PRESIDENZA DEL VICEPRESIDENTE SILVIA VELO

La seduta comincia alle 10,30.

(La Commissione approva il processo verbale della seduta precedente).

Sulla pubblicità dei lavori.

PRESIDENTE. Avverto che la pubblicità dei lavori della seduta odierna sarà assicurata anche attraverso l'attivazione di impianti audiovisivi a circuito chiuso, la trasmissione televisiva sul canale satellitare della Camera dei deputati e la trasmissione diretta sulla *web-tv* della Camera dei deputati.

Audizione del direttore del Servizio di polizia postale e delle comunicazioni, dottor Antonio Apruzzese.

PRESIDENTE. L'ordine del giorno reca, nell'ambito dell'indagine conoscitiva sulla sicurezza informatica delle reti, l'audizione del direttore del Servizio di polizia postale e delle comunicazioni, dottor Antonio Apruzzese.

Do la parola al dottor Apruzzese per lo svolgimento della relazione.

ANTONIO APRUZZESE, *Direttore del Servizio di polizia postale e delle comunicazioni*. Buongiorno a tutti e grazie dell'attenzione, di cui siamo onoratissimi, data la delicatezza del tema che ci vede impegnati ogni giorno. Consegno alla presidenza un documento che illustrerò nel corso della relazione.

La ristrettezza dei tempi e la relativa vastità degli argomenti da trattare mi suggerirebbe di saltare delle parti più o meno « strutturali »; tralascerei dunque – ma lascerò il documento alla vostra attenzione – la parte che riguarda la nostra organizzazione e il nostro modello di attività, mentre mi concentrerei sulle problematiche di maggiore attualità.

Siamo un organo del Ministero all'interno, in particolare del Dipartimento della Pubblica Sicurezza. Abbiamo una diffusione su tutto il territorio nazionale e svolgiamo indagini a tutto campo sostanzialmente su tutto ciò che riguarda l'illecito informatico.

Da una parte, contrastiamo il *cybercrime* classico, ossia i fenomeni di accesso e di utilizzo abusivo ai sistemi informatici e gli attacchi alle reti, dall'altra la pedopornografia *on line*. Svolgiamo un'attività costante e continua per la tutela del diritto d'autore nel mondo del *web*, anche questa una problematica di grande rilievo.

Abbiamo due centri nazionali, entrambi in forza di specifiche leggi, il CNAIPIC (Centro nazionale anticrimine informatico per la protezione delle infrastrutture critiche), su cui vi darò notizie più ampie dopo, e il CNCPO, Centro nazionale per il contrasto alla pedopornografia sulla rete Internet.

Soffermandoci sulla problematica della sicurezza delle reti, oggetto dell'audizione odierna, ci preme porre l'attenzione su due modi diversi di concepire la problematica stessa: quella dei rischi per attacchi dall'esterno e quella dei rischi per attacchi o comunque per illeciti interni, ossia la ripartizione tra rischi esogeni ed endogeni.

Secondo un sentire comune e diffuso, l'opinione pubblica in generale teme gli attacchi informatici che distruggono le reti

e possono bloccare una nazione. È un'ipotesi che può essere ammessa, ma al momento le indicazioni che abbiamo riguardano gruppi criminali, sia di origine ordinaria che di origine eversivo-terroristica, che tendono a utilizzare la rete come strumento piuttosto che porla come oggetto di atti dirompenti.

Sicuramente più diffusa e più pericolosa, in questo momento particolare, si palesa la situazione che interessa la rete come strumento per commettere una serie di illeciti. È una realtà in fortissimo sviluppo.

Faccio una considerazione preliminare per illustrare quanto sia radicalmente cambiato il mondo nel giro di pochissimo tempo. Come si evince dal documento depositato, si è passati, nel giro di dieci anni, da 360 milioni di persone che utilizzavano la rete Internet ai 2 miliardi 200 mila circa di oggi. È un'esplosione inimmaginabile ed è un'esplosione che continua perché il ritmo di espansione è elevatissimo, se si pensa che uno dei fattori che hanno indotto una maggiore espansione del fenomeno è connesso all'utilizzo dei congegni portatili di telefonia. Oramai tutti i nostri telefonini consentono connessioni alla rete.

Questo ha determinato un'esplosione del numero degli utenti: sappiamo che in Italia sono state attivate più connessioni telefoniche mobili di quanti siano gli italiani. È stato calcolato che ogni italiano adulto dovrebbe essere titolare di due-tre schede telefoniche. Oggi ogni scheda telefonica è un terminale per avere connessioni a Internet; quindi, oltre alla fortissima diffusione dei computer veri e propri, tutti ci connettiamo a Internet con il telefonino e per la stessa ragione lo abbiamo dato ai nostri figli. Abbiamo insomma una fortissima espansione del fenomeno.

Questo ha comportato che, per una ragione fisiologica, i nuovi gruppi criminali dediti alla criminalità informatica si sono sviluppati in maniera altrettanto determinata; si tratta di organizzazioni molto composite e molto vaste che richiedono fortissime iniziative di contrasto.

Cos'hanno di particolare queste nuove organizzazioni criminali? Non sono più organizzate in forma individuale, né potrebbero esserlo; hanno strutture organizzative molto composite, transnazionali; arruolano i loro adepti in maniera assolutamente innovativa attraverso il *web*, quindi in forma assolutamente anonima; hanno introdotto nuovi schemi di riciclaggio degli enormi proventi che si assicurano e questo ha reso estremamente difficile il tracciamento delle attività criminali e l'individuazione degli autori; sono organizzazioni decisamente e marcatamente transnazionali.

Oggi, come è stato acutamente individuato dalla Commissione che ha dato avvio a questa indagine conoscitiva, una delle problematiche più serie e più gravi riguarda il furto dell'identità digitale, fenomeno di enorme portata perché alla base di tutto ciò che si riferisce all'illecito sul *web*. Il *web*, in pratica, ha modificato il concetto di identità classica basato sulla presenza fisica di una persona, su una serie di riconoscibilità ovvie per tutti noi – dalle impronte digitali al marcamento dell'iride o ad alcuni particolari della fisiognomica – ed ha portato all'affermazione dell'identità digitale. L'identità digitale non è che la sintesi dell'identità di un essere, di una persona, di un ente, espressa in un concetto numerico, perché l'informatica conosce solo numeri. Se si falsificano quei numeri si falsifica l'identità.

Per essere concreti e per dare una visione pratica di quello che sta succedendo, sono opportuni alcuni richiami alla realtà corrente. Oggi il fenomeno del furto d'identità digitale interessa in forma massiccia i servizi bancari *on-line*, che sono sempre più diffusi, il commercio elettronico e la monetica.

È superfluo rilevare e sottolineare che oggi viviamo all'insegna del *war on cash*: è stata fatta la scelta molto decisa di privilegiare l'utilizzo della moneta elettronica rispetto a quella ordinaria, perché la moneta ordinaria costa. Utilizzare la moneta elettronica costa molto meno e dà molte opportunità e garanzie. Abbiamo infatti rilevato, come struttura di Polizia, che da

quando sono diminuite le quantità di denaro contante nelle banche, negli uffici postali e via dicendo, si è cominciato inevitabilmente a registrare un calo delle forme di criminalità classica, perché i delinquenti sanno che oramai il contante è sempre meno utilizzato. È chiaro che la *mission* è quella di cercare di ridurlo al minimo.

All'interno del documento è contenuta una *slide* che ci diedero i colleghi d'oltreoceano, degli Stati Uniti d'America, sei anni fa, e che noi prendemmo come una di quelle tipiche prospettazioni tecniche di stampo anglosassone, sulle problematiche dell'identità digitale; quei contenuti si stanno rivelando di grande attualità. È chiaro che l'*identity cloning* consiste nel sostituire fisicamente la persona; il *financial identity theft* è il furto di identità per rubare, il *criminal identity theft* è sostituirsi a un'altra persona per commettere reati al suo posto.

In questa *slide* è più o meno sintetizzato tutto il discorso che si vorrebbe cercare di fare oggi. Questi sono i tre tipi di furti di identità digitale più comuni e più importanti; dietro ad ognuno di essi – li illustro velocemente – c'è la spiegazione di tutto ciò che sta accadendo.

Il disegno color salmone in alto riguarda gli attacchi rivolti agli utenti. Si tratta del *phishing* tradizionale, quella che in altri termini viene definita *social engineering*, ovvero un'attività molto capziosa tendente, sostanzialmente, a farsi comunicare dagli utenti del *web* alcuni dati particolari che servono a scoprire il numero di conto corrente *on-line* e il numero della carta di credito. L'utente riceve delle e-mail fasulle, apparentemente provenienti dalla sua banca o dalla direzione delle Poste, tese a rubare questi dati, ormai preziosi per ogni cittadino.

In questo caso, l'errore è favorito in maniera determinante dalla leggerezza della persona. Ci sono dei margini per poter arginare il fenomeno, cercando di sensibilizzare gli utenti verso questo tipo di problema.

Parliamo sempre di attacchi che sono mirati a rubare dati, perché tali sono quelli relativi all'identità digitale.

Questi dati personali possono essere rubati in due modi. Il primo, quello che ho già illustrato, consiste nell'ingannare l'utente *web*: inviare una mail a un signor « x » o a un signor « y » e rubare i suoi dati. Si tratta di un'azione diretta a singoli individui, che richiede un'estrema fatica, perché bisogna ripetere molte operazioni per poter mettere insieme tanti dati.

Un altro tipo di insidia che viene usata oggi è quella connessa all'attacco sistemico alle grandi banche dati. In seguito, mostrerò alcuni casi venuti alla ribalta e riportati dai *mass media*. Attaccando, per esempio, soggetti o enti che gestiscono milioni o miliardi di dati relativi a transazioni o ad attività commerciali, si riescono ormai a ottenere dati delicati e sensibili di centinaia di migliaia o di milioni di persone. In pratica, oggi si ottengono gli stessi risultati che si ottenevano in passato con attività di tipo « artigianale » – ad esempio con il famoso *phishing* di prima generazione – attraverso un'attività criminale massiva e di tipo industriale.

Un'altra forma altrettanto insidiosa, e gravissima, che viene utilizzata per rubare dati delicati e sensibili riguarda l'infezione dei computer degli utenti. L'espressione « virus informatico » è ormai nota a tutti. I virus informatici oggi vengono diffusi con una facilità estrema, anche attraverso un altro fenomeno, che noi non esitiamo a definire la « peste » di questo secolo sul piano informatico e che risponde al nome di *botnet*, un termine tecnico bruttissimo però molto efficace. È un acronimo anglosassone che sta per « *robot network* », cioè una rete di robot.

Una delle principali attività di questi virus consiste nel pregiudicare il funzionamento di centinaia, migliaia, milioni di computer. Ciò non solo crea il malfunzionamento di questi computer, ma consente a chi lo ha determinato di governare da lontano tutti quei milioni di computer come se fossero suoi, all'insaputa di chi ne è proprietario o gestore.

Lo scenario, a questo punto, diventa molto preoccupante: questo genere di insidia porta a infettare centinaia di computer, direttamente o attraverso le *botnet*, ossia le reti di computer. Quindi, dal *phishing* di carattere tradizionale descritto prima, passiamo allo scenario raffigurato nella successiva *slide*. Così si ingannano i computer, che quindi svelano i dati sensibili senza che sia la persona raggirata a farlo. Mentre prima dovevo mandare una *mail* per truffare la persona, ora è possibile inviare un comando al computer mediante il virus. In questo modo, quando la persona si connette alla sua banca, invece di accedere alla Banca di Franconia, invia direttamente al computer del mio complice i dati delicati e sensibili, portandoli a conoscenza di chi non dovrebbe averli.

Questo schema mostra quello che avviene oggi sul piano criminale nella rete.

Per avere un'idea concreta di quello che sta accadendo: la maggior parte di queste insidie vengono diffuse nel mondo degli strumenti elettronici di pagamento e delle carte di credito.

Troverete nel documento dei ritagli di stampa. Questo è un famoso caso da 400 milioni di dollari che in America nel 2005-2007 ha riguardato Gonzales. Il caso della Stratfor è venuto all'attenzione di tutti. Si tratta di una multinazionale americana che vende informazioni di alta qualità a milioni di utenti. Il database della Stratfor è stato violato, ed è stata rubata un'enorme quantità di dati sensibili su persone ed enti. Henry Kissinger è stato tra le prime vittime. Questo è un esempio anonimizzato dei dati da carte di credito sottratti violando la banca dati di Stratfor.

Gli allarmi vengono lanciati da persone autorevolissime. Lo scenario che si sta profilando lascia poco tranquilli: il 7 giugno di quest'anno il segretario generale del Consiglio d'Europa ha dichiarato che ogni giorno vengono infettati tre milioni di personal computer.

Un altro virus formidabile che ha contagiato la rete è *Flame*. Lo cito perché è un esempio di conseguenze deleterie di una sorta di « fuoco amico », che certe attività di difesa delle istituzioni possono produrre. *Flame* è uno di quei famosi virus d'attacco che alcune nazioni hanno messo a punto come possibile strategia di risposta a minacce informatiche di natura bellica. Purtroppo questo virus, dopo poco tempo, è caduto nelle mani di organizzazioni criminali classiche ed è stato rivolto contro chi lo aveva creato.

Riassumendo quello che si è detto finora, i furti d'identità possono realizzarsi attraverso: il *phishing*, di cui si è parlato; gli attacchi logici, rubando le credenziali mediante infezioni dei computer; gli attacchi fisici, che consistono nel manomettere gli Atm per il prelievo bancomat interponendo una telecamera o un minischermo per rubare i dati; le clonazioni di carte di credito; e infine, il famoso *social engineering*, ossia ingannare artatamente e con astuzia una persona per ottenere i suoi dati sensibili.

Le nuove forme di azione criminale sono estremamente efficaci. Per dare una dimensione del fenomeno, vi illustro i dati che abbiamo rilevato, aggiornati al 31 luglio. Potete vedere la progressione dal 2009 al 2011. Abbiamo registrato un notevole aumento nei furti di identità digitali. Attualmente, in Italia, questi riguardano in maniera preponderante i codici di pagamento elettronico, ma anche i codici di accesso ai servizi di *home banking*.

Un'altra indicazione estremamente importante è che i clienti bancari che subiscono questo tipo di attacchi criminali sono passati dallo 0,06 per cento del 2010 allo 0,16 per cento del 2011. Questi ultimi dati riguardano i clienti *retail*, quindi al dettaglio. Ma quando si considerano i clienti *corporate*, quindi le aziende, il dato è enormemente più alto; si parla infatti dello 0,51 per cento. Questa differenza è dovuta al fatto che le aziende sono in genere molto meno attente dei privati nella gestione dei propri sistemi informatici, in parte perché non vi è un'adeguata cultura della sicurezza.

Questi dati ufficiali ci mostrano come il *phishing* tradizionale sia molto diffuso anche nell'anno in corso. Qui potete farvi un'idea sintetica di dove gli utenti del *web* incontrano le pagine di *phishing*. Nel do-

cumento troverete un dettaglio sull'Europa, dove a destra sono elencati i posti dove si trovano i siti che contengono pagine clone e pagine di *phishing*. Potete vedere che l'Italia, pur non essendo tra i Paesi più attaccati, è comunque molto interessata da questo fenomeno.

In un'altra *slide* è mostrata la differenza tra il *phishing* di nuova generazione – basato sull'attacco dei computer attraverso i virus – e quello tradizionale, con una prevalenza del 96 per cento del primo tipo; si tratta quindi, ormai, di un predominio assoluto.

Quello che vedete è un dato relativo ad una giornata, quella del 19 luglio, e queste sono le *botnet*, quelle micidiali reti di computer infette. Abbiamo rilevato che l'Italia era tra i primi Paesi al mondo in quanto ad attività di *botnet* in quel momento. Nel mese di ottobre del 2011, l'Italia è seconda solo all'India, per la localizzazione di *botnet*.

In una successiva *slide* potete vedete una *botnet* connessa a un virus, *Torpig*, che è riuscito ad infettare – e parliamo di dati relativi al gennaio 2009 – ben 46.000 computer in Italia: siamo secondi solo agli Stati Uniti d'America.

Sono mostrati, ancora, altri virus con *botnet* che danno un'idea di quello che sta succedendo in materia di telefonini, spiega come il contagio passi dai computer ai telefoni ed evidenzia il grave pericolo che si corre.

Vi illustro come agisce il virus *Zeus*, uno dei più pericolosi, che ha determinato anche *botnet* che lo utilizzano. Poniamo che stiamo consultando il sito della nostra banca; all'improvviso compare una pagina con una grafica che sembrerebbe assolutamente conforme a quello che può essere un comunicato della banca, in cui, spiegando che si sta sistemando il sito, ci si chiede di scrivere il numero (e il modello) del telefonino e di specificare la nazione cui si appartiene.

Dopo aver comunicato questo dato sul nostro telefonino arriverà immediatamente un *sms* in cui si comunica che in un *link* che viene specificato troveremo una serie di indicazioni per migliorare la sicurezza del nostro sistema. Nel momento in cui apriremo quel *link* dal nostro telefonino, questo sarà infettato da *Zeus*. Ciò significa che il sistema informatico del telefonino è pregiudicato. L'infezione, quindi, si sposta dai computer fissi ai telefonini e questo segna la fine della nostra *privacy* perché abbiamo consegnato la chiave di casa al nemico. Potete capire perché il pericolo è veramente serio.

Trovate anche, nel documento, pagine consultabili liberamente in rete – un vero mercato nero – dove è indicato il costo in dollari delle carte di credito per nazione; c'è un esempio schermato di attività investigative che si riferisce a *chat* tra bande criminali, da cui si può vedere come si scambino dati di carte di credito italiane, con o senza il numero di sicurezza e con tutti i dati.

Veniamo ora all'attività di contrasto che stiamo svolgendo. In una *slide* potete leggere il dato riferito ai denunciati che, apparentemente, si presentano in flessione rispetto allo scorso anno, anche se il dato si legge diversamente quando parliamo degli arrestati. La tecnica di contrasto è stata molto affinata e come vedete non sono mancati importanti risultati.

Come guardare al futuro per trovare ulteriori margini di sicurezza e di prevenzione ? Sicuramente è necessario agire nel settore della prevenzione. È fondamentale la sinergia pubblico-privato, che noi abbiamo cercato e ottenuto, per esempio, nella tutela delle infrastrutture critiche, e vi mostreremo in che modo.

Il progetto OF2CEN è un piano di lavoro importante finanziato dalla Comunità europea, cui abbiamo aderito e che abbiamo portato avanti in sinergia con tutte le banche italiane attraverso l'ABI (Associazione Bancaria Italiana).

Si tratta di schemi, sia il primo che il secondo, basati sulla condivisione in tempo reale delle situazioni di rischio poiché nel mondo dell'informatica è di estrema rilevanza conoscere immediatamente le anomalie che si stanno verificando, così da poter allestire barriere di difesa comuni a tutti. Questo modo di operare sta dando grossissimi risultati.

Occorre affinare sempre più gli organismi investigativi e migliorare le tecniche di risposta, che coinvolgano tutti i settori istituzionali, non ultimo il legislatore. Il furto di identità digitale non ha, oggi, un'autonoma previsione normativa in Italia: ciò significa che dobbiamo arrangiarci, insieme ai magistrati, utilizzando schemi obsoleti sul piano giuridico per cercare di inquadrare questo fenomeno. Sarebbe opportuno prevedere autonome configurazioni legislative.

Abbiamo parlato di prevenzione attiva e formativa; dobbiamo insistere molto con i giovani, nelle scuole – cosa che stiamo facendo – e con campagne generali che stimolino l'aumento della sensibilità verso forme di sicurezza più adeguate.

Se tutti aumentiamo il livello di sicurezza nell'utilizzo degli strumenti informatici, possiamo rendere più difficile la vita ai criminali. Lo possiamo percepire, ritornando allo schema illustrato precedentemente, parlando di sinergie di contrasto. Abbiamo già notato che contro la forma di *phishing* tradizionale sono state particolarmente produttive le campagne di stampa, gli annunci, i consigli alla gente a non affrettarsi a comunicare dati personali quando vengono chiesti.

È chiaro che, nel caso in cui parliamo di attacchi ai sistemi informatici degli utenti, di virus e *botnet* che ingannano i nostri computer di casa, richiediamo una sensibilità verso forme di sicurezza più evolute, che attengono alle macchine e, quindi, a una serie di accorgimenti tecnici che tutti noi dovremmo sentirci obbligati ad adottare perché, oramai, comunichiamo attraverso queste macchine.

A proposito dei grandi sistemi informatici, affrontiamo un'altra tematica molto seria relativa a quello che potrebbe essere lo scenario del prossimo futuro: l'intensificarsi degli attacchi alle grandi banche dati. I dati oggi valgono molto di più del denaro, perché sono essi stessi produttori di denaro. Per questo motivo, a tutela di tutti, si impone l'adozione di criteri di sicurezza adeguati da parte di chi gestisce grandi banche dati. È chiaro che tutto ciò comporta degli oneri: migliorare le strutture di difesa di queste banche significa aumentare i costi. È però fondamentale rafforzare queste banche, perché si rischiano perdite molto ingenti.

Quando una banca dati di grandi dimensioni « salta », non si perdono i dati di cento cittadini, ma di milioni di cittadini, assicurando introiti enormi a chi riesce a fare questo « colpo ».

Per chiudere, parlando di sicurezza esterna, vorrei fare l'esempio del nostro CNAIPIC, il centro di tutela delle infrastrutture critiche contro gli attacchi informatici. Abbiamo stupito i nostri colleghi dei Paesi più avanzati, americani e inglesi, applicando una logica che ci siamo forse portati dietro dalle nostre esperienze medievali, quando eravamo il « Paese dei castelli », laddove i vari micro-centri avevano capito che il sistema migliore per proteggersi dalle aggressioni dei barbari era quello di avvertirsi immediatamente dell'attacco in corso, magari attraverso i segnali di fumo.

Applicando lo stesso principio all'informatica, abbiamo creato una rete di collegamento tra la maggior parte degli enti più importanti nella vita strategica nazionale. In questo modo, il minimo attacco verso uno di questi « castelli » immediatamente ci viene segnalato, e noi lo comunichiamo a tutti, in maniera anonimizzata, affinché tutti possano subito tirare su il ponte levatoio, alzare le mura e mettere gli arcieri dietro i merli per difendersi.

Questo sistema ci fornisce anche una serie di dati identificativi di chi prova gli attacchi, dati che possono essere utilizzati in futuro per eventuali indagini, permettendoci di studiare il fenomeno. È un'idea che si sta rivelando vincente e che consideriamo un piccolo motivo di vanto nazionale soprattutto quando se ne discute in ambito internazionale.

Faccio un'ultima considerazione sul problema delle banche dati. Spesso ci troviamo a discutere in ambito istituzionale con il settore che tutela la *privacy* in Italia. La situazione attuale lascia chiaramente capire che la *privacy* dei cittadini è veramente a rischio a causa di questo tipo di attacchi. Si tratta infatti di aggressioni

mirate a far saltare banche dati contenenti dati riservati. L'attività di contrasto comporta la necessità per noi di attingere a certe banche dati che dobbiamo costituire per creare i precedenti su cui lavorare. Non è sicuramente in questo tipo di detenzione di dati che si possono riscontrare dei pericoli per la *privacy* dei cittadini. Il pericolo risiede nell'attacco che arriva in maniera sistemica dall'esterno.

Le problematiche connesse all'imminente esaurimento dei dati di connessione del vecchio tipo IPv4, nelle more del passaggio al nuovo tipo IPv6 richiedono una forte sensibilità verso nuovi metodi di archiviazione dei dati. Paradossalmente, un'attività di contrasto richiede la possibilità, da parte degli operatori, di archiviare dati relativi ad attacchi e criminali. Questo è fondamentale per condurre una lotta concreta.

Ho concluso la mia sintesi. Resto a disposizione per ogni tipo di chiarimento.

PRESIDENTE. Grazie. Do la parola ai deputati che intendono intervenire per porre quesiti o formulare osservazioni.

JONNY CROSIO. Ringrazio il direttore Apruzzese per la sua relazione e vorrei chiedere alcuni chiarimenti.

Innanzitutto concordo sul fatto che è estremamente preoccupante quanto la rete sia altamente debole e vulnerabile. Se paragonata, infatti, al modo corrente con cui si riesce a contrastare la criminalità nel mondo reale, la rete è molto più debole. Questo ci preoccupa molto perché è patrimonio del Paese e come tale, oltre che essere valorizzata, deve essere tutelata. Le nostre audizioni sono proprio centrate su questa questione.

Vorrei capire, in relazione alla pedofilia, quanto si deve ancora fare nella collaborazione internazionale. Risulterebbe che i dati siano parcheggiati in un sistema ridondante in vari Paesi, specialmente quei Paesi *border line* per quanto riguarda determinate regole che dovrebbero esserci o che i Paesi dovrebbero avere: quante difficoltà avete nel contrastare questo fenomeno nei rapporti internazionali ? Quali problemi riscontrate ? Servono accordi bilaterali ? Dovete ricorrere a rogatorie internazionali ?

Credo, infatti, che da questo punto di vista il problema esista e anche questo aspetto è molto preoccupante. Credo che la « porcheria » depositata sulla rete in questi grandi *server*, che adesso sono qua e tra due ore possono essere parcheggiati da un'altra parte, a centinaia di migliaia di chilometri, crei grossissimi problemi nell'individuazione e nell'annientamento di questo fenomeno, che coinvolge gli utenti più deboli, anche se alla fine sono quelli che navigano in maniera più dinamica. Vorrei capire quanto possiamo fare.

Inoltre, lei ha accennato agli *Zeus' botnets*, un fenomeno veramente preoccupante. Anche in questo caso, sappiamo che le banche, anche importanti, stanno sempre più implementando quale procedura di sicurezza l'utilizzo del secondo passaggio, ossia il secondo livello di sicurezza, per cui inviano un sms con un ulteriore codice. Prima esisteva il *token*, in cui era generato questo numero. Si stanno orientando tutti a un ID *number* con una *password* che andrebbe a generare un sms. Questo va in pieno contrasto coi nuovi virus, devastanti per gli *smartphone*. Sotto questo aspetto, cosa si può fare ? Questa strada è sbagliata ? Credo che le banche o i grandi istituti finanziari possano essere, da questo punto di vista, sensibilizzati.

Concordo con lei sul fatto che in campo normativo forse potrebbe uscire, anche da questa Commissione, una proposta di legge sul furto di identità, in modo che diventi un reato perseguibile ben specifico all'interno dell'ordinamento nazionale.

SANDRA ZAMPA. Ringrazio il dottor Apruzzese per la sua relazione molto interessante. Il vostro lavoro mi è noto per l'alta qualità anche di ciò che ho visto dall'osservatorio della Commissione infanzia, di cui faccio parte.

In questo momento al Senato si sta votando in sesta lettura la ratifica della Convenzione di Lanzarote, che tra l'altro metteva in discussione anche il vostro ruolo. Probabilmente, questo sarà, invece,

un problema che si dovrebbe risolvere, visto che è stata approvata alla Camera in quinta lettura con dei paletti molto precisi. Ritengo che la Convenzione, dal punto di vista della tutela della pedopornografia, rappresenterà, effettivamente, un passo avanti.

Il tema mi interessa molto. Mi domando se dopo Lanzarote vi stiate interrogando sulle nuove frontiere. Quanto ci avete mostrato questa mattina ci dimostra che si tratta di una sorta di rincorsa nel sistema di controllo. Lei stesso ha riconosciuto che occorre intervenire immediatamente, altrimenti si arriva sempre troppo tardi. Mi domando se, invece, non convenga e non sia già, come mi auguro, allo studio a livello internazionale una sorta di previsione di cosa convenga cominciare a mettere in atto trattandosi di un inseguimento a tutti gli effetti.

Mi interessa anche molto un approfondimento sulla *slide* relativa al CNAIPIC, in cui elencate tutti gli enti o aziende che partecipano. Quelli che non sono presenti nella lista non partecipano ? Poste Italiane non c'è e lo sottolineo per una ragione. È arcinoto a tutti noi, ma credo anche a voi, che i parlamentari sono oggetto di una valanga di *e-mail* con cui si cerca, ovviamente, di fare in modo che siano forniti i nostri dati. Arrivano normalmente dalle banche, per cui mi domando perché il sistema finanziario italiano sia così assente da questa rete. Da Poste Italiane, ad esempio, arrivano in una quantità mostruosa.

Inoltre, sicuramente la nostra posta passa attraverso un filtro: perché non esistono filtri o, se esistono, perché non funzionano e perché arriva così tanto di quello che volgarmente chiamiamo *spam*, in realtà un fenomeno molto peggiore da quanto andate affermando ? Immagino che siano pochi tra noi quelli che, come pesci, abboccano, appunto, al *phishing*, ma se arriva a noi chissà a quanti altri arriva.

Mi aveva meravigliato, a suo tempo, nella breve esperienza che ebbi anche a Palazzo Chigi, la stessa identica cosa. Mi colpisce molto che ai livelli più alti, dove ci si aspetterebbe forme di filtro nella posta, invece non ci sia assolutamente nulla. State lavorando, da questo punto di vista, in vista di un filtro nell'arrivo ? Possiamo enumerarvi, se vi interessa, le banche, ma darei per scontato che sappiate che tutte le banche risultano clonate, ossia tra quelle false che chiedono i dati.

L'altro ente presente sempre è Poste Italiane. Qui vedo, tra le aziende coinvolte, anche UniCredit Group, che infatti arriva molto meno. Montepaschi Siena c'è spessissimo, come Banca Intesa: non converrebbe, a meno che non sia già in corso, un lavoro molto più intenso con le banche ?

Lei, però, ha fatto un'affermazione molto più preoccupante, ossia che sono le aziende, ancor peggio, a lasciare il cliente molto più scoperto. Significa che quando si effettuano acquisti con la carta di credito i dati possono essere pescati con molta più facilità: è così ? Ho capito bene ?

DARIO GINEFRA. Ringrazio il dottor Apruzzese. Pongo una domanda secca rispetto a un fenomeno che nella relazione non è stato trattato, ma che è all'ordine del giorno dell'agenda politica. Abbiamo sempre più a che fare con una sorta di squadrismo informatico, che colpisce la politica attraverso i *social network*, le reti, tutti gli strumenti anche di comunicazione politica. Molto spesso queste azioni sono figlie di una vile copertura attraverso *nickname* che non consentono di conoscere direttamente l'identità della controparte, di per sé deterrente a qualsiasi azione legale nei confronti dei protagonisti.

Vorrei comprendere se esiste, da fornire alla Commissione, un dato circa il successo delle indagini compiute per l'identificazione dei protagonisti a seguito di denunce. Mi risultano presentati diversi esposti proprio per colpire un fenomeno che – mi rendo conto – dovrebbe essere oggetto di una più attenta trattazione da parte del legislatore. Anche a questo proposito, quindi, le chiedo qual è la percentuale dei reati perseguiti, quale è stata la percentuale, eventualmente, dei trasgressori colpiti e quali possono essere, invece, i limiti all'azione di controllo e di identificazione.

Molto spesso non incidono direttamente sull'economia o sui reati che lei ha avuto l'attenzione di sottoporci dal punto di vista statistico, ma non sappiamo quanto influenzino il decisore politico e il cittadino e consumatore, soprattutto quando protagonista della discussione. Può trattarsi di materie economiche, questioni che riguardano la vita del Paese. Potrebbe crearsi un'influenza che si riversa nell'individuazione del trasgressore facendo emergere anche fenomeni politici – è inutile fare nomi, credo che il mio riferimento sia abbastanza chiaro – dell'ultima ora, finendo per condizionare, sia pure indirettamente, tutto il sistema Paese.

ANTONIO MEREU. Anch'io ringrazio il dottor Apruzzese per la sua utile relazione. Parlo da persona non esperta in materia, che quindi, come tale, predilige il contante alla carta di credito, e parlo quindi a nome dei molti che si trovano nella mia stessa condizione.

Questa diffidenza mi porta a rivolgerle questa domanda: quando il singolo, non le aziende o le società, può accorgersi di essere stato truffato ? Quali iniziative può prendere ? Deve aspettare necessariamente che sia la banca a essere coinvolta ? Se può prendere un'iniziativa, verso chi può farlo ? Può esserci con la polizia una relazione diretta o indiretta in modo che anche il singolo si senta più tranquillo ?

Onestamente, devo dire che oggi non sempre le banche sono troppo attente a queste problematiche. Devo essere io a controllarmi ogni giorno il conto per essere tranquillo. Chiedo se, per migliorare questo tipo di rapporto, esiste la possibilità che il singolo contatti la polizia, e quindi possa essere tutelato in una maniera particolare.

PRESIDENTE. Mi aggancio a quest'ultimo intervento e a quanto detto dal dottor Apruzzese e dai colleghi. Ho già sollevato il dubbio in altre audizioni su quali tutele esistano per i consumatori.

Per il caso di furto di identità digitale si è già risposto: nessuna, se ho capito bene, e, in ogni caso, mi pare risulti problematico definire una fattispecie di reato. Quali sono le tutele per i consumatori nel caso in cui un utente subisca gli effetti di un attacco perpetrato contro una banca, e quindi sia vittima di una sottrazione di denaro dalla carta di credito o dal conto ? Può rivalersi nei confronti della banca o dell'altro soggetto che ha subìto, rimanendo comunque egli stesso la vittima ?

Se non è così, credo che sia il caso, al di là se questa indagine conoscitiva sia arrivata o meno a compimento, che come Parlamento ci poniamo il problema di un'iniziativa legislativa che tenga conto delle fattispecie di reato non previste dal codice rispetto alle innovazioni tecnologiche, sia dal punto di vista dell'identità dei furti di dati, di identità digitale e così via, sia dal punto di vista del rapporto tra consumatore e istituti di credito e analoghi.

Dalle audizioni svolte mi pare, infatti, di capire che anche in questo secondo caso l'utente paghi di tasca propria e l'istituto di credito non risponda all'utente dell'eventuale attacco. Alla domanda aggiungo, quindi, la richiesta di una proposta che possa aiutarci dal punto di vista tecnico nei confronti di un percorso legislativo che potrebbe vedere proprio l'iniziativa della nostra Commissione.

Cedo la parola al dottor Apruzzese per la replica.

ANTONIO APRUZZESE, *Direttore del Servizio di polizia postale e delle comunicazioni*. Vi ringrazio per le osservazioni, che sicuramente saranno utili. Cercherò di seguire l'ordine degli interventi.

La prima istanza riguarda le problematiche nell'evoluzione della pedofilia e del coinvolgimento di realtà di Stati diversi, quindi le possibilità che più o meno aveva l'Italia. In parte, su questo argomento, penso anche di rispondere all'onorevole Zampa: in materia di pedopornografia, grazie a un intervento forse unico nel panorama internazionale fino a pochissimo tempo fa, l'Italia è riuscita a ergere un muro forte perché ha introdotto il discorso famoso delle *blacklist*, e quindi del filtraggio.

Questo significa che il problema in Internet, in generale, non sorge quando le vicende riguardano esclusivamente situazioni italiane. Se i *server*, i siti sono in Italia, giochiamo con le nostre armi istituzionali, con la magistratura, col nostro codice di procedura penale, sequestriamo, oscuriamo e ci muoviamo sul territorio in cui vige la giurisdizione dello Stato italiano.

Purtroppo, nella quasi totalità dei casi Internet ci porta fuori, a siti con contenuti pedopornografici anche pesantissimi, diffusi e nascosti in giro per il mondo, oggetto di trattative tra trafficanti di questi dati che definire turpi è ben poco. Con la norma che ha istituito la *blacklist*, a seguito dell'attività di monitoraggio che svolgiamo, anche sulla base di segnalazioni di utenti, di cittadini, redigiamo una lista di siti stranieri che contengono questo genere di materiale, e che quindi vanno oscurati, usando un termine forte.

Si procede quindi a una comunicazione a tutti i *provider* della lista nera affinché questi possano impedire agli utenti italiani di connettersi a quei siti. Questo ha costituito una svolta decisissima per l'Italia, un punto di arrivo fondamentale. Il problema è che, nel frattempo, la realtà tecnica e di costume si è evoluta enormemente e questo vale un po' tutta la rete, tutte le fenomenologie criminali connesse, non solo la pedopornografia.

Oggi il pericolo non è più o, comunque, non è più tanto nelle realtà dei siti, in queste piattaforme più o meno fisse diffuse per il mondo, che consentirebbero l'operazione di oscuramento, ma è dato dal fatto che Internet ha consentito forme sempre più invasive di interrelazione. I *blog*, le *chat* – realtà di soli tre anni fa – sono diventate preistoriche dopo l'avvento dei *social network*.

Uno dei pericoli più seri per la nostra infanzia è costituito dal fatto che il problema non è più tanto rappresentato dal sito con materiale pedopornografico, quanto dalla possibilità di navigare in rete in forma illimitata attraverso i *social network*. La lotta si sposta su altri fronti, e purtroppo non abbiamo le chiavi per gestire un certo tipo di contesto. I *social network* sono quasi esclusivamente stranieri, e quindi gestiti e regolati da altre normative e altre autorità di governo.

Vi è da dire che, in materia di pedopornografia, data la delicatezza del tema e in forza di un riconoscimento quasi sulla base di un diritto naturale, notiamo e abbiamo rilevato una consonanza quasi unanime da parte della compagine internazionale, per cui si stanno compiendo grossi passi per cercare di bloccare questo tipo di condotte, in particolare anche nei rapporti con i *social network*, e si stanno ponendo dei freni, per limitare i danni.

È chiaro che un'attività di sostegno, di formazione, di vicinanza verso le classi più deboli, i giovani, i ragazzi, sono fondamentali. *Facebook* è diventato un nuovo Internet, elevato al quadrato, e noi dobbiamo formare i ragazzi all'utilizzo di queste nuove macchine, che sono piccole navicelle spaziali che consentono di andare in giro nel mondo e forse anche fuori dal mondo. Ecco la necessità di percorsi di formazione ed educazione alla legalità, che devono impegnare un po' tutte le istituzioni.

I *social network* stanno cominciando a sensibilizzarsi alla vicenda e a dare delle risposte abbastanza concrete in termini di collaborazione e di aiuto. Si stanno stipulando accordi di cooperazione, che però necessariamente passano attraverso il complicato percorso dell'assistenza giudiziaria internazionale, rogatorie e tutto quanto ne consegue.

Stiamo cercando di accorciare questi tempi, questi spazi, con accordi diretti per semplificare e accelerare le procedure, grazie a rapporti intensi con i magistrati di collegamento che abbiamo in Italia, per cercare di evadere nella maniera più sollecita un certo tipo di richieste, e contemporaneamente attivandoci su tavoli internazionali per definire strategie comuni e provare a portare più persone possibili a questo tavolo.

La Convenzione di Lanzarote, che speriamo sia approvata dal Senato nella sua forma definitiva, introduce, ad esempio, nuove forme di illecito prima neanche

previste, come il famoso adescamento, con termine anglosassone, il famoso *grooming*. Prima adescare un minore attraverso Internet non era illecito, e quindi non era perseguibile. Se passa questa norma, lo sarà. La Convenzione di Lanzarote prevede anche un'intera altra serie di norme di dettaglio anche sul piano processuale, che sicuramente miglioreranno l'attività di contrasto.

Vengo a una velocissima considerazione per quello che riguarda, invece, il settore delle *botnet*, dei filtri presenti nei rapporti con le banche e altro. Bisogna fare chiarezza su un punto. Giustamente e con estrema acutezza, è stato rilevato che mancava l'indicazione di Poste: quello era un semplice riferimento indicativo essendo un quadro in evoluzione. La convenzione con Poste sta per essere sottoscritta, ma sono già in corso attività di contatto con questo ente.

Il problema delle pagine di *phishing* di Poste Italiane, delle banche, va visto in una sua dimensione un po' più tecnica. Molto spesso diamo per scontati alcuni concetti che, invece, tali non sono. Le pagine di *phishing* sono create da organizzazioni criminali per ingannare gli utenti, e quindi rubare credenziali. Si crea la pagina di *phishing* della banca o di Poste Italiane e lì si vanno a ingannare i cittadini sul piano personale. Parlavamo di *social engineering*.

È chiaro che, per quanto il fenomeno sia ormai abbastanza ridotto rispetto alle forme di *phishing* molto più evolute tecnologicamente, quelle che ingannano i computer degli utenti, campagne di formazione, di sensibilizzazione verso forme di maggiore sicurezza hanno dei grossissimi risultati. È, inoltre, evidente che addentrarsi nel complicatissimo discorso, a questo punto di natura civile, per individuare responsabilità o altro attiene a un altro contesto molto complesso, che porta ad analizzare le eventuali condotte più o meno colpose nella causazione di certi danni.

Per quello che riguarda le pagine di *phishing* oggi c'è una forte attività di contrasto. Si tende a trovarle, ad eliminarle. Gli stessi istituti bancari ne hanno tutto l'interesse. La stessa società Poste Italiane ha sviluppato un suo reparto autonomo. Stiamo lavorando in sinergia. Il progetto di cui parlavo alla fine della mia relazione è una delle manifestazioni più concrete ed evidenti e ci stiamo lavorando in maniera molto definita.

Sfugge forse alla maggior parte degli utenti del *web* e dei cittadini, per esempio, che le pagine clone possono riguardare *Facebook*, come abbiamo scoperto la scorsa settimana. Realizzare una pagina clone di *Facebook* è come avere creato una trappola per mosche in cui cadono miliardi di mosche. Immaginate le migliaia di persone che incautamente pensano che quella sia la porta di *Facebook*, vi bussano, danno le proprie credenziali e da lì rubano i dati bancari, i dati dell'*account* di posta. È chiaro, infatti, che rubando l'*account* di posta si rubano i dati bancari, quindi il problema è il furto dei dati personali, come dati patrimoniali, codici di accesso ai sistemi di *home-banking*, alla monetica, o semplicemente dati personali *tout court*.

Una delle cacce più grosse che oggi alcune organizzazioni criminali stanno esercitando è quella della conquista dei dati personali. In ambito commerciale, ad esempio, le campagne pubblicitarie devono essere oggi estremamente mirate, c'è un bisogno fortissimo di disporre di dati sulle persone. Chi vende creme di bellezza deve sapere quali sono le signore di una fascia d'età dai 40 ai 60 anni – l'ho buttata lì – perché deve mandare a quelle utenti un certo tipo di pubblicità, per cui pago per certi tipi di dati. Ecco perché chi ruba quei dati o se ne appropria illecitamente ha un mercato estremamente florido. Questa è una realtà.

Credo ci sia stata una mancanza di chiarezza da parte mia, soprattutto dovuta alla velocità con cui ho dovuto esporre la difficile *slide* dei dati dei sistemi bancari *on-line* vittime di forme di *phishing* di prima o, soprattutto, di seconda generazione. Ho indicato la differenza tra clienti delle reti *retail* e quelli *corporate*, ossia tra

utenti singoli, Antonio Apruzzese col suo conto bancario *on line*, e l'azienda che ha un conto *on line*.

In sostanza, oggi stiamo rilevando insieme alle banche che sono proprio le aziende a subire un maggior numero di attacchi rispetto ai singoli. La spiegazione concorde è che ciò sia dovuto al fatto che, mentre il singolo, oggi, comincia a essere più attento nella gestione della sua vicenda personale, del suo rapporto con la banca, l'azienda lo è meno proprio perché il rapporto si spersonalizza e perché non ha ancora quell'adeguata cultura di sicurezza per cui i centri di governo dell'azienda gestiscano direttamente attuando controlli gerarchici più attenti. C'è molta più improvvisazione e più leggerezza. Queste sono spiegazioni date su un fenomeno. Di fatto, questo è il dato reale che abbiamo rilevato.

Vado a una velocissima considerazione sulle problematiche dei *social network* e delle campagne di diffamazione orchestrate, mirate. Posso dire subito, per tranquillizzare, che, laddove l'esperibilità di certi tipi di percorsi investigativi e giudiziari è consentita, i risultati sono ottimi e si arriva a identificare chi ha messo su *Facebook* o *Twitter* un certo tipo di contenuto.

Il problema base è che, siccome, come dicevo, questi *social network* sono governati da altri sistemi stranieri, altre leggi, altri giudici, bisogna esperire un certo tipo di percorso e accertare se, sostanzialmente, quello che giudichiamo illecito penale in Italia, tale quindi da avviare un percorso giudiziario ad esempio per diffamazione, ad esempio, sia riconosciuto dal Paese verso il quale andiamo a porgere certi tipi di istanze per avere dei dati.

Purtroppo, ad esempio – questa è una delle fortissime limitazioni – nel mondo anglosassone, che gestisce la maggior parte dei *social network*, il concetto di diffamazione come reato, come concetto giuridico, è molto diverso dal nostro. Loro sono a favore di un principio generalizzato del *free speech*.

Purtroppo, io ragiono in termini *de iure condito* per la situazione in piedi attualmente. Quando ci troviamo di fronte a situazioni di semplice diffamazione, la risposta che ci proviene è sempre negativa perché ci dicono che nel loro sistema non è reato.

Attivano sistemi di risarcimento civile, un tipo di logica completamente diverso, che magari è molto più pesante sul piano risarcitorio, ma a livello di cooperazione internazionale crea indubbiamente delle difficoltà. Qualora, tuttavia, si tratti di attività come l'incitamento alla violenza o l'istigazione a delinquere, una serie di reati riconosciuta anche da parte dei Paesi corrispondenti, i risultati investigativi sono assolutamente positivi, anzi riusciamo quasi sempre ad arrivare a un punto finale.

Un ultimissimo dato, credo sempre comune a molte questioni poste, riguarda i rapporti con le banche: la tutela. Chiedo ancora scusa per l'estrema velocità con cui ho esposto *slide* molto delicate sul piano del contenuto. Oggi, gli attacchi informatici ai sistemi di *home-banking* avvengono o perché si ingannano le persone o perché si ingannano i computer delle persone, e quindi normalmente non è il sistema informatico della banca, o comunque che presiede ai servizi di *home-banking*, a essere fallato, ma questo ritengo sia abbastanza ovvio. Se così fosse, infatti, qualunque giudice italiano aprirebbe la strada al risarcimento. Il problema della sicurezza riguarda soprattutto gli utenti ed è a loro che vanno rivolte campagne di formazione, di aumento della sensibilità.

Chi dispone di un conto bancario *on-line*, utilizza carte di credito, deve fare attenzione a che il computer, ad esempio, di cui si serve per queste connessioni sia « protetto ». È chiaro che l'utente normale può contestare dicendo che si tratta di una complicazione, però i vantaggi che derivano dall'utilizzo di un certo tipo di sistema bilanciano enormemente il fastidio di porre maggiore attenzione all'utilizzo di un certo tipo di macchine.

Su questo siamo abbastanza convinti di una cosa: attingo a quella che è stata l'esperienza di poliziotto « di strada » e ricordo che, all'epoca in cui i famosi furti

in appartamento nel periodo estivo erano un flagello su tutti i territori, da alcune statistiche rilevammo in maniera abbastanza semplice che il 50 per cento dei furti, un numero che allarmava, erano determinati da persone che dimenticavano se non proprio la porta di casa aperta, quanto meno la finestra oppure la finestrella per il gatto.

Già adottando queste cautele minime si potrebbe sfrondare quasi di un 50 per cento il fenomeno. I criminali informatici sono molto attenti alla finestrella, al lucernario aperti, per usare termini corrispondenti. Già adottare queste cautele può essere un validissimo deterrente.

La considerazione di fondo è che la linea di utilizzo verso il mondo informatico, l'aiuto che l'informatica può offrirci è tracciata. Purtroppo, ripeto che abbiamo degli enormi vantaggi da queste tecniche e dobbiamo pensare a un loro utilizzo estremamente più consapevole in vista della sicurezza.

PRESIDENTE. Ringrazio il direttore del Servizio di polizia postale e delle comunicazioni, dottor Antonio Apruzzese, per il suo intervento e per la documentazione depositata, di cui autorizzo la pubblicazione in allegato al resoconto stenografico della seduta odierna *(vedi allegato)* e dichiaro conclusa l'audizione.

La seduta termina alle 11,45.

IL CONSIGLIERE CAPO DEL SERVIZIO RESOCONTI
ESTENSORE DEL PROCESSO VERBALE

DOTT. VALENTINO FRANCONI

Licenziato per la stampa
il 25 ottobre 2012.

STABILIMENTI TIPOGRAFICI CARLO COLOMBO

PAGINA BIANCA