PRESIDENZA DEL PRESIDENTE MARIO VALDUCCI

La seduta comincia alle 10,05.

(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 di rappresentanti di Cisco Systems Italy Srl

PRESIDENTE. L'ordine del giorno reca, nell'ambito dell'indagine conoscitiva sulla sicurezza informatica delle reti, l'audizione di rappresentanti di Cisco Systems Italy Srl.

Do la parola al dottor Paolo Campoli per lo svolgimento della relazione.

PAOLO CAMPOLI, *Direttore mercato europeo telecomunicazioni, Cisco Europa*. Buongiorno. Vi ringrazio a nome di Cisco Systems per l'opportunità offerta da quest'audizione.

Vorrei iniziare introducendo il profilo dell'azienda che rappresento in questa sede. Cisco è *leader* mondiale nella fornitura di soluzioni di rete, ossia di soluzioni di connessione di computer voce e video, che mirano a trasformare il modo in cui le persone collaborano, comunicano ed effettuano intrattenimento digitale.

Attualmente abbiamo circa 66.000 dipendenti a livello mondiale, alla chiusura dell'anno fiscale, ossia al luglio del 2012. È un numero che varia, perché la nostra è un'azienda che compie numerose acquisizioni e tende a crescere nel tempo.

Con lo scorso anno fiscale abbiamo registrato 46,1 miliardi di dollari di fatturato a utili crescenti. Peraltro, è una connotazione positiva in un mercato piuttosto difficile.

Cisco ha come obiettivo quello di guidare la transizione verso un nuovo ambiente tecnologico che mantiene al proprio centro la rete. Abbiamo una visione in cui la rete Internet, la rete basata sul cosiddetto protocollo IP, svolge un ruolo di trasformazione sia dei processi *business*, sia del modo in cui le famiglie e i consumatori spendono il loro *budget* per l'intrattenimento, la comunicazione e l'informazione.

A livello italiano l'azienda è stata istituita in Italia nel 1994 ed è attualmente guidata da David Bevilacqua, che è anche *vicepresident* per il mercato sud-europeo, ovvero per Spagna, Portogallo, Grecia, Francia e Italia.

La filiale italiana consta di 700 dipendenti e comprende anche il centro di ricerca a livello mondiale per Cisco per tutto ciò che riguarda la fotonica, le tecnologie ottiche e il cosiddetto *routing* IP. Si tratta di un centro con base a Monza che è un fiore all'occhiello per la Cisco europea, in quanto esporta tecnologia di punta in tutto il resto del mondo.

I temi che sono stati proposti nell'ambito di quest'audizione fanno capo a tre argomenti principali.

Il primo riguarda la sicurezza informatica per quanto attiene all'identità digitale, quindi ai tentativi di furto o alla duplicazione dell'identità digitale.

Il secondo riguarda le reti di comunicazione, sia cablate, sia *wireless*. Guarderemo gli aspetti di sicurezza informatica relativi ai due tipi di rete, fissa e mobile.

Il terzo riguarda il concetto di *cloud computing*, che sta avendo una rilevanza enorme in tutto ciò che facciamo. Se pensiamo oggi a come consumiamo il *software* e le applicazioni che girano sui *tablet*, notiamo che tutto fa riferimento al cosiddetto modello di *cloud computing*. Quindi bisogna accertare quali sono le valenze di sicurezza, di *cyber security*, quando ci si avvale di un modello di fruizione quale il *cloud computing*.

L'idea era quella, in base alle vostre richieste, di trattare questi tre temi. Prima, però, vorrei compiere un piccolo *excursus* sull'evoluzione delle rete.

Cito un dato per tutti. Oggi vi sono 13 miliardi di dispositivi connessi alla rete a livello mondiale, il che significa mediamente due dispositivi per abitante di questo pianeta. Peraltro, la soglia dell'1 a 1 è stata superata già da alcuni anni e oggi siamo in un rapporto di 2 a 1.

Chiaramente non stiamo parlando soltanto di telefoni mobili, di personal computer e di *tablet*, per i quali il numero per persona nei mercati evoluti è piuttosto alto, ma anche di tutti i dispositivi che consentono alle macchine di comunicare tra loro. Abbiamo visto recentemente addirittura l'avvento di elettronica di consumo, con frigoriferi o sensori collegati alla rete che comunicano con i centri di controllo e tra di loro.

La rete ha oggi un ruolo pervasivo dal punto di vista della connettività. Entro il 2020, una data piuttosto dietro l'angolo, prevediamo che ci saranno 50 miliardi di dispositivi a livello mondiale connessi a Internet, con una media di sei dispositivi per persona.

Se guardiamo oggi in una casa e raffrontiamo ciò che vedevamo soltanto alcuni anni fa, vediamo che il numero di dispositivi connessi, se consideriamo *set-top box*, Playstation, *tablet*, è dell'ordine della decina, se non della dozzina e il numero dei 50 miliardi non è neanche troppo futuristico.

L'altro fenomeno a cui accennavo prima riguarda quanto la rete, in particolare quella ad altissima velocità, stia abilitando in maniera sempre più capillare e pervasiva l'utilizzo dei servizi dati nel *cloud*, nella cosiddetta nuvola. Per il prossimo anno, il 2013, le statistiche ci indicano che il 70 per cento delle aziende, in misura diversa tra di loro, a livello mondiale utilizzeranno il modello di fruizione *cloud*.

Ciò significa che il *software*, invece di risiedere su un personal computer, risiederà da qualche parte nella nuvola, in un *data center* distribuito e che, come utente dell'azienda, io potrò utilizzare i processi di produttività e di comunicazione in maniera indipendente dal terminale, attraverso un *tablet*, uno *smartphone* o un personal computer.

Significa anche che il modello di pagamento e di fruizione sarà sempre più basato sul consumo, senza dover acquistare un titolo, ma pagando un canone o una licenza di consumo. Anche questo è un fenomeno essenzialmente guidato dalla rete, con tutti i problemi sia di larghezza di banda, sia di sicurezza che ne connotano oggi l'utilizzo.

Un'ultima discussione che è utile svolgere per quanto riguarda le tendenze è attinente ai paradigmi di sicurezza all'interno delle aziende. Oggi un'azienda come Cisco, ma anche aziende più piccole, fa un utilizzo molto esteso del *social networking*, ossia di piattaforme che consentono ai membri di una comunità di scambiare oggetti, comunicare e interagire in modalità audio-video. È quella che in inglese si chiama *consumerization*, la consumerizzazione della vita aziendale.

Oggi, quando le assumiamo, le nuove generazioni vogliono portare con sé il telefono o lo *smartphone* che utilizzano normalmente. Non accettano di avere un telefono aziendale con applicazioni diverse da quelle che utilizzano di solito. Si tratta del fenomeno che gli inglesi chiamano

bring your own device (BYOD), per il quale diventa molto importante il fatto di poter portare all'interno dell'azienda il proprio *device* e fare in modo che questo dispositivo diventi, nel momento in cui si entra nell'ambito aziendale, un terminale virtuale della rete aziendale con tutte le politiche di sicurezza, di autenticazione e di protezione dei dati che l'azienda si aspetta di realizzare.

Ciò vale sia per i dipendenti, sia, sempre di più, per i *partner*. Ricordiamoci che oggi quello delle aziende è un mondo sempre più collaborativo, in cui questo tipo di accesso deve essere garantito a dipendenti e *partner*.

Quando pensiamo alla rete, essa viene normalmente viene banalizzata come un insieme di connessioni e di circuiti – io li chiamo tubi – per trasportare informazioni. In realtà, la rete ha un ruolo sempre più pervasivo in considerazione del numero di terminali, di *device*, come abbiamo ricordato prima, collegati alla rete stessa e alla quantità di dati pubblici e privati sensibili che vi transitano.

Da questo punto di vista, credo che l'Agenda digitale italiana stia indirizzando i temi più importanti, che sono quello dell'utilizzo dell'*open data* nell'ambito dell'amministrazione pubblica, della banda ultralarga e del modello di fruizione *cloud*. Esiste una cornice regolamentare che indirizza questi aspetti.

Le transizioni che dobbiamo considerare riguardano, però, anche quanto velocemente si modifica la modalità con cui si accede alla rete da terminali mobili, come abbiamo accennato prima, terminali che possono essere dei dipendenti di un'azienda o dei suoi *partner* e che devono essere intrinsecamente resi sicuri, nonché una rapidissima accelerazione dei crimini informatici legati all'utilizzo pervasivo di terminali fissi e mobili e della rete.

Ci sono due modi diversi di vedere la rete. Il primo paradigma è quello di un insieme di circuiti e di strumenti di connettività che consentono di scambiare dati che devono venire protetti ai bordi della rete.

L'altro paradigma è, invece, quello di pensare alla rete come a un elemento fondamentale nella piattaforma di sicurezza, l'unico elemento di intersezione tra il mondo dei terminali fissi e mobili e il mondo della nuvola, del *cloud*. La rete è l'elemento che sta in mezzo e che possiamo arricchire di funzionalità mirate a prevenire o a mitigare i fenomeni di *cybercrime*, ossia di crimine informatico.

Quest'ultimo è il paradigma su cui vorrei riflettere con voi nel contesto di questa consultazione. Abbiamo ricordato velocemente che cosa succede nel mondo delle imprese. Tipicamente, c'è un ufficio centrale, una sede principale, con un dato numero di uffici remoti. Sempre più spesso, per motivi sia di produttività, sia di flessibilità, si offre la possibilità sia ai *partner*, sia ai dipendenti di lavorare da remoto.

Le applicazioni vengono gestite dal responsabile dell'*information technology*, ma risiedono sempre di più in un ambiente eterogeneo, *cloud* o ambiente ibrido, *cloud* e nuvola privata. La rete sta al centro di tutto questo ecosistema e può avere un ruolo di rafforzamento della sicurezza dei dati.

Il modo classico di progettare la sicurezza a livello delle imprese – arriverò poi, invece, alla dimensione dell'utente privato, ma mi soffermo ancora un attimo sul mondo delle imprese – era quello di proteggere in primo luogo i dati presenti sul personal computer o sui *tablet*, la propria base dati, ovunque essa fosse, nella sede principale o in un posto relativamente sicuro, e poi di avere una rete dati di telefonia offerta dall'operatore di telecomunicazioni intrinsecamente sicura. Questo era il paradigma valido fino a tre, quattro o cinque anni fa.

Oggi il paradigma tende a evolvere in un senso diverso. Riconosciamo infatti la mobilità dei dipendenti e l'eterogeneità dei sistemi di accesso, nonché il fatto che i dati risiedano nella nuvola. La rete può compiere fondamentalmente tre operazioni. Può essere resa più robusta intrinsecamente, ragion per cui possiamo avere

una rete intrinsecamente meno vulnerabile agli attacchi esterni. Questo è quasi un dato assunto come base di partenza.

Possiamo avere poi una rete che ispeziona quello che succede alla sua periferia, ai suoi confini, e tenta di correlare gli eventi. Un attacco informatico è un attacco che muta nel tempo. Se ne parlava prima informalmente come di un gioco tra guardie e ladri.

Io ho provato ad aggiornare questa presentazione, dopo che l'audizione era stata posticipata, e a vedere gli attacchi informatici che si sono verificati nelle ultime due settimane. Le modalità, se non radicalmente diverse, sono profondamente cambiate già da un mese fa. Esiste un concetto, di cui parlerò tra poco, di *darknet*, ossia di reti parallele, che sta diventando purtroppo molto diffuso per effettuare transazioni illegali in modo completamente trasparente rispetto alla rete Internet.

Non esiste la formula magica per identificare i problemi di sicurezza e risolverli una volta per tutte. Esiste, invece, il concetto di poter correlare alcuni sintomi, capire che qualcosa di anomalo sta succedendo e iniziare a prevenire e a prendere dei provvedimenti. La rete è l'unico sistema distribuito che collega terminali, *server* e *cloud* che può avere questo tipo di intelligenza residente e può essere in grado di iniziare a correlare sintomi e capire che qualcosa sta succedendo per controllare i dati, assicurare la *privacy* e avere la possibilità di reagire agli attacchi in maniera preventiva.

Non credo di affermare nulla di nuovo svolgendo una piccola rassegna stampa di quanto è successo negli ultimi tre o quattro mesi dal punto di vista della sicurezza informatica, della *cyber security*, dal furto dei dati confidenziali sulla piattaforma Sony, notizia finita sulla stampa, al fatto che ci siano alcune forme di *hackering*, ossia di attacco informatico che hanno forti connotazioni « politiche », mirate ad attaccare specifiche aziende. Sono situazioni che vediamo tutti i giorni, purtroppo, e che tendono a crescere nel tempo, dal punto di vista dell'incidenza.

L'elemento nuovo è dato dagli attacchi del tipo *denial of service*, nei quali, per esempio, una serie di personal computer si mettono d'accordo e attaccano un sito aziendale o un sito pubblico con l'intento di abbatterlo e renderlo indisponibile. Questo genere di attacco può essere addirittura creato *online* da qualsiasi utente.

Se un utente accede al sito JS LOIC, gli viene chiesto qual è il sito *web* che vuole attaccare – non so quale sia la remunerazione per chi svolge questo lavoro, ma immagino che ci sia – e viene invitato ad assistere semplicemente a quello che succede. Nei prossimi dieci minuti il sito in oggetto verrà messo fuori servizio. Si tratta di un'attività che non richiede nemmeno di essere esperti o addetti ai lavori, essendo di estrema facilità di esecuzione. Basta conoscere il punto di accesso dal punto di vista dei siti *web*.

Accennavo prima al concetto di *darknet*. In merito è uscito alcuni mesi fa su *la Repubblica* un bell'articolo di Riccardo Luna che ha svelato un fenomeno che si andava formando e che, purtroppo, sta accelerando notevolmente. Si tratta del concetto di una rete IP, una rete Internet completamente parallela alla rete pubblica, a cui si accede tramite una forma di accreditamento disponibile *online*, che utilizza la nozione di mascherare l'identità dell'utente.

L'utente si collega, dunque, in maniera casuale a diversi punti di accesso virtuale alla rete e non è tracciabile con strumenti canonici. Su questa rete vengono scambiati beni ed effettuate transazioni illegali in maniera completamente trasparente e sovrapposta alla rete pubblica.

Anche in questo caso l'infrastruttura di telecomunicazione può correlare i sintomi e capire che qualcosa sta succedendo perché la rete di telecomunicazioni ha la visibilità del traffico, dell'identità fisica e logica degli utenti e delle relazioni tra le applicazioni.

Parliamo ora delle prime dieci minacce informatiche che stiamo tracciando come azienda. Cisco ha un ruolo molto attivo nel continuare a mantenere aggiornate sia le tecnologie di prevenzione, sia quelle di

gestione degli attacchi informatici e mantiene anche un livello di visibilità sul modo di operare del mercato.

Le prime dieci minacce informatiche sono legate all'attacco sofisticato, ma anche sempre più facile da eseguire, ad alcuni siti *web*; alle cosiddette *botnet*, reti di computer dormienti che, a un dato punto, vengono svegliati e sincronizzati per attaccare determinati siti; allo spionaggio informatico; al *phishing*, un fenomeno che purtroppo si verifica quando effettuiamo commercio elettronico. Si tratta di pagine in cui ci vengono chieste le nostre *username* e *password* col logo della banca o dell'azienda, ma che in realtà sono duplicazioni di pagine reali, mirate a rubare l'identità digitale.

Non vorrei elencare tutte le dieci minacce informatiche, ma si tratta di un mondo in costante evoluzione e con barriere di accesso sempre più basse.

La buona notizia è che, da un lato, esiste un'attività regolamentare a livello sia europeo, sia nazionale, che inquadra il problema e inizia a definire alcune misure sia di consapevolezza di quello che sta succedendo, sia di sviluppo di casistica e di misure di prevenzione; dall'altro c'è un ruolo della rete sempre più attivo nel prevenire questo genere di problemi.

Vorrei portare un esempio che esula dal documento che accompagna la mia relazione, ma che mi è capitato ieri e che mi sembra estremamente rilevante per l'audizione di oggi. Vediamo se riesco a rappresentarlo *on-screen*. La mia *inbox* contiene una *mail* arrivata ieri, che incidentalmente proponeva un *link* che io credevo fosse di una pubblicità. Io mi sbarazzo delle *mail* irrilevanti di prima mattina e poi inizio a lavorare a quelle più serie, come immagino facciamo quasi tutti.

Ho cliccato, dunque, su questo *link* e, mentre ero connesso con una *virtual private network* (VPN) alla mia rete aziendale, la rete mi ha comunicato di prestare attenzione, perché, nonostante la *mail* non fosse stata filtrata – è una *mail* aziendale che è arrivata nella mia *inbox* – c'era qualcosa di anomalo. L'avviso evidenziava che potessi essere guidato verso un sito non sicuro. Questa è una funzione della rete.

Ho provato, dunque, a spegnere la VPN, il circuito logico verso la mia azienda, e ad accedere come un qualsiasi utente Internet allo stesso *link*, finendo su quella che sembrava una pagina pubblicitaria. In realtà, quando ho fatto girare l'antivirus, ho trovato ogni sorta di *malware* su questo PC aziendale. Ho ripulito il tutto e ho scelto di continuare a mantenere la connessione VPN verso la mia *corporate*, perché la rete si autoprotegge.

Questo è un esempio del ruolo della rete che complementa le funzioni di sicurezza e aiuta, grazie a un disegno architetturale che può essere replicato su qualsiasi scala, a mantenere intrinsecamente la sicurezza dei dati ed eliminare buona parte degli attacchi informatici.

L'ENISA a livello europeo è il centro di competenza per la *cyber security* e ha giocato un ruolo estremamente attivo negli ultimi anni dal punto di vista di quella che si chiama l'*advice and recommendation*, cioè la fornitura di raccomandazioni, linee guida, metodi e procedure per prevenire gli attacchi informatici.

Esiste poi la mozione di CyberEurope, una sorta di test di resistenza, un *crash test* come quello che abbiamo effettuato anche con le banche, che viene eseguito ogni anno – credo che l'ultima volta sia stato effettuato nell'ottobre di quest'anno – in cui si verifica a livello europeo, nel caso di un attacco generalizzato, quale potrebbe essere la reazione dei sistemi informatici.

Nel 2013 la Commissione europea ha annunciato che pubblicherà un pacchetto di misure legislative e/o di *policy* atte a rafforzare le linee guida sia preventive, sia di rimedio per quanto riguarda la sicurezza informatica. È un passo avanti rilevante per passare dal modello consultativo a un modello più orientato all'azione. Noi crediamo che a livello europeo sia necessario adottare il concetto di *blueprint* di architettura di riferimento unificata,

che consiste nel compiere non solo educazione, ma anche nell'avere alcune linee guida effettivamente implementabili.

A livello degli Stati membri e, quindi, anche dell'Italia è nato il concetto di CERT, il *Computer Emergency Response Team*, che in Italia, come in tanti altri Stati membri, si è declinato in diverse maniere, a seconda dell'ente istituzionale che ha bisogno di utilizzarlo.

Esistono un CERT per la difesa, uno per le strutture di telecomunicazioni pubbliche, il Centro nazionale anticrimine informatico per la protezione delle infrastrutture critiche della Polizia di Stato. Ognuna di queste entità riveste un ruolo estremamente attivo sia nella prevenzione, sia nella gestione dei crimini informatici.

Noi riteniamo che, a questo punto, visto il ruolo sempre più pervasivo della rete e la necessità di avere uno schema architetturale di riferimento che possa essere replicato, un livello di consolidamento e di deframmentazione possa rappresentare un passo avanti nella direzione giusta per avere un'uniformità di metodi e di procedure attraverso il pubblico e il privato.

Entrando un po' più nello specifico, una volta enfatizzato il ruolo della rete, che cosa possono fare gli operatori di telecomunicazioni sul tema dell'identità digitale ? Sappiamo che molti furti dell'identità digitale sono collegati al fatto che non esiste un'autenticazione forte. Alcuni siti chiedono semplicemente *username* e *password*, altri chiedono credenziali che possono essere piuttosto facilmente duplicate o falsificate.

L'operatore di telecomunicazione ha un *asset* fondamentale nelle proprie mani, il mappaggio tra identità logica (nome e *e-mail)*, e identità fisica, sia essa la linea a larga banda cui l'utente è collegato o la *SIM card* all'interno del suo telefono. Quest'ultimo è un elemento di mappaggio fisico-logico che potrebbe venire esposto verso chi sviluppa applicazioni e rafforzare ogni sistema di autenticazione con una credenziale che di fatto noi ci portiamo appresso in ogni momento della giornata, ossia la *SIM card*.

L'utilizzo del mappaggio fisico-logico che un operatore di telecomunicazioni può esportare può diventare uno strumento per la cosiddetta autenticazione forte e, quindi, rafforzare i sistemi di prevenzione nel furto dell'identità digitale.

Per quanto riguarda la sicurezza nelle reti cablate e nelle reti *wireless*, abbiamo ricordato prima che essa può essere aumentata dalla rete, la quale correla sintomi, capisce ciò che succede ai propri bordi e si rende essa stessa metodo di prevenzione per quanto riguarda gli attacchi informatici.

Le reti devono essere intrinsecamente capaci di reagire a quelli che vengono chiamati *denial of service*, ossia attacchi perpetrati in maniera concertata da personal computer dormienti che vengono attivati e sincronizzati per attaccare alcune funzioni di rete.

Bisogna però, anche e soprattutto assicurarsi che le reti vengano rese robuste rispetto ad abusi nell'utilizzo delle funzioni di intercettazione legale. Ricordiamo che l'intercettazione legale è un modo di duplicare i flussi per fini normalmente leciti. Bisogna assicurarsi che le funzioni di rete siano rese intrinsecamente sicure rispetto all'abuso nell'utilizzo delle funzioni di intercettazione legale.

Abbiamo parlato velocemente prima – non voglio assolutamente addentrarmi in un terreno tecnico in questa sede – di quello che in gergo tecnico si chiama il *blueprint* architetturale, ossia l'insieme di linee guida dell'architettura di riferimento per rendere i sistemi pubblici e privati più sicuri.

Ho tentato di rappresentare in un grafico, contenuto nel documento che accompagna la relazione, che cosa intendiamo noi dal punto di vista un po' più pratico. C'è un insieme di terminali fissi e mobili che afferiscono a una rete tipicamente ad alta velocità per accedere o a Internet o a dati pubblici e privati, aziendali o del consumatore, che risiedono sempre di più all'interno della nuvola.

La rete compie alcune operazioni, in questo caso: analizza quello che succede

dal punto di vista degli eventi, li correla ed eventualmente isola relazioni di traffico e applicazioni che si stanno comportando in maniera anomala. Gioca, quindi un ruolo attivo sia nella prevenzione, sia nell'isolamento degli utenti anomali. A questo punto il paradigma diventa quello della sicurezza intrinseca che aiuta a prevenire intrusioni, a preservare la confidenzialità dei dati e a garantirne la *privacy*.

Ho citato prima un esempio piuttosto banale di come una funzione di rete, che in questo caso è realizzata all'interno di una rete *corporate*, ma che potrebbe venire estesa alla rete nazionale, mi abbia aiutato ieri a prevenire una criticità che non avrei nemmeno individuato immediatamente sul computer e che si sarebbe rivelata probabilmente settimane o mesi dopo. Il sito cui accedevo era completamente uguale a un qualsiasi sito pubblicitario. In questo caso la rete mi ha aiutato e lo schema architetturale di riferimento è quello che ho presentato nel grafico.

Per quanto riguarda il modello *cloud* e la sicurezza di tale modello, noi riteniamo che il documento di strategia della Commissione sia una buona base di partenza. Il documento, pubblicato nel luglio di quest'anno, non definisce le iniziative specifiche nelle aree della sicurezza e della *privacy* per i servizi *cloud*, ma rimanda all'azione normativa più generale in corso da parte della Commissione stessa. Definisce che cos'è il modello *cloud*, qual è il paradigma di funzione e quali sono gli aspetti critici dal punto di vista della sicurezza, ma non legifera in termini di sicurezza specifica per il *cloud*.

Noi riteniamo che questo sia l'approccio corretto, perché si tratta di un mercato nascente. Se la rete è intrinsecamente sicura, se esistono metodi e procedure per rendere sicuro lo scambio dati, il modello di funzione *cloud* eredita questi attributi.

Esiste comunque un tema sulla portabilità e sulla confidenzialità dei dati all'interno del *cloud* che va trattato in maniera dedicata, ma le funzioni di rete per rendere intrinsecamente sicure le transazioni sono trasferibili in base al modello di sicurezza che illustravo prima.

Per concludere, sperando di non aver abusato del vostro tempo e della vostra pazienza, ma ho tentato di gettare uno sguardo sia ai *trend* di mercato, sia ai contenuti più specifici, passo alle raccomandazioni che ci sentiamo di fornire in questa sede.

Secondo noi, bisogna considerare la rete nella sua accezione più ampia, come rete pubblica e privata, non solo come una struttura per trasferire dati e informazioni, un insieme di circuiti o di tubi logici, bensì come la piattaforma centrale per la sicurezza dell'identità dei dati e dell'accesso al *cloud*, che, grazie a funzioni intelligenti, residenti nella rete stessa, può prevenire e individuare intrusioni e proteggere il contenuto dei dati.

È molto importante definire alcune linee guida e un'architettura di riferimento, quello che chiamavo prima *blueprint*, sempre più a livello nazionale, senza entrare nello specifico tecnologico, ma come criteri guida architetturali, per la sicurezza delle reti sia pubbliche, sia private.

Questa potrebbe essere una strategia nazionale di *cyber security* che si articola in una cabina di regia e in un consolidamento delle funzioni di CERT che portano all'adozione di un approccio architetturale unificato.

Per quanto riguarda il *cloud*, le raccomandazioni della Commissione europea sono una buona base di partenza per un primo quadro regolamentare. Dal punto di vista di quello che abbiamo visto succedere anche su altri mercati, riteniamo che sia necessario evitare di legiferare in merito a specifiche soluzioni tecnologiche e, quindi, mantenere una neutralità tecnologica e un'aderenza agli standard internazionali anche quando si guarda a un tema così scottante, che richiede interventi immediati, come quello della sicurezza nelle reti e nella nuvola.

Spero di non avervi confuso troppo con la mia presentazione, tra termini tecnici e concetti più generali, e di aver centrato gli aspetti principali per cui quest'audizione è stata convocata.

Vi ringrazio dell'attenzione e ovviamente sono disponibile per le domande del caso.

PRESIDENTE. Grazie, ingegner Campoli, per la relazione, che penso sia stata molto utile a tutti i componenti della Commissione.

Do la parola ai deputati che intendano intervenire per porre quesiti o formulare osservazioni.

JONNY CROSIO. Ringrazio l'ingegner Campoli per la sua esposizione molto chiara e interessante e gli pongo una domanda.

Partiamo dalla considerazione che noi cerchiamo di avere reti sempre più performanti e di ampliare il sistema di rete, nella consapevolezza che in questi tubi, come li chiama lei, buona parte delle merci che circola sono merci avariate. Questa è la realtà. Se avessimo la stessa situazione sulle nostre strade, mi chiedo che cosa succederebbe.

Credo che questo sia un processo molto difficile da controllare, anzi assolutamente difficile da controllare, ragion per cui viviamo in un paradosso, il che è piuttosto preoccupante.

Vengo al punto. Noi abbiamo tenuto un'audizione con la polizia postale, che su questi tubi e su queste strade è l'istituzione che dovrebbe immediatamente controllare chi trasporta le merci, in particolare le merci avariate. La Polizia postale ci ha rappresentato la difficoltà di poter intervenire in maniera incisiva, perché c'è un buco nel sistema giuridico del Paese, cui bisogna arrivare a trovare una soluzione.

Sono perfettamente d'accordo sul fatto che probabilmente, a seguito di queste considerazioni, quella che viene considerata la *strong authentication* debba essere rafforzata, ma sappiamo benissimo che nel nostro Paese si arriva a creare un meccanismo piuttosto stridente tra la garanzia della *privacy* dell'utente e la necessità di avere queste garanzie di sicurezza.

La domanda che le pongo, da tecnico e operatore quale lei è, è la seguente: è conveniente e opportuno alleggerire la *privacy* sull'utente al fine di raggiungere questo obiettivo ? Qualora il Governo dovesse decidere di prendere questo indirizzo, quale sarebbe la vostra posizione ?

DEBORAH BERGAMINI. Ho trovato molto interessante la vostra presentazione. Vorrei porre due domande. Una è piuttosto irrituale, in realtà, ma, come legislatori, dobbiamo porcela.

A fronte del quadro che voi ci avete presentato e dei grandissimi numeri – mi hanno colpito molto i 13 miliardi di dispositivi connessi alla rete; oggi sono ormai 2,4 miliardi gli utenti della rete, che stanno ovviamente aumentando – a fronte di questo gigantesco sviluppo della rete e della sua utilizzazione e a fronte delle tante minacce informatiche che dobbiamo contrastare, la mia domanda è se siamo o non siamo appesi a un filo. Tutta la grande connettività del mondo può essere spezzata in un momento e con quali rischi ?

Porto un esempio. Il sistema delle transazioni bancarie può essere annichilito in un momento ?

Passo alla seconda domanda. Ogni volta che ci troviamo a intervenire in termini di legiferazione possibile sulla rete, si creano fortissimi anticorpi. La civiltà della rete non ha ancora deciso quale e quanto grande debba essere il perimetro di regolamentazione della rete.

Tra poco a Dubai si terrà un importantissimo incontro sulla *governance* della rete. È in corso un disegno per spostare da ICAM a ITU il Governo della rete.

Vorrei conoscere la vostra posizione in merito. Purtroppo, ancora una volta, l'attenzione dei *media* è piuttosto debole su questo argomento, mentre invece si stanno decidendo questioni di primaria importanza per tutti noi.

PRESIDENTE. Do la parola all'ingegner Campoli per la replica.

PAOLO CAMPOLI, *Direttore mercato europeo telecomunicazioni, Cisco Europa.* Per quanto riguarda la domanda sul bi-

lanciamento tra autenticazione forte e rispetto della *privacy* e quanto questo tipo di tensione possa rappresentare una zavorra per lo sviluppo dell'economia *online*, è un punto assolutamente valido. Il bilancio è un gioco molto raffinato.

Idealmente e anche operativamente noi prevediamo che possa venire sviluppato a livello sia nazionale, sia europeo un piano su quattro o cinque fasi che parta con l'abilitare la rete stessa ad avere più intelligenza per iniziare, come accennavo prima, a correlare sintomi e a capire che c'è qualcosa che, in alcuni casi, non sta andando nella direzione giusta.

Dal punto di vista legislativo questo piano potrà portare ad azioni più specifiche per ogni Stato membro, ma il fatto che la rete stessa sia consapevole di quello che succede è già di per sé un mezzo di dissuasione.

Io l'ho notato anche dal punto di vista dell'esperienza familiare. Sappiamo tutti che i ragazzi tendono a utilizzare e ad abusare del cosiddetto *peer-to-peer*. Nel momento in cui figli e amici hanno capito che c'è un modo per sapere esattamente che relazioni di traffico *peer-to-peer* stanno avvenendo, alcuni hanno considerato che probabilmente fosse il caso di rientrare un poco nei ranghi.

È un aneddoto, ma io credo che abilitare le funzioni di intelligenza di rete, senza per questo entrare nello specifico della transazione e violare la *privacy*, sia un elemento molto importante, un elemento di irrobustimento, ma anche di dissuasione.

Dopodiché, la *strong authentication*, se basata su concetti di credenziali che noi ci portiamo comunque in giro in ogni caso, come la *SIM card*, potrebbe venire accettata in maniera un po' più aperta dai consumatori e dalla base degli utenti.

È chiaro che non bisogna zavorrare lo sviluppo dell'economia su Internet. Abbiamo visto l'impatto che questa ha sia sul prodotto interno lordo, sulla crescita del PIL, sia sulla produttività e sull'inclusione sociale.

Sono d'accordo con lei che si tratta di un bilanciamento molto raffinato. Sviluppare un piano su quattro o cinque fasi partendo dalla rete e traguardando l'autenticazione forte potrebbe essere un approccio.

Per quanto riguarda le altre due domande, siamo appesi a un filo in termini di robustezza della struttura Internet, della struttura IP e di ciò che vi ruota attorno ?

Io ritengo che i *crash test* compiuti dall'ENISA, di cui ho parlato prima, creino un momento di confronto su quanto sia robusta in realtà la rete e su quali siano le misure disponibili per far fronte a eventuali attacchi concertati.

Ricordiamoci che la rete Internet è nata negli anni Sessanta intorno ad ARPANET con un concetto di intelligenza distribuita e che questo aspetto è quello che l'ha sempre « salvata » da malfunzioni di progetto o indotte da attacchi informatici.

Noi siamo forti fautori, dal punto di vista tecnologico, del controllo distribuito nella rete Internet. Ogni tentativo che abbiamo visto in passato di centralizzare, da un punto di vista tecnico, il controllo e l'intelligenza di rete in pochi privilegiati ha esposto la rete stessa a vulnerabilità. Il controllo distribuito è uno dei princìpi guida nel progetto della rete Internet ed è esso stesso un elemento di robustezza.

Credo anche che una maggiore consapevolezza e un dialogo tra esperti a livello di Stati membri possa anticipare molti dei fenomeni che illustravo in questa presentazione.

Quanto allo spostamento del baricentro tra ICAM e ITU, sono d'accordissimo sul fatto che sia un tema di importanza estrema dal punto di vista del futuro dell'Internet e credo che ci sia ancora troppo poca consapevolezza dell'importanza di quello che verrà deciso a Dubai.

La nostra posizione è che Internet, in termini generici, si è autoregolamentata molto bene negli ultimi anni e che, quindi, dobbiamo prestare particolare attenzione a spostamenti repentini del baricentro verso enti che sono stati e che sono tuttora estremamente efficaci nel regolamentare il mondo delle telecomunicazioni. Il bilan-

ciamento che c'è stato fino a oggi tra ITU e ICAM è stato, tutto sommato, salutare per l'industria.

Per rispondere alla sua domanda, dunque, uno spostamento del baricentro repentino non è un'operazione che vediamo necessariamente come positiva.

PRESIDENTE. Ringrazio i rappresentanti di Cisco Systems Italy Srl per essere intervenuti 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 10,45.

IL CONSIGLIERE CAPO DEL SERVIZIO RESOCONTI ESTENSORE DEL PROCESSO VERBALE

DOTT. VALENTINO FRANCONI

Licenziato per la stampa il 13 febbraio 2013.

STABILIMENTI TIPOGRAFICI CARLO COLOMBO

Camera dei Deputati
IX Commissione Trasporti, Poste e Telecomunicazioni
Indagine conoscitiva sulla sicurezza informatica delle reti.

Relatore: Ing. Paolo Campoli
Direttore mercato europeo Telecomunicazioni

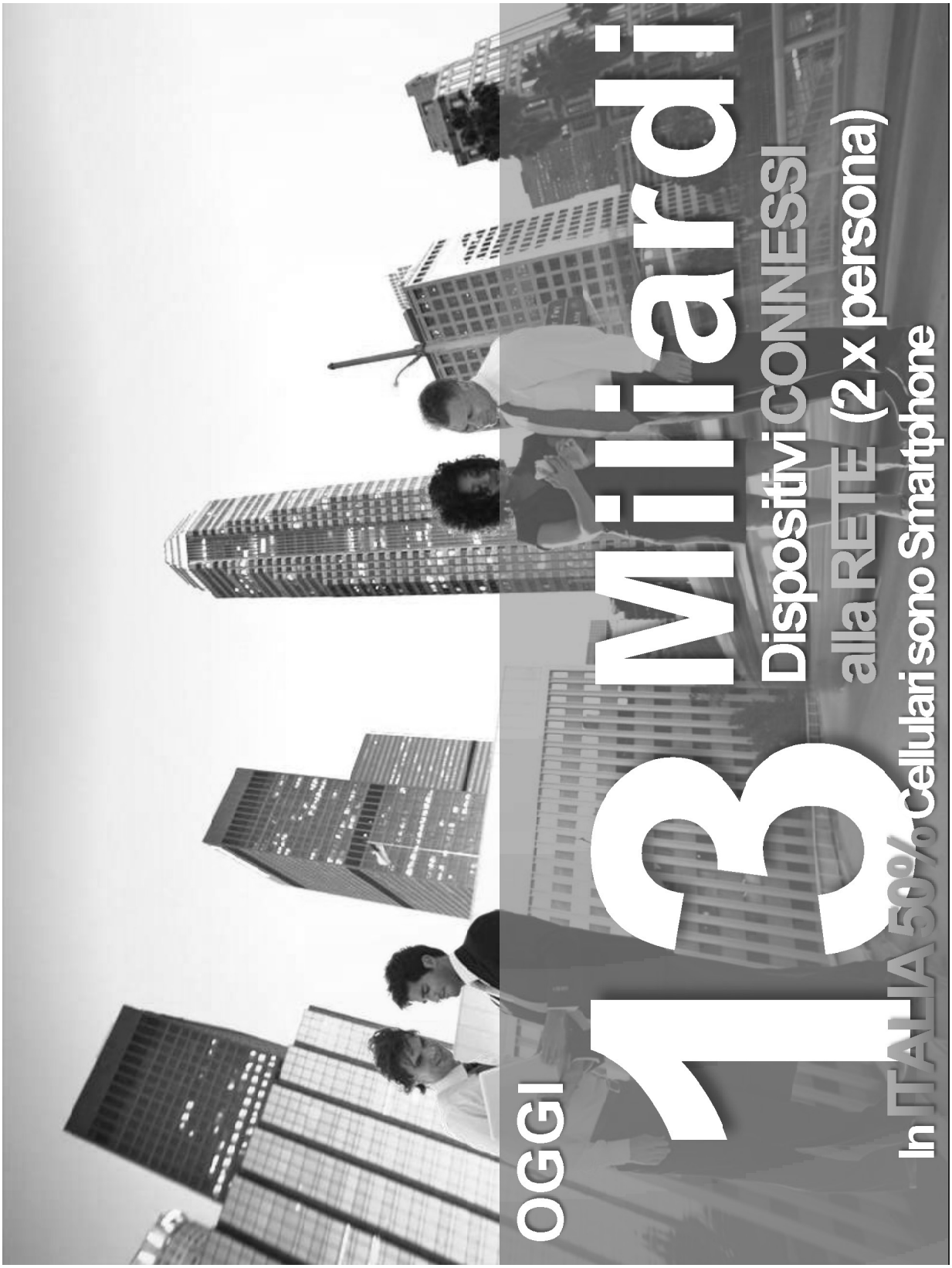
Cisco Systems - Italy

Il profilo di Cisco

- Cisco è leader mondiale nella fornitura di soluzioni di rete che trasformano il modo con cui le persone comunicano e collaborano
- Cisco impiega oltre 66.000 dipendenti nel mondo e nell'anno fiscale 2012 (concluso il 28 luglio 2012) ha registrato un fatturato di 46,1 miliardi di dollari
- Cisco guida la transizione verso un nuovo ambiente tecnologico che ha al centro la Rete IP: una piattaforma di comunicazione intelligente, sicura e convergente
- Cisco è presente in Italia dal 1994 ed è guidata da David Bevilacqua, Vice President, EMEAR South Region di Cisco Systems ed Amministratore Delegato di Cisco Italia. La filiale italiana conta circa 700 dipendenti nella sede principale di Vimercate (MI), a Roma, Torino, Padova e Monza, dove ha sede il laboratorio di Ricerca e Sviluppo sulla fotonica e sul Routing IP che serve tutto il business Cisco a livello mondiale

Sintesi dei temi relativi alla *sicurezza informatica* che la Commissione ha chiesto di affrontare

1. l'identità digitale
2. le reti di telecomunicazione wired e wireless
3. i sistemi distribuiti di servizio e il «Cloud Computing»


OGGI
13 Miliardi
Dispositivi CONNESSI
alla RETE (2 x persona)
In ITALIA 50% Cellulari sono Smartphone