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.