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*.