integratori di sistema. Ovviamente la soluzione più radicale è stata la creazione di una nuova carta con cifratura AES a 128-bit, nettamente più resistente agli attacchi.

Un caso con uno strascico legale si è verificato il 9 agosto 2008 a Boston, quando l'ente dei trasporti pubblici del Massachusetts (*Massachusetts Bay Transportation Authority)* ha bloccato per vie giudiziarie la presentazione di tre giovani su come violare la *CharlieCard*, usata nella metropolitana della città. La presentazione includeva tecniche d'attacco, vulnerabilità e *software* correlato. Successivamente la MBTA ha rinunciato ad adire le vie legali (l'ordine di divieto di diffusione dei dati era arrivato troppo tardi) ed ha preferito accettare la collaborazione dei giovani *hacker* nel ridurre le vulnerabilità, offerta che era già stata avanzata sin dall'inizio secondo la pratica di *responsible disclosure*.

* * *

L'attacco al trasporto aereo.

Il 30 giugno 2009 durante una conferenza specializzata Defcon, venne fatta una presentazione in cui si è ipotizzato un DoS (*Denial of Service)* contro una torre ATC (*Air Traffic Control)*. Un attacco basato innanzitutto su un furto d'identità per assumere le vesti di un legittimo pilota, interlocutore di una torre di controllo, in modo da preparare piani di volo credibili e multipli e conclusivamente paralizzare la torre di controllo via Telnet, per via telefonica oppure disturbando le sue radiofrequenze.

Poco tempo prima lo stesso Dipartimento per i Trasporti aveva pubblicato i risultati di un'analisi condotta da KPMG sulla vulnerabilità delle reti in quel settore. Nell'anno 2008 si erano verificati 800 incidenti, dei quali 150 non erano stati neutralizzati alla fine del medesimo anno. Tra questi, alcuni più critici avrebbero potuto riguardare i computer dell'ATO (*Air Traffic Organization)*, la quale a sua volta controlla l'intero sistema ATC.

Anche se le due reti sono indipendenti, specialmente quella amministrativa da quella dell'ATC, mancano i sistemi di scoperta delle intrusioni, tanto più che le reti all'interno del singolo centro ATC sono invece dialoganti. Basta insomma compromettere un centro ATC per penetrare anche l'infrastruttura *telecom* dell'ATC. Per di più, i sistemi per scoprire eventuali attacchi ed intrusioni (IDS, *Intrusion Detection Systems)* sono presenti in misura irrisoria nel sistema della FAA (*Federal Aviation Administration)* e nel *Cyber Security Management Center* (CSMC), che è il centro nevralgico della sicurezza nel *Department of Transportation*. Inoltre gli IDS coprono soltanto alcune componenti di sostegno alla missione della FAA, ma non quella critica del controllo del traffico aereo. A causa di questa carenza, un numero importante di incidenti (17%) non sono stati nemmeno affrontati, perché mancavano dati precisi per poterli individuare al di là di una generica segnalazione.

La risposta della FAA all'analisi della KPMG, pur sottolineando la separazione tra le due reti, ammise la necessità di accettare tutte le raccomandazioni contenute nel rapporto e di lavorare per eliminare i punti deboli segnalati.

* * *

Incertezze tecnologiche e giuridiche.

Un caso che dal 2003 sta ponendo un difficile problema giuridico è quello dell'allora diciannovenne britannico Aaron Caffrey, accusato di aver fatto saltare la rete di computer del porto di Houston (Texas) con un DoS che sfruttava una vulnerabilità del sistema operativo Windows NT e bloccando l'accesso a dati vitali delle compagnie di navigazione e d'attracco per aiutare le navi durante le fasi d'ingresso ed uscita dal porto.

Sia l'accusa che la difesa concordavano sul fatto che:

– dalla macchina di Caffrey era partito l'attacco;

– esisteva una lista di 11.680 indirizzi di *server* compromessi;

– c'era un programma nocivo firmato da qualcuno di nome Aaron, dedicato ad una Jessica (una persona reale all'epoca in una fitta relazione elettronica con l'accusato).

L'accusa aveva sostenuto che l'attacco era preterintenzionale perché inizialmente diretto contro una persona specifica in una *chat line*, mentre la difesa ha ritenuto che fosse vera la storia raccontata da Caffrey, secondo cui altri si erano impossessati della sua macchina con un *trojan*, iniziando l'attacco. Non sono state prodotte prove né che la macchina fosse compromessa, né che esistessero *trojan* autocancellantisi, ma la giuria ha ritenuto di prosciogliere l'imputato.

Questo argomento era già stato usato con successo in un caso di pedopornografia e rischia di creare un precedente nei casi in cui vi siano indizi sulla macchina, ma non sul possessore del *computer*.