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