notiziariotecnico

SPECIALE "FUTURE OF INTERNET"

PRIVACY
SECURITY
NUOVE RETI
GOVERNANCE

1/2013

TELECOM ITALIA

TELECOM ITALIA

Caro Lettore,
da oggi il **Notiziario Tecnico** di Telecom Italia è aumentato, cioè arricchito di contenuti speciali interattivi.
Con la nuova APP di Telecom Italia in realtà aumentata, "**L'Editoria+**", che comprende anche l'APP "Editoria", puoi, con un semplice tap sul tuo smartphone non solo visionare videointerviste ad esperti del settore ICT, ma anche ricevere approfondimenti multimediali, consultare photo gallery aggiuntive e comunicare sui principali social network direttamente con gli autori dei vari articoli della rivista.
Per accedere a tutti i contenuti aumentati del Notiziario Tecnico è sufficiente:

1) *scaricare gratuitamente sul tuo smartphone l'APP "L'Editoria+" di Telecom Italia, disponibile su Apple Store, Google Play (Android) e TIM Store*

2) *cercare l'icona del telefonino con l'occhio presente sia sulla copertina del* ***Notiziario Tecnico****, che in molte pagine interne della rivista, come quelle di apertura dei singoli articoli o quelle con le foto degli autori;*

3) *attivare l'APP "**L'Editoria+**" sul proprio smartphone e, tenendo il telefonino a circa 20-30 cm di distanza, inquadrare con la fotocamera l'immagine cartacea di proprio interesse, arricchita dall' icona.*

In questi pochi passi puoi così visualizzare sul tuo smartphone varie icone 3D, che, cliccate singolarmente, ti faranno accedere a un mondo nuovo tutto da esplorare ricco di informazioni aggiuntive, interattive e aggiornate di volta in volta.

Scopri il nuovo **Notiziario Tecnico** di Telecom Italia aumentato!

EDITORIALE

Dal punto di vista tecnologico Internet è solo una suite di protocolli, un'infrastruttura di rete ed una serie di apparati che garantiscono il trasferimento dei dati,ma dal punto di vista sociale ed economico é un fenomeno che sta rivoluzionando il modo di comunicare, di lavorare, di apprendere, di produrre, di socializzare, di fare politica per miliardi di persone.

Una profonda comprensione dei nuovi usi della rete, dei modelli di business e degli scenari competitivi è essenziale per chi, come noi, opera sul mercato della comunicazione ma è altrettanto necessario che i governi e le istituzioni siano consapevoli delle opportunità e anche delle minacce derivanti dallo sviluppo del nuovo ecosistema digitale e che, di conseguenza, vengano ridefinite le politiche industriali e il sistema delle regole in modo coerente con i nuovi scenari.

Mentre i tradizionali servizi di telecomunicazione forniscono una serie di garanzie e tutele che rispondono alle esigenze dei diversi utilizzatori, Internet è intrinsecamente più indifferenziata, più anonima, meno strutturata. Queste caratteristiche di flessibilità, apertura, capacità di adattamento, sono state la chiave del suo successo e devono essere preservate ma in un mondo di comunicazioni sempre più pervasive, Internet dovrà cambiare: il suo impatto nelle relazioni sociali, nell'informazione, negli scambi economici, nei cicli produttivi mette in crisi il paradigma del best effort. Gli usi e gli utilizzatori sono intrinsecamente differenti: uno scambio di mail tra amici non ha nulla a che vedere con la visione di un film in HD o con una transazione finanziaria tra due società. L'Internet del futuro dovrà essere in grado di garantire ciò che oggi gli operatori di reti di telecomunicazioni già garantiscono ed andare oltre. La sicurezza, la privacy, la qualità e la predittibilità delle prestazioni sono elementi di "differenziazione del servizio" assolutamente imprescindibili ai quali gli utenti (cittadini e imprese) non possono essere costretti a rinunciare.

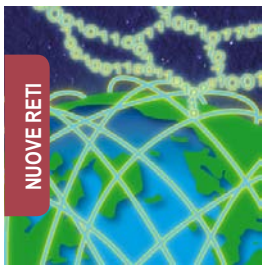
L'Internet del futuro avrà bisogno di reti capillari e performanti e dovrà essere capace di remunerare gli enormi investimenti in infrastrutture fisse e mobili attualmente in corso di realizzazione. Fino ad oggi gli operatori di telecomunicazioni, pur costruendo e gestendo le reti di distribuzione che permettono di accedere ad Internet a centinaia di milioni di persone in tutto il mondo, non sono riusciti a catturarne il valore. Hanno dovuto sostenere ingenti investimenti in infrastrutture d'accesso e nel backbone in uno scenario di prezzi in diminuzione ed ora devono fronteggiare una competizione diretta sui servizi "core" di comunicazione che vengono offerti, molto spesso in forma gratuita e su scala mondiale dai cosiddetti Over The Top. Il rischio è chiaro: gli investimenti in infrastrutture di rete avranno redditività sempre più differita e potrebbero non essere più sostenibili per operatori privati.

In sintesi credo che Internet, intesa come insieme di tecnologie, meccanismi economici, regole, necessiti di una profonda rivisitazione. Telecom Italia vuole contribuire, con gli altri operatori, con i governi, con le istituzioni a determinare il profilo della nuova Internet e, per questo motivo, ci siamo fatti portatori di una serie di iniziative mirate a stimolare il dibattito e a proporre soluzioni concrete.

Questo numero del Notiziario Tecnico è dedicato a questo dibattito e riporta alcune riflessioni dei nostri colleghi più impegnati nei diversi progetti sulle principali criticità del mondo Internet e su possibili ipotesi di soluzione.

Buona Lettura!

Il Presidente Telecom Italia
Franco Bernabè



MOBILE SECURITY: QUALI SFIDE, QUALI PROSPETTIVE

CYBERSECURITY E LOTTA ALLE BOTNET

VERSO UNA NUOVA GOVERNANCE GLOBALE DI INTERNET

SGUARDO AUMENTATO: SCENARI APPLICATIVI

Usa il tuo smartphone per visualizzare approfondimenti multimediali

ALLA RICONQUISTA DELLA NOSTRA IDENTITÀ DIGITALE

Luigi Artusio, Corrado Moiso, Gialuca Zaffiro

l successo dei servizi digitali offerti tramite Internet sta determinando la progressiva migrazione di servizi dal mondo reale "offline" a quello "online". Una delle principali sfide di questo scenario è la realizzazione di meccanismi per la gestione delle identità delle persone, o, più in generale, delle entità che vi interagiscono. Vediamo come.

1 Introduzione

Un'identità digitale è la rappresentazione nel mondo "online" di un'entità, sia essa una persona, un'organizzazione o un dispositivo. In particolare, una persona viene univocamente descritta all'interno di un contesto mediante uno o più elementi informativi, detti attributi. Un particolare tipo di attributo è costituito dagli identificatori (es. gli "username"), che vengono usati quando si accede ad un servizio e permettono di distinguere un'entità all'interno di un particolare dominio. Altri attributi hanno il compito di descrivere le caratteristiche dell'entità, quali, ad esempio, la data di nascita, l'indirizzo, il colore degli occhi, o le sue preferenze. Alcuni di questi attributi, i cosiddetti PII (*Personally Identifiable Information*), permettono di identificare in maniera precisa un utente, associandolo univocamente ad una persona del mondo reale.
La richiesta di essere identificati prima di accedere ad un servizio "online" può essere motivata da svariate esigenze: da quella di potere associare in maniera sicura l'utente ad una persona fisica, a quella di potere mantenere un profilo dell'utente con le sue preferenze e la storia delle sue transazioni passate. Nella maggior parte dei casi ogni fornitore di servizio gestisce in proprio le identità dei suoi utenti/clienti.
Tipicamente prima di potere usare un servizio "online" è necessario registrarsi: la procedura è in genere automatica, ad esempio per ottenere "username" e "password" e per fornire alcuni dati di profilo, ma in altri casi, in cui è necessario un livello di sicurezza maggiore (ad esempio per i servizi di "online banking"), è richiesta una procedura di riconoscimento di persona.
Durante la fase di accesso il fornitore del servizio verifica le credenziali presentate dall'utente.
Il modello di gestione dell'identità digitale descritto ha alcune limitazioni dovute al fatto che porta ad un'esponenziale crescita di registrazioni di credenziali per l'accesso ai servizi; inoltre, i meccanismi di identificazione spesso non sono abbastanza robusti da favorire lo sviluppo di servizi a maggior valore; infine, non vi è una politica comune a livello internazionale nell'utilizzo delle identità digitali.
Stanno emergendo modelli alternativi che prevedono la distinzione dei ruoli di fornitore dei servizi, e di gestore delle identità digitali, nel seguito rispettivamente identificati con i termini di Service Provider ed Identity Provider.

2 Lo status quo

Sul mercato sono presenti innumerevoli organizzazioni pubbliche o private che supportano funzionalità di gestione delle identità digitali nell'ambito della propria offerta di servizi "online". Fra queste, le WebCos, ossia le società che in qualità di Service Provider offrono servizi ed applicazioni sul Web, sono certamente le più attive e meglio posizionate anche nel ruolo di Identity Provider, già disponendo di basi cliente a livello mondiale dell'ordine delle centinaia di milioni (Facebook a fine dicembre 2012 ha raggiunto 1 miliardo di utilizzatori registrati).
Per le WebCos il ruolo di Identity Provider è funzionale al proprio core business, principalmente ba-

sato sulla profilatura degli utenti per finalità pubblicitarie. Le WebCos, essendo nella maggior parte dei casi basate negli Stati Uniti d'America, sono conformi alle leggi ed alle regole di privacy americane, spesso meno stringenti di quelle europee.

Inoltre, il modello economico perseguito dalle WebCos pone le persone in una posizione svantaggiata, in quanto le esclude sia dal controllo della propria identità digitale, che dal flusso economico da essa derivante. Le informazioni ottenute dall'analisi delle identità e delle relative transazioni sono infatti scambiate, spesso dietro pagamento, tra le WebCos e le Terze Parti ad esse interessate. Più in dettaglio, le WebCos offrono, spesso gratis, i loro servizi, richiedendo agli utilizzatori la registrazione ed assegnando loro le relative credenziali di accesso. Sempre più frequentemente altri siti Web, per concedere l'accesso ai loro servizi, accettano tali credenziali, secondo il modello Federated Identity Management (si veda il box "*Federated Identity Management: una prima risposta per ridurre la complessità*"), risparmiando all'utente la noiosa procedura di registrazione ed assegnazione di credenziali specifiche. Ad esempio, il sito di Alitalia consente di accedere ai servizi personalizzati del Club Millemiglia anche usando le credenziali di alcune WebCos (es. Facebook, Google). Questo meccanismo, che apparentemente si presenta come una semplificazione a favore delle persone, nasconde in realtà il modello economico di cui si è accennato prima. Nell'esempio riportato Alitalia, che agisce da Service Provider, utilizza i servizi di gestione delle identità delle altre WebCos (in questo caso agenti da Identity Provider) e, probabilmente, fornisce loro informazioni relative alle transazioni effettuate dalle persone che accedono al sito, senza che le stesse possano decidere diversamente. Questo modello è rappresentato in Figura 1.

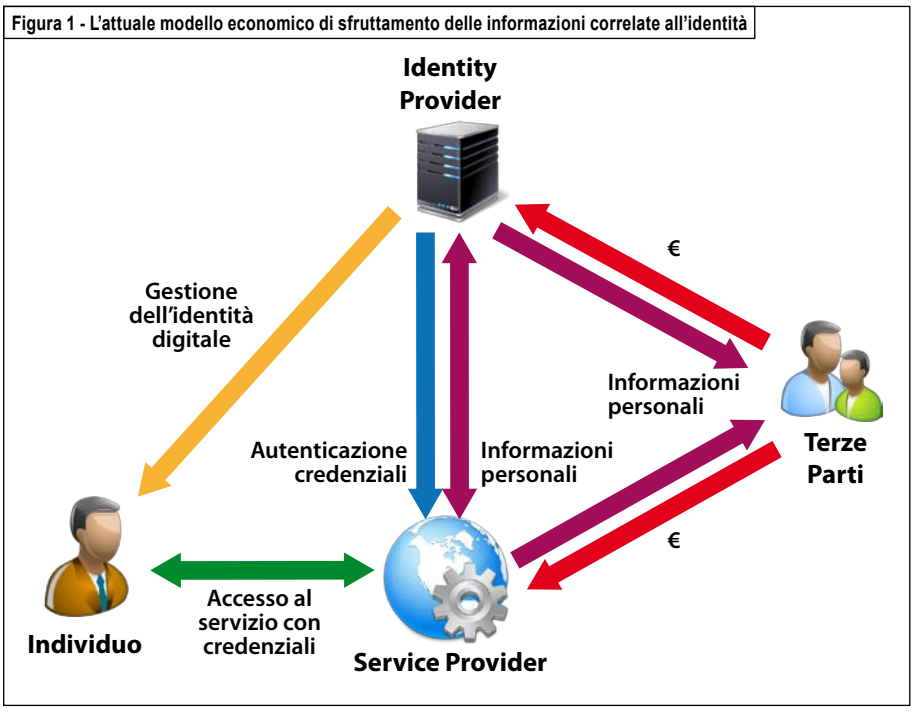
Il meccanismo è tanto appetibile, quanto maggiore è la quantità di informazione personale che si mette a disposizione. Da uno studio condotto da Harvard University [1] i Service Provider sono tanto più disponibili a consentire l'accesso con identità fornite da altri Identity Provider, quanto maggiori sono le informazioni condivise sulle persone che accedono. Nello studio di Harvard si evidenzia come, ad esempio, Facebook trasmetta al Service Provider un insieme molto ampio di dati personali tratti dal "profile" della persona stessa. Questo atteggiamento ha condotto i Service Provider a preferire le credenziali di Facebook rispetto a quelle di Google, dato che quest'ultima limita notevolmente la condivisione di informazioni personali. Conseguentemente Facebook, sempre secondo tale studio, è stata preferita dal 35% dei siti Top 300, contro il solo 11% di Google.

Le istituzioni finanziarie (banche e società di carte di pagamento) potrebbero, in modo del tutto naturale, agire da Identity Provider all'interno di ecosistemi di identità federata per almeno due ottime ragioni: la prima è che, proprio per la natura del loro business, esse utilizzano metodi e strumenti ad alta affidabilità per la gestione dei conti "online"; la seconda, invece, è relativa al fatto che l'opinione pubblica attribuisce a dette istituzioni un elevato livello di fiducia.

Detto ciò, al momento esistono ancora alcune barriere da superare, affinché queste istituzioni entrino in campo, prima fra tutte la definizione di un più innovativo quadro giuridico che regoli chiaramente le responsabilità e le relative assunzioni di rischio nei casi di atti od eventi illegali riguardanti le identità digitali gestite.

Su questo fronte vi sono alcuni primi casi di istituzioni finanzia-

Figura 1 - L'attuale modello economico di sfruttamento delle informazioni correlate all'identità



rie che agiscono come Identity Provider all'interno di ecosistemi specifici come, ad esempio, quello di e-commerce di eBay e Paypal [2], oppure quello di eGov in Canada [3].
Gli operatori di telecomunicazione, dal canto loro, possiedono asset distintivi per la creazione di potenziali nuove fonti di ricavi provenienti dall'impiego e/o dall'offerta di funzionalità di gestione delle identità [4]. Gli operatori dispongono, infatti, di abilitatori tecnologici formidabili sia nelle reti di telecomunicazione, sia nei terminali mobili che, in questo contesto, diventano potenti strumenti di autenticazione. Il ruolo di Identity Provider può risultare naturale per gli operatori, considerando che essi già dispongono e trattano un gran numero di dati personali, relativi all'identificazione ed all'autenticazione dei propri clienti.
NTT Docomo, Deutsche Telecom e Movistar, ad esempio, impiegano le funzionalità di gestione delle identità per la profilatura dei propri clienti finalizzata alla personalizzazione dei servizi. Vi sono, inoltre, alcuni operatori quali AT&T [5] e Verizon [4] che hanno iniziato a vendere servizi IDaaS (*Identity as a Service*) e soluzioni di gestione dell'identità in promettenti settori come sanità e pubblica amministrazione.
Recentemente si stanno affacciando sul mercato aziende che forniscono unicamente servizi o soluzioni di gestione dell'identità e che prevalentemente si orientano al mercato "affari". Nella maggior parte dei casi si tratta di piccole aziende o di start-up, supportate da società di venture capital, con fatturati ancora modesti. Esse adottano approcci differenti per la gestione delle identità, da quello "organization-centric" con la tipica finalità della profilatura degli utilizzatori finali (es. Gigya [6]) a quello "user-centric" focalizzato sulla protezione della privacy e sulla sicurezza degli utenti (es. OneID) [7].
Per completare il panorama è utile considerare anche il mondo delle comunità P2P (es. eMule, BitTorrent, Diaspora). La gestione dell'identità è presente nei servizi P2P al fine di bilanciare al meglio due esigenze contrapposte: la protezione della privacy, fino all'anonimato, particolarmente sentito in contesti spesso ai confini della legalità (ad esempio per il rispetto del Diritto d'Autore), e la garanzia dell'affidabilità di un "peer" partecipante alla comunità [8].
In generale, i "peer" si identificano alla rete P2P mediante uno pseudonimo, eventualmente generato implicitamente dal computer; al fine però di alzare il livello di affidabilità della rete P2P è necessario potere associare in maniera sicura dei parametri ai partecipanti, ovvero agli pseudonimi con cui questi si presentano; tali parametri servono per

Federated Identity Management: una prima risposta per ridurre la complessità

Uno dei principali ostacoli al pieno sviluppo di Internet e dei suoi servizi consiste nel consolidato approccio verticale alla gestione delle credenziali di accesso, che ha rapidamente generato i problemi della proliferazione e della conseguente scarsa gestibilità di dette credenziali.
Per mitigare questo fenomeno, organizzazioni pubbliche e private hanno definito un modello, identificato con il termine FIM (*Federated Identity Management*), che consente di utilizzare le identità in domini multipli. In pratica, sulla base di un insieme comune di regole, protocolli e procedure, il FIM fornisce un modo per condividere le informazioni di identità di una entità (credenziali ed attributi), consentendo alla medesima l'accesso a servizi appartenenti a domini differenti a seguito di un'unica autenticazione (single sign-on).
Sebbene l'interoperabilità inter-dominio delle identità digitali sia un concetto ampiamente condiviso, l'applicazione di soluzioni FIM ha sinora avuto alterne fortune [1]; nei casi di successo si osserva che tutte le parti coinvolte hanno ottenuto un'equa distribuzione dei benefici sui seguenti aspetti:

- adeguata condivisione fra Identity Provider e Service Provider dei dati transazionali degli individui;
- appropriato livello di autenticazione in relazione sia alle esigenze di semplicità d'uso, sia ai requisiti di sicurezza necessari;
- giusta suddivisione delle responsabilità nei casi di malfunzionamenti o frodi.

Per evitare il commercio incontrollato delle informazioni personali all'interno di un ecosistema FIM è necessario che tutti i partecipanti si attengano fedelmente ad un insieme di regole chiare ed obbligatorie, che stabiliscono come dette informazioni possono essere utilizzate nel rispetto dei principi di privacy e sicurezza. Questo insieme di regole viene identificato con il termine "Identity Framework" e tiene conto di tutti gli aspetti, siano essi economici, legali o sociali [10] [11] ■

fornire informazioni sulla affidabilità del "peer" (ad esempio rispetto alla qualità dei contenuti forniti) e per misurare il livello di cooperazione nella rete per evitare il fenomeno del "free riding". Per soddisfare entrambi i requisiti, sono state elaborate numerose soluzioni, in generale distribuite onde evitare di creare "autorità centralizzate" per la gestione delle identità, nelle quali, molto spesso, il partecipante risulta essere l'Identity Provider di se stesso [9].
Come si può notare questo fenomeno si colloca all'estremo opposto dell'approccio di gestione delle identità attuato dalle WebCos.

3 Spinte per il cambiamento

L'evoluzione del modello di gestione dell'Identità trae spunto principalmente da due fattori: uno legato alla dimensione economica e l'altro generato dalle crescenti esigenze di privacy delle persone.
Secondo il governo americano l'evoluzione verso una Internet affidabile è la chiave per aumentare il commercio elettronico ed il fatturato del mondo digitale. Oggi l'impatto delle frodi "online" e dei furti di identità causa notevoli danni sia alle aziende che ai cittadini. Oltre a combattere il fenomeno citato è ritenuto importante aumentare il livello di qualità dei dati disponibili su Internet in termini di tracciabilità ed affidabilità.
Un'altra motivazione forte risiede nella digitalizzazione dei servizi della pubblica amministrazione (eGov) attraverso strategie di gestione dell'identità dei cittadini, così da stimolare, grazie ad una rinforzata sicurezza cibernetica, l'innovazione dei servizi elettronici sia pubblici che privati. Questa strategia si articola attraverso l'introduzione di documenti di riconoscimento digitali, della certificazione delle e-mail, delle cartelle digitali per la salute o per lo studio, e nello sforzo di costruire uno standard cross-nazionale.
Dal punto di vista degli individui, la crescente attenzione per la privacy nel trattamento di dati personali su Internet, emergente soprattutto in Europa [12], coinvolge anche la gestione dell'identità digitale. Tra i requisiti "user-centric" più interessanti si segnalano:

- possibilità per una persona di scegliere l'Identity Provider da utilizzare per accedere ai servizi "online"; i Service Provider devono essere aperti ad accettare le credenziali fornite da differenti Identity Provider;
- flessibilità nella selezione della modalità di identificazione in base al contesto ed al livello di sicurezza richiesto dal servizio a cui si vuole accedere, secondo un ampio spettro di identità (si veda riquadro);
- possibilità di negoziare con l'Identity Provider le regole con cui i dati relativi alla propria identità e al suo uso sono raccolti ed utilizzati o sono dischiusi ai Service Provider;
- possibilità di accedere ai servizi fornendo la minima quantità di informazioni necessarie, ad esempio, presentando la certificazione di certi requisiti (es. la maggiore età) pur rimanendo anonimi.

Infine è importante che, così come oggi è possibile mantenere il proprio numero di cellulare passando da un operatore ad un altro, anche la portabilità dell'identità sia garantita, compreso il diritto alla totale cancellazione dei propri dati dai sistemi degli Identity Provider.

4 Iniziative a livello governativo

Le istituzioni governative nazionali hanno un ruolo fondamentale sia nell'indirizzamento delle strategie di gestione delle identità digitali, sia nella messa in pratica delle medesime. Basti pensare che le istituzioni statali sono da sempre le fonti primarie delle credenziali più forti relative agli attributi di identità degli individui (es. nome, data di nascita, cittadinanza, stato civile). Inoltre, le istituzioni governative hanno intrinsecamente le potenzialità per generare una massa critica di individui equipaggiati ed in grado di utilizzare credenziali digitali con livelli di sicurezza elevati per l'accesso a servizi "online" di valore rilevante [13].
Appare evidente quanto sia essenziale identificare una chiara strategia nazionale per la gestione delle identità digitali per potere ulteriormente sviluppare Internet e l'economia da essa abilitata. Le istituzioni riconoscono che, per sfruttare appieno le potenzialità di Internet sia in termini sociali che economici, è fondamentale garantire alla medesima livelli di sicurezza e di privacy paragonabili a quelli in essere nel mondo reale: solo in questo modo sarà possibile proseguire nel processo di rinnovamento sociale e culturale della popolazione e nella completa migrazione dei servizi "offline" nel mondo "online".
Un altro elemento caratterizzante le strategie governative in questo ambito è la semplificazione della fruizione dei servizi "online": in

particolare è considerato determinante ridurre o limitare il numero delle credenziali digitali che ciascun individuo deve obbligatoriamente utilizzare per accedere ai servizi pubblici e privati, fermo restando il diritto inalienabile della persona di dotarsi del numero di credenziali desiderato.
I governi nel definire dette strategie devono considerare attentamente la storia, la cultura e le usanze governative tipiche dei loro paesi per massimizzare le probabilità di successo delle iniziative conseguenti. Vi sono, infatti, esempi di fallimenti dovuti a scelte di gestione delle identità digitali in contrasto con gli usi e costumi dei paesi e dei relativi popoli.
Negli Stati Uniti d'America, il governo federale ha definito la NSTIC (*National Strategy for Trusted Identities in Cyberspace*), il cui fine ultimo è quello di incrementare il livello di affidabilità associato alle identità delle entità coinvolte nelle transazioni "online". Concretamente, l'applicazione di NSTIC conduce alla realizzazione di un ecosistema di identità federate, ossia di un ambiente "online" ove gli individui e le organizzazioni possono fidarsi reciprocamente, perché tutti hanno accettato e seguono un comune insieme di regole, procedure e standard per l'ottenimento e l'autenticazione delle identità digitali. L'ecosistema è progettato per supportare transazioni sicure con uno spettro di livelli di identità che può variare da "anonimo" a "totalmente verificato" [14].
Nel Regno Unito l'ente governativo "Government Digital Service" ha definito il programma IDA (*Identity Assurance Programme)* avente l'obiettivo di consentire ai cittadini inglesi di accedere ai

Lo spettro delle identità digitali

Nel mondo reale le persone si presentano in modi differenti secondo le specifiche occasioni. Quando attraversano una frontiera devono mostrare il passaporto, ma se si recano in ufficio utilizzano il badge, mentre per il giornale al giornalaio è sufficiente vedere i soldi. La stessa flessibilità dovrebbe essere garantita quando si accede ai servizi "online".
Un vero e proprio spettro di identità può essere definito, come, ad esempio quello proposto da K. Hamlin [18]:

- *Anonimato*: tutte le volte che accede ad un servizio la persona utilizza un identificatore differente (solitamente generato in maniera implicita). Il Service Provider non è in grado di correlare le diverse transazioni e non riesce a raccogliere informazioni sull'utente;
- *Pseudonimo*: l'individuo usa un identificatore differente per ogni servizio o gruppi di servizi. Il Service Provider può creare una "storia" delle interazioni ed associare all'identificatore un profilo; se l'utente non fornisce volontariamente al servizio delle PII il servizio non è in grado di associare l'identificatore ad una persona reale;
- Identità autocertificate: per accedere ad un servizio l'utente crea un profilo fornendo anche delle PII, le quali però sono auto-certificate, senza garanzia che corrispondano al vero;
- *Identità socialmente validate*: sono una estensione della modalità precedente in cui però l'affidabilità dei profili autocertificati viene aumentata, inserendo tali profili all'interno di una rete sociale i cui partecipanti possono garantire reciprocamente la correttezza delle informazioni inserite nei singoli profili;
- *Anonimato verificato*: una persona accede ad un servizio in modalità anonima o con uno pseudonimo, ma fornendo anche degli attributi (ad esempio, l'età) validati da una terza parte; il Service Provider non è in grado di associare l'utente ad una persona reale, ma è sicuro che l'utente che accede è in possesso dei requisiti richiesti (ad esempio la maggiore età nel caso di siti di giochi d'azzardo);
- *Identità verificata*: la persona accede ad un servizio mediante un identificatore a cui sono associati delle PII verificate dall'Identity Provider.

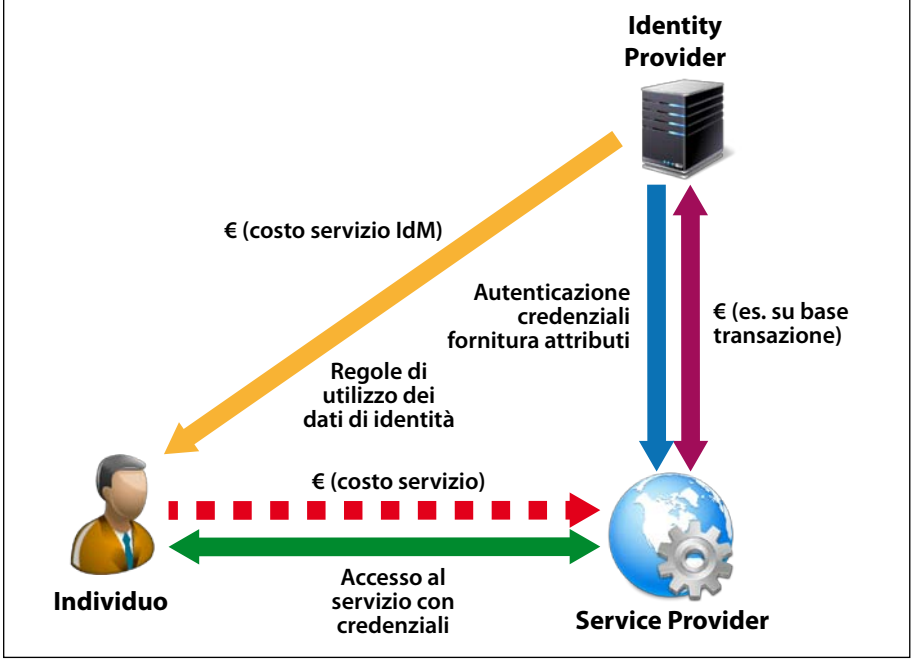
Da parte loro i Service Provider possono richiedere determinate modalità di identificazione, secondo il livello di sicurezza richiesto. Una persona può accedere ad un blog mediante uno pseudonimo, ma ha bisogno di una identità validata nel caso in cui debba richiedere un permesso di caccia su un sito di eGov.
Come si può notare lo spettro di possibili modalità di identificazione offre un'ampia scelta di opzioni di bilanciamento tra privacy e sicurezza, al fine di fornire garanzie sia alle persone sia ai fornitori di servizi, in conformità ai requisiti descritti in Sez. 3.
Le diverse modalità richiedono tecnologie differenti, che vanno dai protocolli di identità federata quali OpenID, o SAML [19], alle soluzioni di credenziali digitali [20] utilizzabili per l'anonimato verificato o per garantire livelli di sicurezza maggiori nel caso di utilizzo di pseudonimi ■

servizi governativi mediante credenziali già rilasciate loro da un ampio gruppo di organizzazioni non governative. Gli aspetti caratterizzanti il programma inglese sono l'assenza di infrastrutture IT a carico del governo e l'approccio "user-centric", che si concretizza nella libertà del cittadino nello scegliere le credenziali di identità preferite. La prima applicazione del programma avverrà nel 2013 e permetterà l'accesso ai servizi del "Department for Work and Pensions" mediante l'utilizzo di credenziali rilasciate da circa una decina di organizzazioni private (es. The Post Office, Mydex, Verizon, PayPal) [15].
Vi sono, inoltre, molteplici iniziative governative tese alla creazione di carte d'identità digitali sostitutive di quelle tradizionali; il processo attuativo richiede lassi temporali di media / lunga durata e l'esito non è sempre scontato: vi sono casi positivi (es. Germania, Spagna) [16], ma anche esperienze negative dovute ad aspetti culturali (es. Australia) o legislativi (es. Francia) [17].

5 Il valore dell'identità personale

Come è stato descritto, il modello attualmente più utilizzato per trarre valore dell'identità digitale è quello adottato dalle WebCos, le quali, accanto alla fornitura dei loro servizi, hanno iniziato ad offrire anche prestazioni di FIM. Dal punto di vista dei siti federati, questo modello permette di accrescere la conoscenza dei propri clienti grazie alle informazioni di profilo che possono essere fornite dagli Identity Provider così da potere realizzare delle offerte personalizzate. Inoltre, facilita l'acquisizione di nuovi clienti: infatti, soprattutto i siti di e-commerce, riducono il numero di "abbandoni di carrello" [21] nel momento in cui si richiede ai clienti di creare il proprio profilo.
Questo modello non è in grado di rispondere agli orientamenti evolutivi emergenti per le identità digitali: maggiore sicurezza e privacy richieste dalle organizzazioni e dalle persone. Infatti, la modalità con cui vengono creati nuovi account legati ai servizi delle WebCos non offrono adeguati livelli di affidabilità nell'associare un profilo ad una persona reale: in genere è adottato un approccio di auto-certificazione nell'acquisire i dati relativi all'utente, mentre i meccanismi di validazione sociale utilizzati devono essere potenziati con algoritmi di "reputation" per evitare auto-conferme "reciproche". Inoltre, le persone hanno poco controllo su come i loro profili e le informazioni sulle transazioni eseguite siano gestite da parte delle WebCos.
L'esigenza di livelli maggiori di sicurezza e privacy richiedono pertanto di riconsiderare il modo con cui è trattata l'identità personale nel mondo digitale: non più come semplice meccanismo di "single sign-on", ma come un mezzo per abilitare scenari applicativi di maggiore valore sia per le organizzazioni (pubbliche o private) che per gli individui.
Adottando tale rivisitazione delle identità digitali, le prestazioni necessarie per il loro trattamento possono essere valorizzate in termini di servizi offribili sia agli individui che alle organizzazioni.
Gli individui riscontrano valore nell'adozione del modello "user-centric" che consente loro di aumentare il controllo sulle loro identità digitali e su come queste vengono "usate" nel mondo "online". Per le persone è essenziale ridurre al minimo i furti di identità, per evitare che qualcuno si presenti ad un sito al posto loro, soprattutto nel caso di servizi ad alto valore, come quelli relativi

Figura 2 – Un possibile modello economico "user-centric" per la gestione delle identità



a transazioni economiche o a richieste a siti di eGov. Inoltre, le persone devono essere in grado di "presentarsi" ad un sito rivelando solamente le informazioni strettamente necessarie ad espletare una specifica transazione. Infine, gli Identity Provider devono permettere ai loro clienti di controllare il trattamento delle informazioni raccolte durante la realizzazione di una transazione.
Per le organizzazioni risulta essenziale avere informazioni certe e sicure relative agli utenti che accedono ai loro siti "online", in modo tale da potere offrire nuovi servizi di valore, possibilmente replicando o spostando quelli offerti nel mondo "offline". Da un lato queste soluzioni permettono loro di aumentare le opportunità di business, possibilmente riducendo i costi operativi, e dall'altro di limitare le perdite dovute a frodi, riducendo al minimo gli investimenti necessari.
La realizzazione di tali scenari richiede la presenza di Identity Provider "user-centric" in grado di offrire servizi per la gestione delle identità alle persone che desiderano operare nel mondo "online" con una elevata attenzione agli aspetti di privacy e di sicurezza (si veda la Figura 2). È essenziale però trovare modelli di business che portino vantaggi a tutti gli attori coinvolti, individui, Service Provider ed Identity Provider [1].

6 Sinergie fra il modello di gestione dell'identità "user-centric" ed il Personal Data Store

L'identità digitale di una persona non si limita solo ad un insieme di identificatori, ma è un insieme di informazioni, gli attributi, che la caratterizzano.
In una prospettiva più ampia si potrebbe pensare che all'identità digitale di una persona possa essere associata la sua "impronta digitale", ovvero l'insieme dei "record" digitali che ognuno di noi produce (direttamente o indirettamente, consapevolmente o inconsapevolmente) mentre interagisce con i servizi "online" oppure opera nel mondo reale. Esempi di tali record sono i log delle chiamate fatte o ricevute, le ricevute dei pagamenti effettuati, la descrizione dei consumi elettrici, le fotografie scattate, le misurazioni fatte dai sensori integrati nei dispositivi elettronici oppure disseminati nell'ambiente.
Come è stato descritto in [22], al momento queste impronte digitali sono memorizzate in maniera sparsa nei sistemi informativi di una miriade di organizzazioni, le quali le usano secondo le loro necessità ed i loro scopi, con un limitato coinvolgimento da parte delle persone. Al fine di superare questi limiti sta emergendo la proposta di adottare un nuovo paradigma per permettere agli individui di riacquistare il controllo sui "loro" dati personali. Tale paradigma può essere concretizzato mediante la realizzazione di servizi di PDS (*Personal Data Store*), tramite cui le persone possono controllare la raccolta, la memorizzazione, la gestione, l'utilizzo e la condivisione dei loro dati personali; in questo modo una persona può sfruttare i propri dati secondo il proprio volere e bisogno, così da trarne benefici personali o economici, nonché valorizzarli a vantaggio della collettività.
I servizi di PDS hanno una stretta relazione con quelli di gestione dell'identità. Infatti, la condivisione sicura dei dati richiede l'identificazione di chi accede e di chi espone i dati. Inoltre, l'impronta digitale può diventare parte integrante dell'identità digitale di una persona, permettendo così di offrire ai Service Provider una descrizione più completa dei loro utenti. Infine, il PDS, con le sue prestazioni di controllo dell'accesso ai dati personali, abilita intrinsecamente la gestione "user-centric" delle informazioni di identità.
Pertanto si può affermare che la gestione delle identità digitali ed il PDS sono due aspetti complementari associati allo stesso obiettivo, cioè garantire agli individui un migliore bilanciamento tra protezione della loro privacy e valorizzazione delle loro identità digitali.

Conclusioni

Riassumendo gli aspetti sinora trattati, se da un lato il mercato delle identità digitali risulta attualmente saldamente in mano alle WebCos, dall'altro è evidente la necessità di cambiamento dettata dai bisogni di maggior affidabilità, privacy e sicurezza espressi dagli individui e dalle autorità governative. Non a caso, seppure con un approccio "estremo", sono nate le comunità P2P aventi l'obiettivo di garantire una mutua anonimità fra i partecipanti senza venir meno alle esigenze di affidabilità.
Può esserci una "terza via"? Probabilmente sì, ma deve rompere gli attuali equilibri di forza, proponendo la centralità dell'individuo come elemento di dirompenza. In questo modello "user-centric" l'individuo possiede molteplici identità, può sceglierne i fornitori e concordare con essi le regole di

utilizzo. Ciascuna persona, come nella vita reale, può decidere quale identità utilizzare a seconda del contesto e della necessità di privacy e di sicurezza, sfruttando lo spettro disponibile, da "anonimo" a "verificato". L'identità personale diventa dunque di proprietà dell'individuo che acquisisce anche i diritti di trasferirla ad un nuovo gestore, unitamente ai dati personali ad essa associati, e di richiederne la totale rimozione a quello abbandonato (si veda la Figura 3).

Un operatore di telecomunicazioni, quale Telecom Italia, potrebbe proporsi nel ruolo di fornitore di identità personali secondo questo modello "user-centric", contrastando il monopolio economico esistente e facendo leva su alcune potenzialità quali l'ampia base clienti e la disponibilità dei relativi dati di identità, la fiducia riconosciuta dai consumatori, l'allineamento alle regole europee sugli aspetti di privacy e sicurezza, l'infrastruttura di rete ed i dispositivi, nonché la vocazione all'offerta di servizi per la collettività.

E se, poi, Telecom Italia si proponesse anche con il ruolo di fornitore di servizi di Personal Data Store, potrebbe porsi sul mercato con un'offerta innovativa e dirompente, in grado di generare nuovo valore ed, al tempo stesso, rispettosa e tutelante i diritti degli individui ■

Bibliografia

[1] S. Landau, T. Moore, "*Economic tussles in federated identity management*", in Proc. 10th Workshop on the Economics of Information Security, (giugno 2011)

[2] PayPal, "PayPal Access", *https://www.x.com/developers/paypal/products/paypal-access*

[3] SecureKey Technologies, "*SecureKey Concierge*", *http://securekeyconcierge.com/sign-in-partners/*

[4] Ovum, "*Telco opportunity: become trusted identity brokers*", (aprile 2012)

[5] AT&T, "*Healthcare Community Online: Enabling Greater Access with Stronger Security*", (2011)

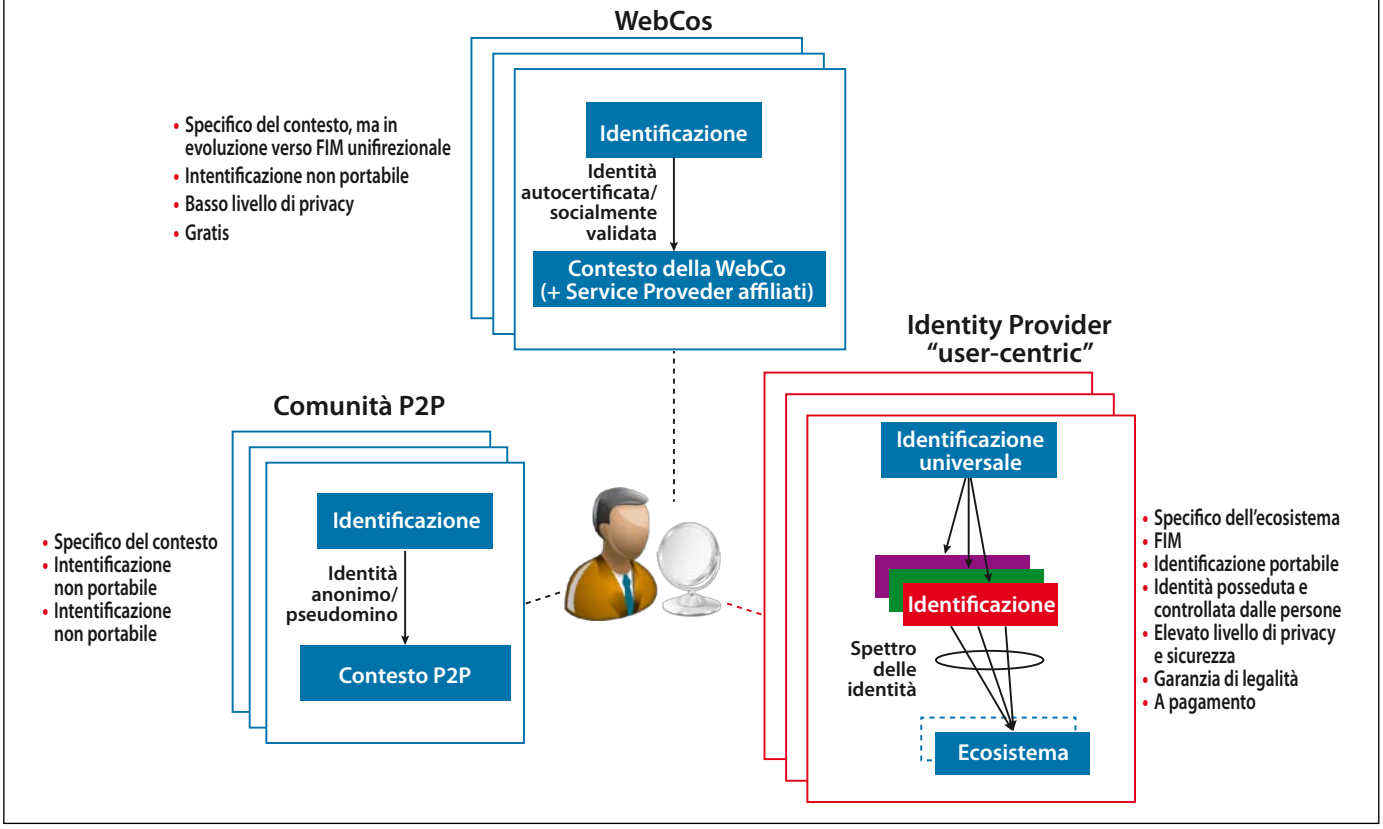
[6] Gigya, *http://www.gigya.com/*

[7] OneID, *http://www.oneid.com/*

[8] Wikipedia, "*Anonymous P2P*", *http://en.wikipedia.org/wiki/Anonymous_P2P*

[9] R.Y. Xiao, "*Survey on anonymity in unstructured peer-to-peer systems*", in Journal of Computer Science and Technology, vol. 23, n. 4, 660-671 (luglio 2008)

Figura 3 – La "terza via": l'Identity Provider "user-centric"



[10] Identity Finder, "*NSTIC's effect on privacy*", (aprile 2011)
[11] Kantara Initiative, "*Identity Assurance Framework*", (aprile 2010)
[12] European Commission, "*Reform of data protection legislation*", (gennaio 2012)
[13] OECD, "*Digital Identity Management - Enabling Innovation and Trust in the Internet Economy*", (2011)
[14] The White House, "*National Strategy for Trusted Identities in Cyberspace (NSTIC)*", (aprile 2011)
[15] Cabinet Office, "*Identity Assurance*", *http://digital.cabinetoffice.gov.uk/category/id-assurance/*
[16] OECD, "*National Strategies and Policies for Digital Identity Management in OECD Countries*", OECD Digital Economy Papers, n. 177 (marzo 2011)
[17] A. Daly, "*A Time Bomb For Civil Liberties: France Adopts a New Biometric ID Card*", *https://www.eff.org/deeplinks/2012/03/french-national-assembly-proposes-new-alarming-biometrics-bill* (marzo 2012)
[18] K. Hamlin, "*The Identity Spectrum*", *http://www.identitywoman.net/the-identity-spectrum* (maggio 2010)
[19] T. Miyata, et alii, "*A Survey on Identity Management Protocols and Standards*", IEICE Transactions on Information and Systems, vol. E89-D, n.1,112-123 (gennaio 2006)
[20] IBM, "*Identity Mixer - Anonymous credentials for strong accountability and privacy*", *http://idemix.wordpress.com/*
[21] OneID, *https://www.oneid.com/for-business*
[22] C. Moiso, "*I dati personali: come trasformarli nell'energia per il mondo digitale*", in Notiziario Tecnico di Telecom Italia, n. 3/2011, 6-19 (dicembre 2011)

luigi.artusio@telecomitalia.it
corrado.moiso@telecomitalia.it
gianluca.zaffiro@telecomitalia.it

Luigi Artusio
dottore in Scienze dell'Informazione, dal 1989 è in Azienda. Nei primi anni ha approfondito gli aspetti di gestione delle reti e dei servizi di telecomunicazione, operando sia negli enti standardizzazione, sia nei progetti di ingegnerizzazione dei sistemi di gestione, assumendo diversi ruoli di responsabilità. Ha sviluppato esperienze di programm and vendor management, contribuendo alla messa in esercizio di soluzioni innovative di rete, come quella di Voice over IP "Alice voce", oltre che di gestione. Attualmente, opera nel gruppo Strategy ove è incaricato di individuare i trend evolutivi del mercato ICT e di intercettare nuove possibili opportunità economiche per il Gruppo.

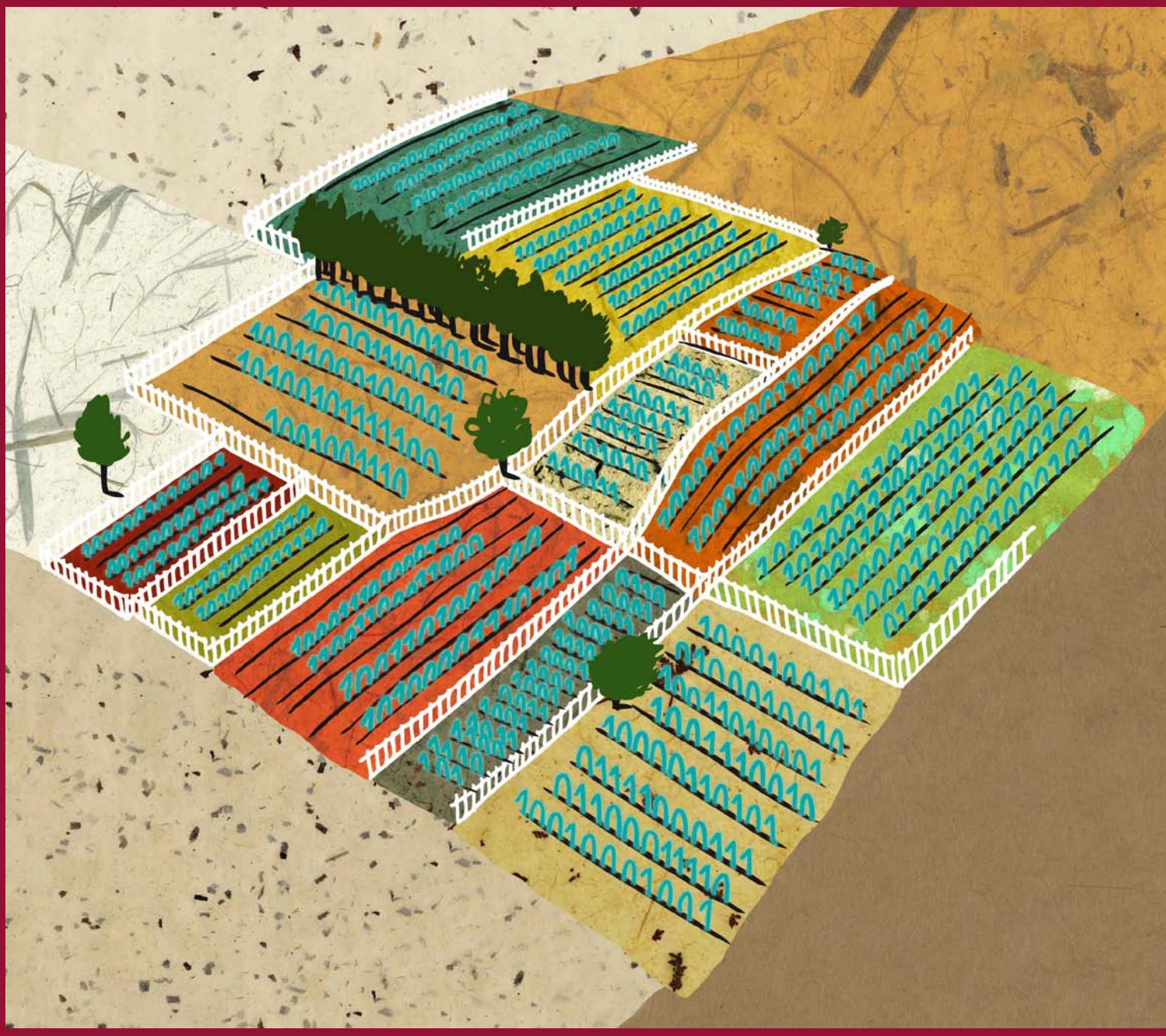
Corrado Moiso
informatico dal 1984 è in Azienda. Inizialmente ha studiato linguaggi logici e funzionali, l'elaborazione distribuita ad oggetti ed il loro uso in TMN. Dal 1994, con diversi ruoli di responsabilità, ha investigato l'introduzione di IT nell'Intelligenza di Rete, contribuendo alla sperimentazione di TINA, allo standard Parlay ed all'introduzione di SOA e di soluzioni autonomiche nelle piattaforme di servizio. Attualmente, nel contesto delle attività di "Innovative Architectures" presso Future Centre di Telecom Italia, investiga come soluzioni IT innovative possono abilitare nuovi scenari applicativi per gli operatori di Telecomunicazione. Ha collaborato a progetti finanziati da EC ed Eurescom; è autore diverse pubblicazioni, nonché di brevetti su sistemi e metodi per servizi.

Gianluca Zaffiro
laureato in Ingegneria Elettronica presso il Politecnico di Torino nel 1992, con Master in Telecomunicazioni presso COREP/SSGRR nel 1995. Entra in Telecom Italia nel 1994 dove si è occupato di reti ottiche, partecipando all'IEC per gli standard e la pubblicazione di numerosi articoli. Da qualche anno opera nel gruppo Innovation Trends di Telecom Italia Lab. È responsabile per Telecom Italia dell'azione di coordinamento ISTFP6Peach per la ricerca sulla Presenza, sul cui tema ha pubblicato alcuni articoli. Si occupa di elaborare scenari innovativi di medio/lungo periodo di interesse per le telecomunicazioni. Nel 2004-2005 ha collaborato a numerose attività sulla Convergenza FissoMobile. Nel 2003 ha collaborato a dare supporto strategico per l'innovazione tecnologica dell'area MobileServices di TIM. Nel 2001-2002 ha partecipato al lancio del servizio di Mobile Instant Messaging, TIMCafè, focalizzandosi su aspetti di marketing.

Usa il tuo smartphone per visualizzare approfondimenti multimediali

LE NORMATIVE SULLA PRIVACY

Francesco Nonno



Oggi nella società dell'informazione, quasi ogni aspetto della nostra vita è caratterizzato dall'utilizzo di dati personali che consentono di identificarci e distinguerci dagli altri e che forniscono a chi ne è in possesso la chiave per accedere alla sfera privata, anche più intima, della nostra persona e delle nostre relazioni e comportamenti. E' questo che ha determinato il radicale cambiamento del concetto di privacy: dal "diritto alla riservatezza o meglio ad essere lasciati in pace" si è passati al "diritto di controllare le informazioni che ci riguardano".
L'attuale concezione di privacy è comunque il risultato di un'evoluzione che si è sviluppata nel corso di diversi secoli. Vediamo come.

1 Introduzione

Il termine "privacy" è oggi comunemente inteso come il diritto della persona di controllare le informazioni che la riguardano, un significato che quindi va al di là dei tradizionali aspetti legati alla riservatezza (intesa essenzialmente come diritto di tutela per le informazioni relative alla sfera privata e familiare, al domicilio ed alla corrispondenza).
La necessità di tutelare la riservatezza della vita privata è stata riconosciuta fin dai tempi delle civiltà antiche. Ad esempio, il Corano indica ai fedeli di non spiare o parlar male gli uni degli altri e la Torah prescriveva di disporre gli accampamenti in modo che le tende non fossero esattamente prospicienti, cosi che non fosse possibile occhieggiare da una tenda all'altra.
Nell'Inghilterra del 14° secolo, il Justice of the Peace Act prevedeva l'arresto per coloro che ascoltavano indebitamente conversazioni private e, circa tre secoli più tardi, il parlamentare inglese William Pitt scriveva: "l'uomo più povero nella sua casupola può sfidare tutte le forze della Corona. Può essere una casupola fragile, con il tetto traballante, il vento può soffiarvi dentro, il temporale e la pioggia possono entrarvi, ma il Re d'Inghilterra non può entrarvi senza permesso".
Anche al di fuori del mondo anglosassone, altre nazioni europee si dotarono fin dal XVIII e XIX secolo di norme relative al trattamento dei dati personali. Ad esempio, nel 1776 il Parlamento Svedese promulgò una legge che prevedeva che il governo utilizzasse le informazioni relative ai cittadini solo per scopi legittimi. Nel 1858, la Francia proibì la pubblicazione di fatti personali, prevedendo multe salate per i contravventori. Il codice penale norvegese vieta, fin dal 1889, la pubblicazione di informazioni relative ai fatti personali o familiari di un individuo.
Ma un punto di svolta nel riconoscimento della privacy come diritto a se stante dell'individuo avvenne nel 1890. Due avvocati di Boston (USA), S. Warren e L. Brandeis, come reazione alle indiscrezioni pubblicate dall'Evening Gazette di Boston sulle amicizie della signora Warren e sulle nozze della figlia, pubblicarono un saggio intitolato "The right to privacy", in cui enunciarono il "diritto ad essere lasciato in pace" ("the right to be let alone"), quindi diritto per le persone a non subire interferenze esterne nella propria vita privata e nelle informazioni che le riguardano. Nasceva così, nel Common Law il c.d. "The right to privacy" inteso come diritto alla riservatezza.
Ma è a partire dalla seconda metà del XX secolo che l'avvento delle moderne tecnologie informatiche ha via via reso disponibili strumenti per la raccolta e l'elaborazione di quantità enormi di dati, il cui uso illecito o scorretto può presentare gravi rischi. Come

conseguenza, diversi stati ed organizzazioni sovranazionali hanno sentito l'esigenza di dotarsi di norme e regolamenti che disciplinassero l'uso di tali dati, dando vita a modelli di regolamentazione che differiscono tra loro e tendono a riflettere le caratteristiche culturali, storiche ed economiche dei diversi Paesi.

Vediamo dunque quali sono i principali modelli di regolamentazione in materia di privacy ad oggi presenti a livello mondiale.

Comprehensive law. E' il modello di regolamentazione adottato nella Unione Europea, che prevede l'adozione di leggi che regolino a livello complessivo la raccolta, l'uso e la comunicazione dei dati personali nel settore sia privato che pubblico. Generalmente, gli stati che aderiscono a tale modello si dotano di una autorità o agenzia indipendente, con compiti di indirizzo e supervisione nel trattamento dei dati personali. Tra le motivazioni che spingono le nazioni, in particolare quelle che hanno sperimentato regimi totalitari, ad adottare questo modello vi può essere il desiderio di rimediare alle ingiustizie passate e prevenire abusi nel futuro. Inoltre, altri Stati, in particolare nell'area asiatica, stanno cercando di dotarsi di leggi di questo tipo, anche al fine di rassicurare i consumatori e favorire così il commercio internazionale ed anche la delocalizzazione di attività di data management, call center ecc.

Sectoral law. E' il modello adottato dagli Stati Uniti, ove il trattamento dei dati personali è regolato da leggi specifiche per i diversi settori considerati critici per la privacy degli individui, ad esempio la sanità o l'ambito del credito e della finanza. In generale, questo modello di regolamentazione non prevede l'esistenza di un'unica autorità di supervisione e controllo, con il conseguente rischio di scarso coordinamento tra le norme dei diversi settori, che tendono talvolta a sovrapporsi creando problemi di interpretazione ed applicazione.

Co-regulatory model. Adottato ad esempio in Canada ed in Australia, si basa sull'integrazione di standard e codici di autoregolamentazione aventi valore cogente, sviluppati dagli stessi comparti economici che li dovranno applicare, sotto la supervisione di un'autorità indipendente.

Self-regulatory model. E' il modello adottato ad esempio negli Stati Uniti (unitamente al succitato "Sectoral Law") ed in Giappone, in cui le aziende devono rispettare i codici di autoregolamentazione adottati da organizzazioni imprenditoriali dei rispettivi comparti industriali o economici o anche da autorità indipendenti.

2 L'approccio USA: la privacy come diritto del consumatore

Ad oggi, due principali approcci alla regolamentazione in materia di privacy sono prevalenti negli Stati Uniti d'America.
Il primo si basa sulle cosiddette "fair information practices", che prevedono come elementi fondamentali l'informativa ed la capacità di scelta dell'interessato. Si tratta di un approccio che prende in considerazione il processo che porta al trattamento dei dati ed è esemplificato dal cosiddetto GLBA (*Gramm-Leach-Bliley Act*). Tale norma rimosse le barriere poste da leggi previgenti alla fusione tra le attività economiche di società operanti in diversi settori finanziari, come banche e assicurazioni. La possibilità di trasferire informazioni tra questi diversi soggetti economici creò preoccupazioni nell'opinione pubblica per la tutela della privacy dei cittadini, tanto più che, pochi anni prima dell'approvazione del GLBA, erano venuti alla luce dei casi di pratiche illecite. In particolare, erano state scoperte alcune importanti istituzioni finanziare che vendevano dettagliate informazioni sui propri clienti a società di telemarketing, che poi le utilizzavano per addebitare a clienti inconsapevoli servizi non richiesti. Il caso più clamoroso riguardò la US Bancorp e l'azienda di telemarketing MemberWorks e terminò con un'ammenda di 3 milioni di dollari inflitta alla banca per frode e pratiche commerciali scorrette. Di conseguenza, furono inserite nel GLBA specifiche disposizioni a tutela dei dati personali, che in sintesi riguardano l'adozione di misure per la sicurezza dei dati, l'obbligo di informare il cliente riguardo le policy di comunicazione dei suoi dati personali a terze parti e la sua possibilità di opporsi alla condivisione dei suoi dati finanziari con terze parti.
Il secondo approccio prevalente negli USA è quello del cosiddetto "permissible purpose", che limita il trattamento dei dati personali a determinate finalità, previste dalla legge; questo approccio prende quindi in considerazione il contesto in cui avviene il trattamento dei dati. Il FCRA (*Fair Credit Reporting Act*), promulgato nel 1970, è una delle leggi sulla privacy in vigore da più tempo negli USA e costituisce il miglior esempio di attuazione di questo approccio. Nell'America degli anni '60 era diffusa tra i commercianti la prassi dello scambio di informazioni relative ai propri clienti ai fini della concessione di credito. In molti casi, i cittadini si trovavano danneggiati a causa di informazioni imprecise, che peraltro essi non potevano né conoscere né correggere. Per risolvere tale situazione, il FCRA prevede che le cosiddette Credit Reporting Agencies garantiscano una ragionevole accuratezza delle informazioni relative al credito e le forniscano solo a soggetti che le trattano per finalità consentite (legittime attività economiche, gestione del rapporto di lavoro, obblighi di legge ecc.). Inoltre, gli interessati devono poter accedere alle informazioni che li riguardano ed hanno il diritto di essere informati qualora sulla base di tali informazioni siano prese decisioni negative, ad esempio negando un finanziamento.
In generale, quindi, le leggi degli Stati Uniti mirano a regolamentare il trattamento dei dati personali in specifici ambiti di attività economica, nella misura in cui vi possano essere rischi per il consumatore. Ne deriva che negli Stati Uniti, differentemente dall'Europa (come di seguito descritto), la privacy non costituisce un diritto fondamentale dell'individuo, ma è un *diritto del consumatore*, da bilanciare con le esigenze di business delle imprese.
In linea con questa impostazione, negli Stati Uniti non esiste una specifica autorità incaricata della tutela dei dati personali dei cittadini, equivalente ad esempio al Garante privacy italiano. La FTC (*Federal Trade Commission*), che è la principale agenzia incaricata della tutela dei consumatori negli Stati Uniti, vigila anche sull'aderenza dei comportamenti delle aziende a quanto esse dichiarano nelle proprie privacy policy e sul rispetto delle leggi in materia di privacy. Al riguardo, occorre notare che il potere di controllare il corretto adempimento di obblighi normativi deve essere previsto dalle leggi stesse, mentre il potere di vigilare sull'applicazione delle privacy policy definite dalle aziende è insito nella legge istitutiva della FTC (il cosiddetto FTC Act). Infatti la FTC ha, tra l'altro, il compito di contrastare le pratiche commerciali "scorrette", cioè che dannose per il consumatore e "ingannevoli", cioè basate su dichiarazioni false. Peraltro, le azioni promosse dalla FTC non precludono indagini anche da parte della autorità giudiziaria.

3 Il modello europeo: la privacy come diritto dell'individuo

In ambito europeo, la privacy è considerata un "*diritto fondamentale dell'individuo*". Il suo primo riconoscimento avvenne con la "Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali" (CEDU) del 1950, il cui articolo 8 recita: "*Ogni individuo ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e della propria corrispondenza*". In questa sua prima formulazione, in linea con l'accezione adottata oltreoceano, il diritto alla privacy in Europa tendeva sostanzialmente a coincidere con il diritto alla non intrusione nelle faccende di natura privata e familiare.

La privacy come un vero e proprio diritto della persona al controllo dei propri dati personali ha trovato specifico riconoscimento in ambito europeo con la Convenzione n. 108 (la cosiddetta "Convenzione di Strasburgo" del 1981), riguardante la protezione delle persone rispetto al trattamento automatizzato di dati di carattere personale.

In tale Convenzione per la prima volta in ambito Europeo vengono stabiliti i principi per trattamento automatizzato dei dati personali (es. i principi di finalità, pertinenza e non eccedenza) e viene introdotta la definizione di dati personali, individuando in particolare i dati sensibili. Inoltre, viene garantita la possibilità di accesso degli individui alle informazioni che li riguardano direttamente.

La privacy è oggi consacrata nell'ambito della Carta dei diritti fondamentali dell'Unione europea del dicembre 2000 (recepita poi nella parte iniziale del Trattato di Costituzione europea, il cosiddetto Trattato di Lisbona in vigore dal 1° dicembre 2009), nonché nel Trattato sul Funzionamento dell'Unione Europea. In particolare, la Carta riconosce i due seguenti distinti e complementari diritti fondamentali:

- *Rispetto della vita privata e della vita familiare*: ogni individuo ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e delle sue comunicazioni (articolo 7);
- *Protezione dei dati di carattere personale*: ogni individuo ha diritto alla protezione dei dati di carattere personale che lo riguardano (articolo 8).

Sulla scia della Convezione di Strasburgo del 1981, nell'ambito della Comunità europea viene introdotta una vera e propria disciplina organica sulla privacy attraverso la Direttiva 95/46/CE, (la cosiddetta "Data Protection Directive" o anche "Direttiva madre"), disciplina che è stata successivamente completata, per il settore delle comunicazioni elettroniche, dalle norme della direttiva 2002/58/CE (cosiddetta "E-Privacy") e della direttiva 2006/24/CE (quest'ultima relativa al trattamento dei dati di traffico per di indagine, accertamento e perseguimento di reati gravi).

Il quadro normativo europeo è stato ovviamente concepito sul principio che la privacy è un diritto fondamentale dell'individuo, il quale va tutelato in quanto tale. Tutti i cittadini europei devono godere di un livello equivalente di protezione dei propri dati personali e, pertanto, le norme sono applicabili a tutti i settori industriali nel trattamento dei dati personali. Inoltre, alcuni settori sono soggetti ad ulteriori specifiche e molto spesso più stringenti norme, come quello delle comunicazioni elettroniche.

L'ambito di applicazione di queste norme riguarda il trattamento dei dati personali, definiti come "*qualsiasi informazione concernente una persona fisica identificata o identificabile; si considera identificabile la persona che può essere identificata direttamente o indirettamente, in particolare mediante riferimento ad un numero di identificazione o ad uno o a più elementi specifici caratteristici della identità fisica, fisiologica, psichica, economica, culturale o sociale*". Tra tali dati rientrano quindi sia i dati anagrafici di una persona (es. nome e cognome) che quelli riconducibili alla stessa persona, quali ad esempio il codice fiscale, il numero telefonico, le proprie immagini, il numero di carta di credito, la matricola, l'indirizzo IP, ed al suo comportamento (es. tipologia e volumi degli acquisti, navigazione in internet, ecc.).

Al trattamento dei dati personali si applicano una serie di principi (ad esempio, quelli di finalità, pertinenza e non eccedenza, aggiornamento), regole (ad esempio, è possibile trattare i dati previa informativa e consenso della persona interessata, salvo che non sussistano altri presupposti di liceità; gli individui hanno il diritto di accedere ai dati che li riguardano e, se necessario, correggerli o opporsi al loro trattamento) e misure di sicurezza.

Altro aspetto qualificante della normativa europea è costituito dalle tutele poste al trasferimento dei dati personali all'esterno dell'Unione Europea. Tale trasferimento è consentito solo verso i pochi Stati a cui la Commissione Europea ha riconosciuto un livello di protezione dei dati personali equivalente a quello comunitario oppure mediante l'adozione di determinate misure. In particolare, per il trasferimento verso gli Stati Uniti vige il regime di "Safe Harbor", applicabile ai trasferimenti di dati verso aziende stabilite negli Stati Uniti che abbiano aderito a tale regime adottando volontariamente determinate misure per la protezione dei dati personali, sotto il controllo della Federal Trade Commission.

4 Gli impatti

A distanza di circa diciotto anni dall'adozione della "Direttiva madre", è possibile affermare che i principi in essa contenuti risultano tuttora validi, ma al contempo vanno riconosciuti alcuni punti di debolezza derivanti soprattutto dallo sviluppo di nuove tecnologie (es. internet), che hanno reso sempre più facile ed immediata la circolazione dei dati a livello internazionale.

In primo luogo, la diversa trasposizione delle norme comunitarie da parte degli Stati membri ha determinato l'assenza di armonizzazione nell'ambito della stessa Unione Europea anche su aspetti importanti quali la gestione consenso dell'individuo al trattamento dei propri dati personali. Ciò ha avuto impatti, ad esempio, sul telemarketing: alcuni Paesi, quali il Regno Unito, hanno privilegiato il regime di "opt-out" (cioè il diritto per l'utente di opporsi a seguito di attività promozionale); altri Paesi, quali l'Italia, hanno adottato invece il più stringente regime di "opt-in" (cioè raccolta del consenso preventivo ed informato), che ovviamente pone maggiori vincoli all'attività imprenditoriale.

Altro aspetto critico è rappresentato dal cosiddetto "principio di stabilimento", che prevede l'applicabilità delle norme privacy europee solo nei confronti delle aziende che trattano i dati presso un proprio stabilimento situato nell'Unione o, nel caso di aziende extra UE, che trattano i dati con

strumenti situati nel territorio di uno Stato membro. Ne deriva uno squilibrio competitivo a favore dei soggetti extra UE che, in base al suddetto "principio di stabilimento", applicano le proprie normative nazionali di norma meno stringenti di quelle europee.
Ciò è particolarmente vero per il mercato dell'on-line che è dominato dai fornitori dei servizi della società dell'informazione, tipicamente statunitensi (i cosiddetti Over The Top, quali Google) che beneficiano, in virtù della diversa impostazione della privacy negli Stati Uniti, di norme che prevedono essenzialmente solo l'obbligo di informativa per raccogliere i dati sul comportamento e sulle preferenze degli utenti on-line ai fini di invio di pubblicità profilata. Al contrario, questa attività Europa è consentita solo previo consenso informato dell'utente, vincolo che limita fortemente lo sviluppo delle imprese europee in questo mercato.
Proprio al fine di superare tali punti di debolezza, la Commissione Europea ha presentato a gennaio 2012 (attualmente in esame presso il Parlamento europeo ed il Consiglio d'Europa) una proposta di revisione del quadro regolamentare privacy europeo, basata tra l'altro su un Regolamento per la protezione dei dati personali, che sostituirà la "Direttiva Madre" e sarà direttamente applicabile agli Stati membri.
Una delle novità più significative del Regolamento è rappresentata dal nuovo criterio di applicazione delle norme europee, che peraltro restano stringenti rispetto a quelle statunitensi, anche alle aziende extra UE che trattano dati di cittadini europei, indipendentemente da dove queste sono stabilite.

Conclusioni

Sicuramente nei prossimi mesi assisteremo sempre più ad un vibrante confronto tra due modelli di "fare" privacy; vedremo se avrà la meglio il pragmatismo statunitense, oppure l'approccio umanistico europeo. Certo è che dalle risultanze di questo confronto ci saranno inevitabili ripercussioni nei modelli di business degli imprenditori; bisognerà solo capire se saranno quelli a stelle e strisce oppure quelli europei ■

Bibliografia

In particolare per l'evoluzione storica del concetto di privacy:

- "*European Privacy*" di Eduardo Ustaran, IAPP Publication, 2012
- "*CIPP Guide – Privacy Fundamentals*", di autori vari, Jon-Michael Brook, 2007
- "*The right to privacy*" di Samuel D. Warren e Louis D. Brandeis, Boston, 1890 (Edito da Garante per la protezione dei dati personali a dicembre 2005)

In particolare per la descrizioni dei modelli internazionali di regolamentazione privacy e la normativa USA:

- "*Information Privacy*" di Peter P. Swire e Sol Bermann, IAPP Publication, 2007

In particolare per la descrizione dei poteri della FTC:

- "*The IAPP Information Privacy Case Book*", di Margaret P. Eisenhauer, IAPP Publication, 2008

In particolare per la descrizione della normativa europea

- "*Sette anni di protezione dati in Italia. Un bilancio e uno sguardo sul futuro*" a cura di Francesco Pizzetti (Garante per la protezione dei dati personali), G. Giappichelli Editore, 2012
- "*Direttiva 95/46/CE relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati*"
- Comunicazione della Commissione Europea del 4/11/2010 "*A comprehensive approach on personal data protection in the European Union*"
- "*Proposta di Regolamento del Parlamento Europeo e del Consiglio concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati del 25/01/2012*"

Urlografia

- *http://www.garanteprivacy*, sito del Garante Privacy italiano
- *http://www.edps.europa.eu*, sito del European Data Protection Supervisor
- *http://ec.europa.eu/justice/data-protection/index.en,* sito della Commissione Europea dedicato alla Data Protection
- *http://www.privacyassociation.org*, sito della IAPP (*International Association of Privacy Professionals*)

francesco.nonno@telecomitalia.it

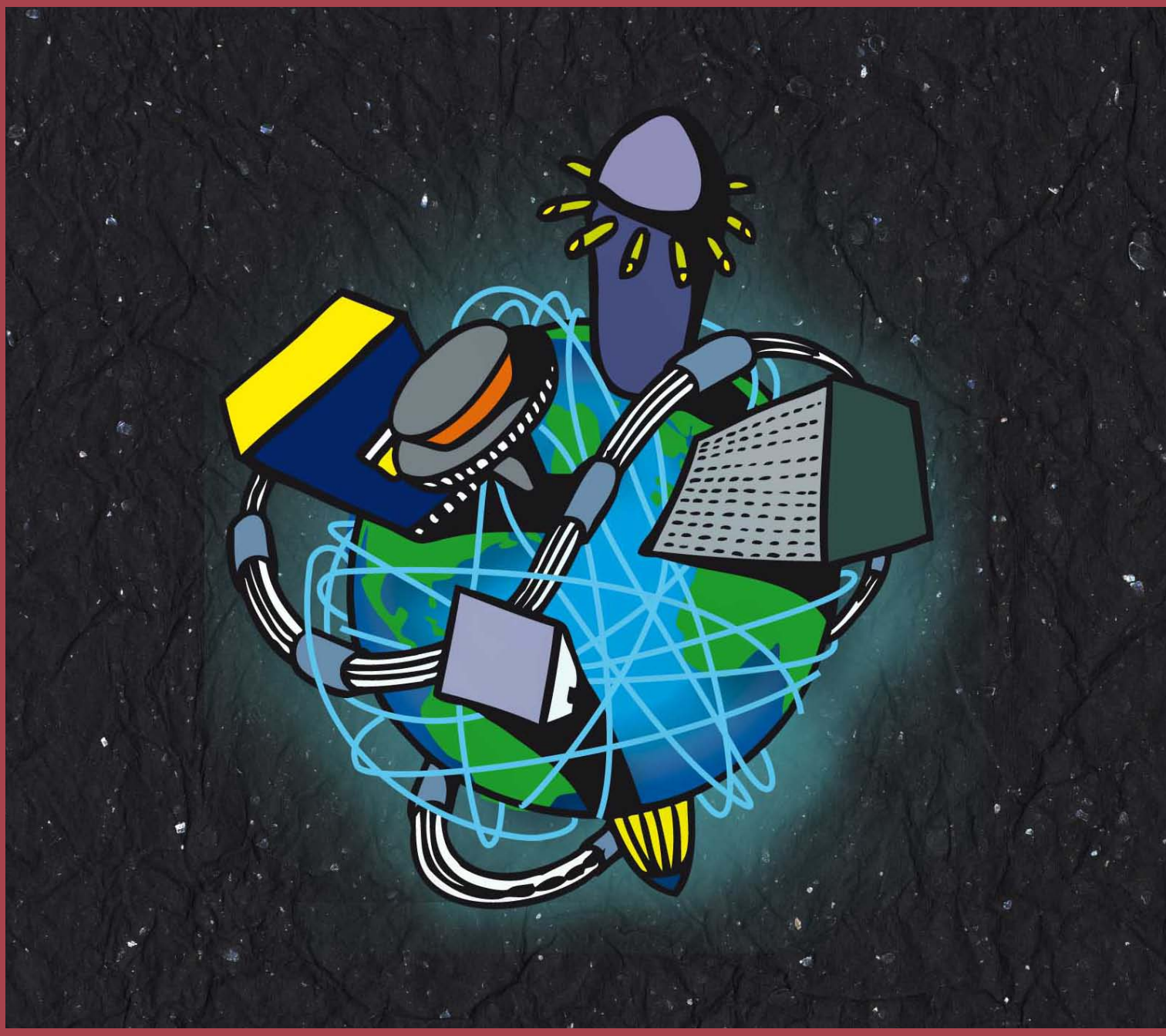
Usa il tuo smartphone per visualizzare approfondimenti multimediali

Francesco Nonno
dal 2004 in Telecom Italia, oggi è responsabile della funzione Rapporti con le Authorities Nazionali di Telecom Italia e consigliere dell'Associazione Italiana Operatori IPTV. Precedentemente ha operato per circa 10 anni in società di consulenza specializzate nel settore delle comunicazioni, in Italia e in Francia, come responsabile di progetti di analisi strategica e di posizionamento di prodotti/servizi di telecomunicazioni. Successivamente ha lavorato presso l'Autorità per le Garanzie per le Comunicazioni, diventando anche responsabile dell'ufficio Operatori e servizi di telecomunicazioni nell'ambito del Dipartimento Vigilanza e Controllo.

Usa il tuo smartphone per visualizzare approfondimenti multimediali

INTERNET OLTRE IL 2020

Roberto Saracco



Per curiosità ho provato ad andare su Google e cercare "Internet Trends". Esistono 158.000.000 puntatori[1]. Confesso di non averli letti tutti!
Il fatto è che Internet è diventata ormai una parte così centrale del nostro mondo da essere nominata in continuazione e giustamente essere al centro di qualunque previsione sul futuro. In questo articolo vorrei condividere alcune riflessioni che ho fatto e continuo a fare e che riporto ogni giorno su un mio blog[2].

1 Introduzione

Internet è più che una rete, più che una immensa biblioteca aggiornata in tempo reale. Per molti giovani oggi è già parte integrante del loro mondo[3], se qualcosa non esiste su Internet (ma cosa non c'è su Internet?) non esiste punto e basta. E quindi, anche la propria esistenza per essere tale deve essere certificata da Internet, sia questo una foto su Facebook o un pensiero su twitter.
Se però si guarda bene, internet è ben distante dall'essere "tutto". Ed è proprio in questa distanza tra ciò che è oggi ed il tutto che dobbiamo, secondo me, cercare la sua evoluzione nei prossimi anni.
Un secondo aspetto è quello che non si ha una semplice espansione di Internet. Quello che si verifica è un cambiamento del contesto, per cui nei prossimi anni Internet non andrà ad occupare semplicemente spazi in cui oggi non è presente, ma cambierà la geografia del mondo e della società. Ed in questo sta la difficoltà maggiore nel prevedere le sue evoluzioni.

2 Ci sono reti e reti

Partirei proprio da questo aspetto, osservando come esistano vari tipi di reti, in una sequenza di astrazioni che ha conseguenze interessanti.
Abbiamo da centocinquant'anni la rete fissa, un insieme sempre più esteso e complicato di fili che connettono ormai quasi tutto il mondo. L'evoluzione sta trasformando questi fili da rame a fibra, ma concettualmente le cose non cambiano: rimane una struttura rigida che connette un punto ad un altro. Negli ultimi quindici anni abbiamo visto l'estendersi di reti radio di terza generazione, che, a differenza di quelle di seconda generazione, che sostanzialmente sostituivano parte del rame con lo spettro elettromagnetico in aria ma mantenevano lo stesso paradigma, forniscono una connettività che cambia a seconda dell'utilizzo istantaneo che ne viene fatto. Infatti, la singola cella coperta da un'antenna varia le sue dimensioni a seconda della posizione degli utilizzatori e del modo in cui viene usato lo spettro. È una rete, quindi, che cambia la sua topologia per meglio sfruttare lo spettro radio (anche se così facendo taglia fuori, a volte, alcuni utilizzatori che vengono a trovarsi in una zona non più coperta). Sistemi radio basati su celle mobili, quali potrebbero essere quelle formati da telefonini che usano Bluetooth (ad esempio per il Bluejacking), piuttosto che in prospettiva aree di comunicazione radio generate da autoveicoli in movimento sono ulteriori esempi di reti che cambiano continuamente la loro topologia. Sebbene anche a livello di reti fisse si abbia una qualche flessibilità che porta a cambiarne le caratteristiche di traffico non si raggiunge ancora la flessibilità che dimostrano le reti radio citate. In prospettiva, il passaggio a Software Defined Networks potrebbe portare a flessibilità paragonabili a queste.
Abbiamo, e da milioni di anni, reti di comunicazione (o forse sarebbe meglio chiamarle di connessione) che cambiano in continuazione: quelle che troviamo nel nostro

1 Cercando Internet 2020 trends vengono trovati 14.200.000 puntatori, mentre cercando Internet trends 2020 i puntatori scendono a 1.790.000. Comunque troppi per i miei gusti.
2 http://www.blog.telecomfuturecentre.it
3 https://www.youtube.com/watch?v=aXV-yaFmQNk

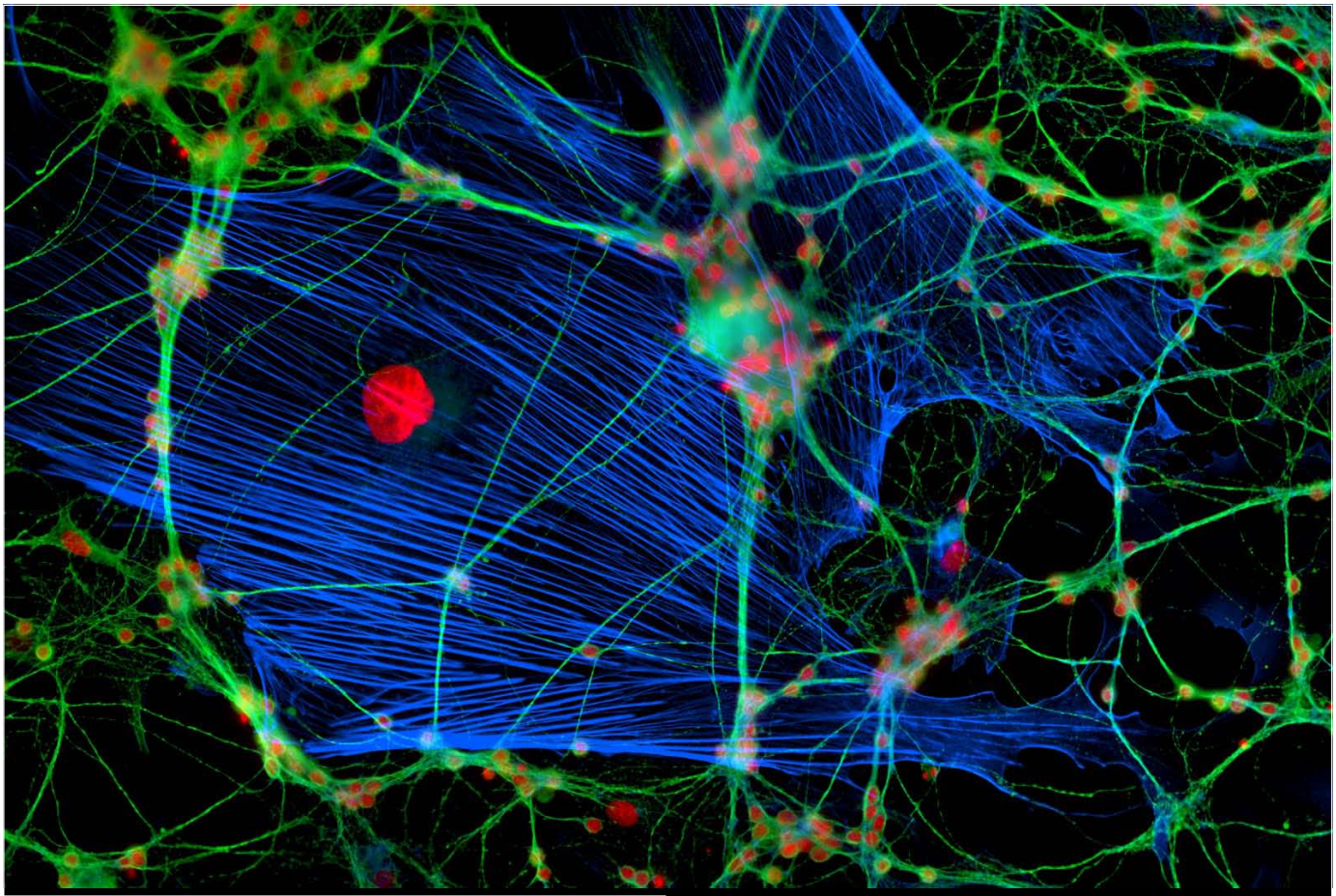


Figura 1 - Rete neuronale *(fonte: http://elenascaratti.blogspot.it/2011/08/microbio-macrourban.html)*

cervello ed in quello di quasi tutti gli animali.
Queste reti hanno la caratteristica di mutare nel tempo sotto la spinta del modo in cui sono utilizzate (in altri termini la reazione ad un "input" porta nel tempo ad un cambiamento della rete stessa) e sono inoltre sensibili al contesto complessivo (uno stesso stimolo può portare a situazioni molto diverse che attivano connessioni diverse nella rete). Esistono tecnologie che consentono di realizzare reti di questo tipo, basate su nuovi tipi di chip (memristor), su particolari architetture di connessione (reti neurali), e su un'integrazione tra connettività, elaborazione e memorizzazione (reti autonomiche).

Per finire, almeno nello scopo di questo articolo, abbiamo un ulteriore esempio di tipo di rete, quella formata dai pensieri (espressi in varia forma, dal parlato alla immagine, allo scritto ed, anche, al solo pensato). Queste reti le troviamo abilitate nella corteccia del cervello e anche su Facebook o Twitter, per non dire in una riunione tra amici. I pensieri che fluiscono innescano nuovi pensieri, del tutto imprevedibili a priori e questi a loro volta ne innescano altri portando ad un cambiamento del contesto complessivo.
Ovviamente, Facebook e Twitter hanno poco a che vedere, dal punto di vista tecnologico, con una tavolata di amici, ma il paradigma di fondo è identico: siamo in presenza di reti in cui quello che fluisce nella rete la cambia, generando ulteriori messaggi sulla rete stessa.
Come si può notare, queste quattro tipologie di rete possono essere considerate come un'evoluzione di paradigma e questo è quello che ritengo vedremo capitare ad Internet nei prossimi dieci quindici anni. Mentre nel passato vi è stato un totale disaccoppiamento tra rete e contenuti, oggi vediamo che alcuni contenuti condizionano la rete ed in futuro sarà molto difficile distinguere la rete dai contenuti, in quanto a livello percettivo, ma anche architetturale, avremo una profonda compenetrazione tra l'aspetto della comunicazione, quello della elaborazione e quello

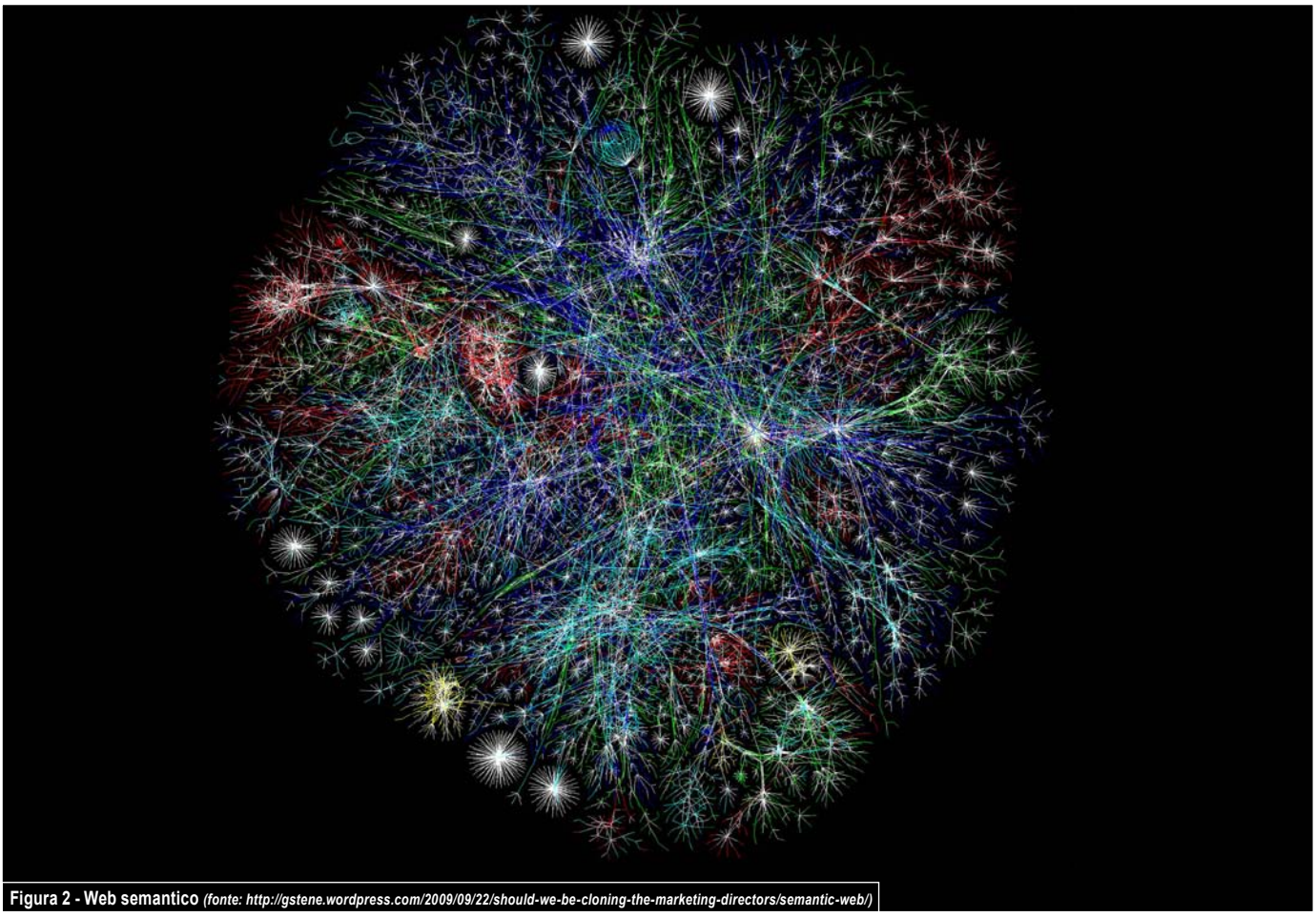


Figura 2 - Web semantico *(fonte: http://gstene.wordpress.com/2009/09/22/should-we-be-cloning-the-marketing-directors/semantic-web/)*

della memorizzazione. Andremo, cioè, verso il Web Semantico, che credo sia riduttivo chiamarlo in questo modo, in quanto perdiamo un elemento fondamentale: noi. In futuro sarà sempre più difficile separare noi dal web ed il web da noi. Internet, e lo vedremo subito, sta evolvendo ancor di più di quanto già non lo sia verso una rete di reti. A differenza di oggi, però, gran parte di queste reti saranno reti formate da oggetti che creano attorno a loro un alone di connettività, le cosiddette "halo nets". Ciascuna di queste racchiude in sé caratteristiche di elaborazione e memorizzazione oltre a connettività locale. L'insieme di un enorme numero di queste reti porta a comportamenti emergenti, così come accade nel cervello: dalle reti di neuroni e astrociti, da segnali elettrici e chimici emerge il pensiero.

Dato l'uso che si farà, in modo autonomico, di questi oggetti e reti relative, emergeranno nuove aggregazione, nuovi "smart ambient".

L'Internet del futuro, anche a seguito dell'evoluzione della comunicazione nel senso della connettività locale, sarà pervasiva a livello degli ambienti e coinvolgerà gli oggetti.

3 Da bit ad atomi

L'evoluzione tecnologica ha reso quasi trascurabile il costo di processing, memorizzazione e trasmissione. Ha tagliato anche il costo "energetico" ed entro 10 anni è possibile prevedere che molti chip potranno trovare nell'ambiente sufficiente energia (potenza) per lavorare.

Anche i materiali con cui i chip verranno fatti migreranno dal silicio al carbonio e soprattutto potranno essere "dipinti" su molti tipi di materiali, biologici inclusi. Benvenuti nell'era degli embedded system.

Sono anni che si parla di embedded system, e ne abbiamo moltissimi intorno a noi, dalla chiave elettronica per la stanza d'albergo all'orologio. Ma entro dieci anni trovare un oggetto che non abbia "embedded" una qualche forma di chip sarà molto difficile.

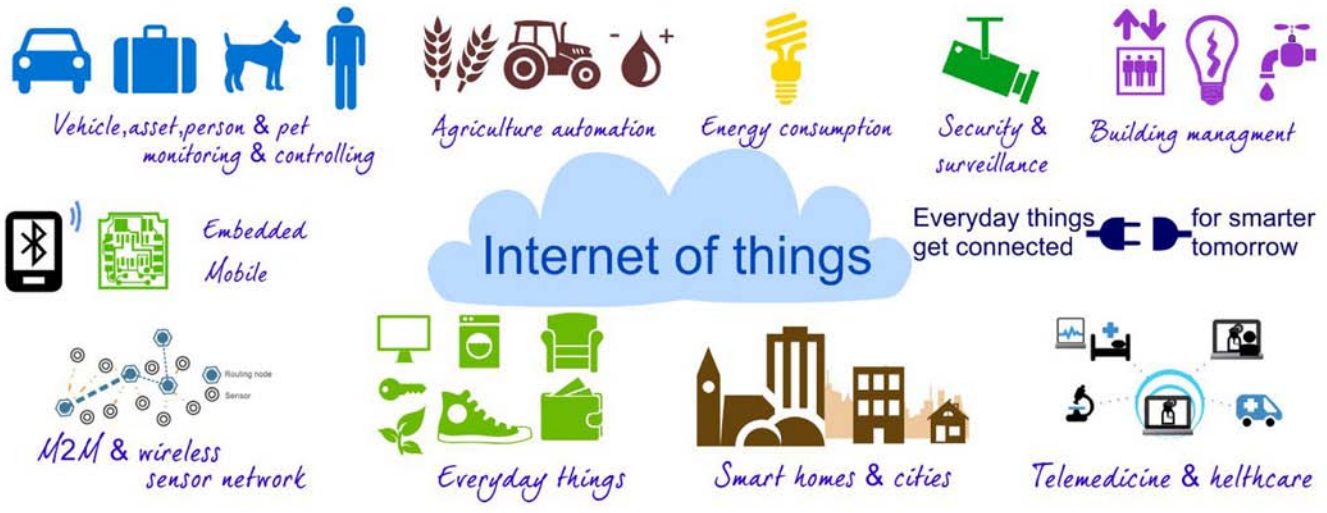


Figura 3 - Internet delle cose *(fonte: http://www.nkonnect.com/technology-solutions/internet-of-things/)*

Questo apre al mondo dell'internet delle cose e con le cose. Interessante notare come Cisco e Ericsson stimino in 50 miliardi il numero di oggetti che saranno connessi ad Internet a fine decade (compresi 7 miliardi di persone), mentre HP ne stima oltre 1.000 miliardi. La differenza non è poca: un fattore 20. E ci sta tutta, in quanto Cisco ed Ericsson tendono a riconoscere, e a contare, come oggetto connesso ad Internet un oggetto che acceda alla rete di un Operatore mentre HP conta come connesso un qualunque oggetto che comunichi, magari indirettamente, con Internet.

Personalmente ritengo sottostimato il numero di HP. In casa, oggi, ho un computer collegato alla rete, ma ho un mouse e una tastiera wireless collegati al computer, una stampante e un disco di back up collegati al computer. Ho un televisore che si collega tramite iPad alla rete e un' Apple TV, che permette allo stereo di ricevere musica da vari computer sparsi per la casa. Poi ho una decina di sensori anti-intrusione, una ventina di locomotive digitali collegate wireless ad un controller, che, a sua volta, si può connettere in Bluetooth ad un gateway, ho decine di carte (di credito, trasporto, fidelity) che non riesco neppure a tenere tutte nel portafoglio. E che dire dei vari mattoncini Lego (Mindstorm) di mio figlio che hanno sensori collegati al controller a sua volta collegato ad un telefonino e quindi alla rete?

Non dobbiamo attendere fine decade per superare i 50 miliardi di oggetti connessi, se facessimo bene i conti li abbiamo già oggi.

Se consideriamo che qualunque oggetto che contenga un codice a barre, piuttosto che una tag RFID (ne abbiamo in circolazione oltre 15 miliardi e nel 2022 si stima ne saranno vendute, solo in quell'anno, tra i 300 e i 600 miliardi[4]), può essere collegato ad Internet per associarvi servizi e informazioni, si vede che i 1.000 miliardi sono decisamente sottostimati.

Il fatto è che nei prossimi anni inizieremo a cambiare il significato che oggi diamo al termine connessione. Oggi, questo è associato a una terminazione di rete, domani oggetti, ambienti, ma anche informazioni e servizi saranno parte di un tessuto di comunicazione completamente pervasivo. Questo tessuto di comunicazione non sarà sincrono, almeno in molti casi. In altre parole, non tutto quanto farà parte di Internet sarà sempre connesso ad Internet: oggetti su uno scaffale, un pillola che abbiamo inghiottito, un sensore ambientale sono solo alcuni esempi di elementi che faranno parte di Internet anche se la connessione con questi sarà saltuaria. La sensazione di presenza sarà data spesso da una rappresentazione virtuale, questa sì sempre presente in Internet.

Questa, secondo me sarà Internet nella prossima decade, una presenza immanente. A fine anni '90 avevo suggerito provocatoriamente, la scomparsa delle telecomunicazioni, nel senso che queste sarebbero diventate così pervasive che non ci avremmo fatto più caso. Ora, che quella previsione si è sostanzialmente avverata, è il momento di estendere questa provo-

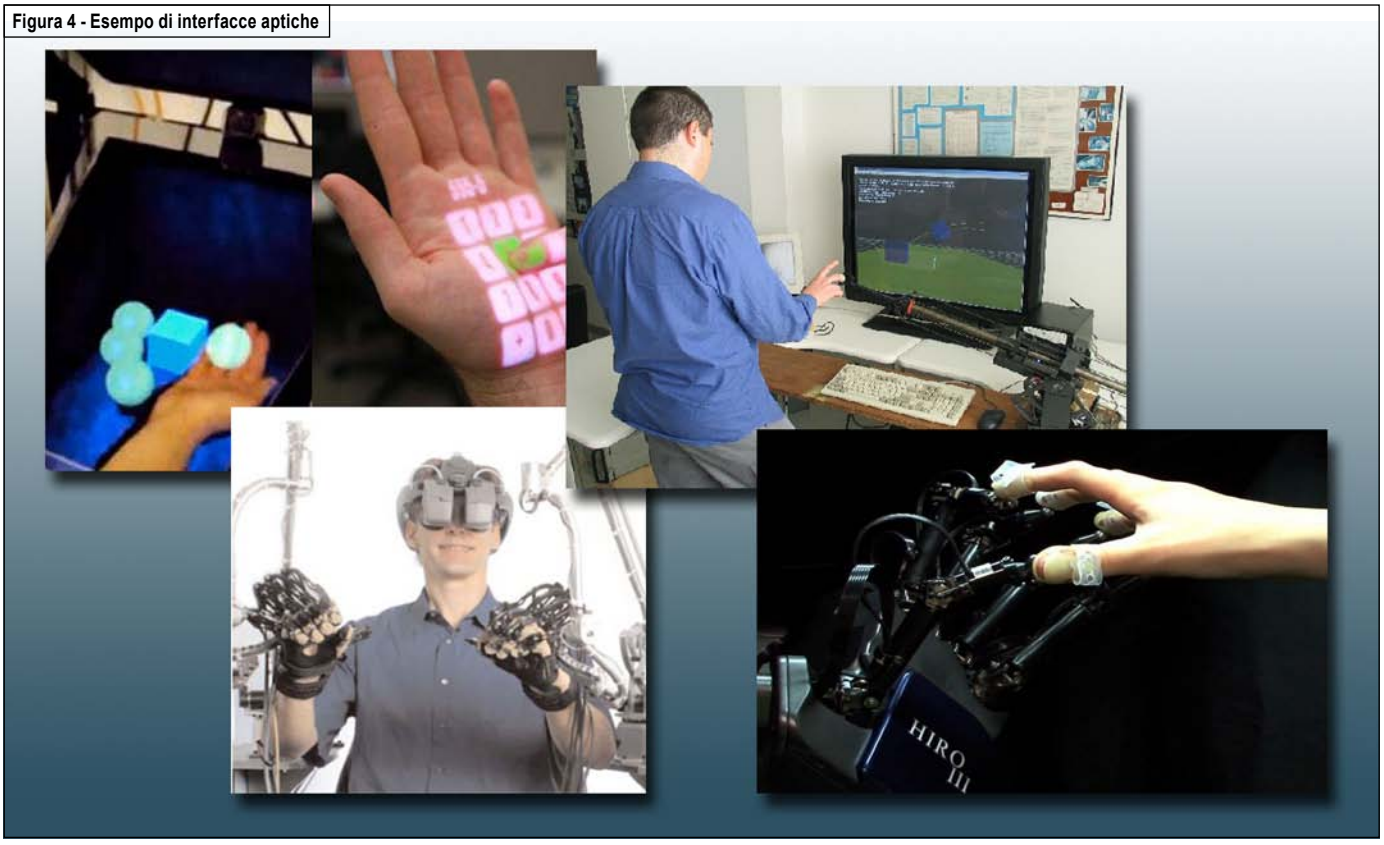
4 IdTechEx - *http://www.idtechex.com/research/articles/rfid-market-reaches-7-67-billion-in-2012-up-17-from-2011-00004585.asp*

cazione ad Internet, dicendo che nelle prossime decadi scomparirà, entrando a far parte dell'ambiente, così come lo sono delle sedie piuttosto che delle arance.
La pervasività, attraverso sensori embedded in medicine ma anche nel corpo, si estende a noi stessi. Abbiamo già visto, anche con esperimenti realizzati nel centro di ricerca di Telecom Italia[5], come sia possibile usare il nostro corpo come una rete di comunicazione e come stringendosi la mano si mettano in comunicazione due reti consentendo il trasferimento di informazioni.

4 Vivere in Internet

Connettività pervasiva e Internet Immanente. Cosa cambia nella nostra vita? La percezione del cambiamento in massima parte è determinata dalle interazioni che abbiamo e mentre oggi questo significa "terminali" nella prossima decade questo significherà "oggetti".
Grazie a smart materials, gli oggetti saranno in grado di comunicare con l'ambiente e quindi anche con noi. Numerose superfici saranno in grado di visualizzare immagini e filmati, se toccate forniranno sensazioni (interfacce aptiche); gli oggetti saranno in grado di interagire comprendendo voce, espressioni, movimenti e, ovviamente, parleranno. Tutto questo non accadrà di colpo; quando accadrà non ce ne accorgeremo neppure, in quanto questo cambiamento sarà graduale. L'interazione basata sul multitouch era sconosciuta cinque anni fa, ora non ci si fa più neppure caso.
La disponibilità di wearable (arriverà a breve l'iWatch?) come gli occhiali di Google renderà possibile l'interazione anche con oggetti che non sono ancora interattivi, attraverso la realtà aumentata. Questa trasformazione degli oggetti trasformerà anche l'industria della consumer electronics, difficile immaginare l'esistenza di un iPhone tra vent'anni. Il telefonino sarà un wearable, integrato in una varietà di oggetti, di qui la "non sorpresa" per una Apple che inizi a prendere possesso di alcuni wearable vista la futura sparizione del mercato dei telefonini. Le biotecnologie e la bio-ingegneria porteranno all'elettronica embedded anche nel nostro corpo per cui, in un certo senso, diventeremo noi stessi "terminali" e a questo punto saremo a tutti gli effetti parte integrante di Internet.

Figura 4 - Esempo di interfacce aptiche



5 *http://www.energy-home.it/SitePages/Home.aspx*

Conclusioni

Quanto sta dietro le quinte, vero motore del cambiamento, in genere non è percepito pur essendo un elemento abilitante e propulsivo nel cambiamento dei processi, dalla produzione alla logistica, dalle città alla sanità.
Qui vedremo una crescita del concetto di rete oltre a quello delle connessioni fisiche, già citate all'inizio e formate da grandi backbone in fibra che si estendono alle aree metropolitane e arrivano in molti casi ai palazzi, a cui si agganciano drop wireless e reti autonomiche, in gran parte wireless formate da oggetti con le loro "halo nets". Sopra queste reti fisiche, si poggiano le reti formate dai dati e dai servizi, in continua trasformazione. Queste saranno simili a quelle reti di pensieri citate nella parte iniziale dell'articolo. Alla loro base i big data, enormi quantità di dati generati da miriadi di sorgenti e in continua evoluzione (le 3 V che caratterizzano i Big Data: volume, varietà e velocità di aggiornamento). Se da un lato si avranno enormi data centre, in grado di gestire Exabyte di informazioni al ritmo di Exaflop al secondo, dall'altro avremo volumi ancora più massivi e con elaborazioni ancora più intense ai bordi, nei vari oggetti e devices. Certo, ciascuno avrà una frazione minuscola di dati, da qualche MB a qualche TB con capacità elaborative intorno ai Gflops (e anche meno nella maggioranza dei casi), ma complessivamente, essendo miliardi avranno un impatto dal punto di vista architetturale e di gestione dei servizi paragonabile, se non maggiore a quello dei grandi data centre.
In altri termini, l'evoluzione del mercato dei servizi e la percezione dei servizi stessi sarà maggiormente influenzata dagli ambienti e dalle loro reti/sistemi autonomici, che non da qualche centro se pur importante.
In questo scenario avremo ancora un forte ruolo di indirizzo da parte di alcuni grandi player, che assicureranno la gestione sicura e affidabile delle nostre identità digitali e il corretto, e invisibile, funzionamento di un mondo in cui bit e atomi sono le due facce di una stessa medaglia ■

roberto.saracco@ictlabs.eu

Usa il tuo smartphone per visualizzare approfondimenti multimediali

Roberto Saracco

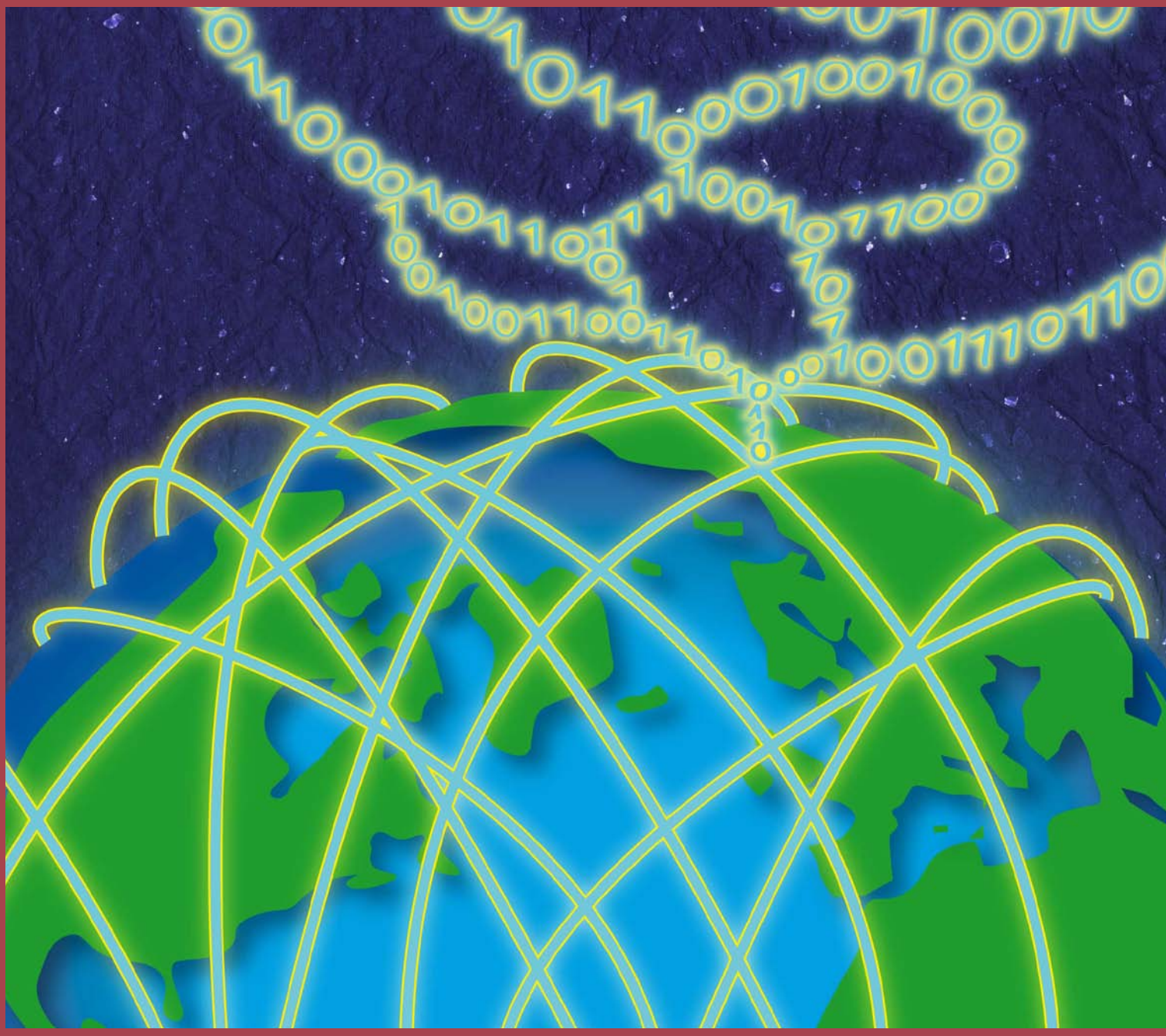
Diplomato in informatica e laureato in matematica con un perfezionamento in fisica delle particelle elementari. Negli oltre trent'anni in Telecom Italia ha partecipato a molti progetti di ricerca in commutazione, reti dati, gestione della rete, occupando varie posizioni di responsabilità. Negli ultimi dieci anni i suoi interessi si sono spostati verso gli aspetti economici dell'innovazione. Attualmente è direttore del Nodo italiano degli EIT ICT LABS con il compito di indirizzare e sviluppare innovazione tramite education (master e dottorati per futuri imprenditori), research e innovation (in particolarecon la creazione di PMI innovative).

È senior member dell'IEEE, tra i direttori della Communication Society, nonché autore di numerose pubblicazioni in Italia e all'estero.

Usa il tuo smartphone per visualizzare approfondimenti multimediali

SOFTWARE DEFINED NETWORKING: SFIDE E OPPORTUNITÀ PER LE RETI DEL FUTURO

Antonio Manzalini, Mario Ullio, Vinicio Vercellone



Il paradigma SDN (*Software Defined Networking*), secondo l'accezione più diffusa, propone l'ambiziosa visione di rendere i nodi di rete (ad es. router e switch) programmabili, introducendo opportuni livelli di astrazione, ai quali accedere attraverso l'uso di interfacce di controllo (API). Nell'ambito di questo paradigma, assume particolare rilievo anche il concetto di virtualizzazione di rete, ovvero l'idea di creare delle partizioni virtuali dell'infrastruttura di rete fisica, in modo da permettere a più istanze di controllo e le rispettive applicazioni di utilizzare le partizioni assegnate: questo permetterebbe coesistenza di più reti virtuali, completamente isolate, che insistono sulla medesima infrastruttura hardware.
La centralizzazione logica del controllo, potrebbe permettere di attuare più facilmente azioni di configurazione e ottimizzazione delle risorse di rete. L'adozione di questo paradigma potrebbe abilitare lo sviluppo di nuovi ecosistemi.

1 Introduzione

Operatore Lean o Smart ? È una delle domande chiave. L'Operatore Lean, in estrema sintesi, investe principalmente sul ruolo di Bit Carrier nell'ottica di consolidare il proprio business tradizionale, quindi punta ad un forte contenimento dei costi ma anche ad uno snellimento dei processi organizzativi; l'Operatore Smart, dovrebbe operare in maniera più disruptive, secondo una galassia di imprese, che puntano allo sviluppo di nuovi ecosistemi e nuovi modelli di business.
L'innovazione tecnologica legata al potenziale sviluppo del paradigma SDN potrebbe impattare entrambi i ruoli, ovviamente in maniera più o meno sensibile, in funzione del livello e delle modalità di possibile adozione: infatti mentre da una parte SDN potrebbe portare vantaggi economici per gli Operatori Lean, dall'altra potrebbe abilitare lo sviluppo di nuovi ecosistemi di servizi, che costituirebbero potenziali opportunità di sviluppo per gli Operatori Smart, nella misura in cui questi riescano a ritagliarsi un ruolo e inserirsi in un modello di business vantaggioso.
Una delle principali sfide tecnologiche del paradigma SDN riguarda la centralizzazione della logica del controllo: questo abiliterebbe le applicazioni ad acquisire una vista astratta della rete, come se questa fosse governata da un piano di controllo concettualmente centralizzato (ed integrato con il sistema di gestione). Diventa quindi possibile implementare logiche di controllo astraendo dalla complessità fisica della molteplicità degli apparati di rete. Lo strato di controllo ha il compito di presentare una vista unica, globale e logicamente centralizzata, gestendo la topologia fisica della rete e la distribuzione delle informazioni di stato necessarie ad implementare le logiche di servizio. Il cuore della SDN assomiglia dunque ad un ecosistema di moduli software di controllo, interagenti fra di loro e capaci di attuare più facilmente azioni di configurazione e ottimizzazione delle risorse di rete. D'altra parte, la stessa centralizzazione logica del controllo potrebbe avere dei punti critici, quali ad esempio livelli di prestazioni, affidabilità, scalabilità e stabilità [1].
L'introduzione di diversi livelli di astrazione di rete coniugata con la virtualizzazione integrata delle risorse IT e di rete potrebbe permettere di estendere alle rete i paradigmi e gli strumenti (opportunamente adeguati) oggi utilizzati all'interno dei Data Center: ad esempio uno dei vantaggi più

concreti potrebbe essere introdurre nella rete dell'Operatore di un livello di flessibilità, ad oggi impensato, abilitandone la programmabilità e permettendo di allocare ed invocare funzionalità virtualizzate di rete a seconda delle esigenze e nei punti più opportuni; a questo si aggiungerebbe la possibilità di realizzare ridondanze (ad es. over-provisioning della connettività virtuale) secondo schemi ad oggi impossibili, e la capacità rinnovare le piattaforme hardware con limitato (o addirittura senza) impatto sui servizi. Inoltre, potrebbe diventare particolarmente significativo valutare le potenziali opportunità offerte dalla declinazione del paradigma SDN all'edge della rete (ad esempio, anche fino a casa dell'Utente) nell'ottica di sviluppare nuovi servizi ICT e nuovi modelli di business.
Infine è utile rimarcare che il tema SDN, a dispetto dell'enfasi e delle aspettative di cui è oggetto in questo momento, sebbene suffragate da indubbie potenzialità dell'idea, necessita ancora di progressi nel processo di standardizzazione e di raggiungere una piena maturità e disponibilità tecnologica per potere essere seriamente considerato per un dispiegamento in campo. A questo proposito, quindi, anche gli esempi di attività internazionali sull'argomento, riportati nel Capitolo 2, stanno a testimoniare soprattutto lo sforzo di elaborare una vision e di verificarne le potenzialità attraverso attività esplorative e "proof of concept".

2 Il paradigma Software Defined Networking

SDN sta diventando una 'keyword' imprescindibile per le architetture di rete evoluta anche se ad oggi manca di fatto una visione comune di quali siano gli obiettivi e gli elementi che identificano questo nuovo paradigma.
Secondo Scott Shenker [2] e Nick McKeown [3] l'obiettivo principale di SDN è ristrutturare l'architettura di networking, introducendo opportuni livelli di astrazione in grado di operare una trasformazione simile a quanto già avvenuto nel campo delle architetture elaborative. Nell'ambito del computing infatti ormai da molto tempo i programmatori sono in grado di implementare sistemi complessi senza dovere gestire le tecnicalità dei singoli dispositivi coinvolti o interagire in linguaggio macchina, il tutto proprio grazie all'introduzione di opportuni livelli di astrazione nell'architettura.
Questa visione, decisamente ambiziosa che propone un cambiamento radicale nelle reti, non è messa in discussione, ma spesso da molti è erroneamente identificata con aspetti specifici che probabilmente hanno un impatto decisamente più limitato. Ad esempio alcuni identificano SDN con il problema della separazione del piano di controllo dagli apparati di rete e della sua centralizzazione, altri si focalizzano sull'apertura di interfacce di controllo sui router attuali: entrambe queste innovazioni sono solo componenti di una soluzione complessiva che permette l'interazione delle applicazioni con la rete in modo sufficientemente semplice da stimolare una vasta produzione di nuove applicazioni. Evidenza di questo fatto è che soluzioni tecniche per questi due problemi specifici esistono da anni (ad esempio i lavori in IETF sul protocollo ForCES, che permette la separazione tra piano di controllo e piano di forwarding, è RFC già dal 2010 [4]; Juniper mette a disposizione da anni API ed SDK sui propri router), ma non hanno trovato sino ad oggi significativo impiego.
L'aspetto su cui si stanno da anni concentrando le attività è la definizione del protocollo OF (*OpenFlow*), sviluppato inizialmente a livello accademico ed ora adottato anche dalla ONF (*Open Networking Foundation*) come principale ipotesi di lavoro e fondamento del lavoro di standardizzazione.

2.1 Il protocollo OpenFlow

Il protocollo OpenFlow si ritiene che rappresenti un fattore abilitante, anche se da solo ovviamente non sufficiente, per realizzare la trasformazione verso i concetti di rete flessibile e programmabile. È inoltre doveroso aggiungere che la sua definizione non è al momento consolidata, ma è ancora suscettibile di evoluzioni e perfezionamenti
L'interfaccia realizzata da OpenFlow si colloca al livello più basso di astrazione previsto dall'architettura SDN, essa permette infatti di svincolarsi dall'hardware di forwarding dei pacchetti. In questo senso, uno degli aspetti fondamentali, che sta alla base dell'attività di specifica avviata da OpenFlow, consiste nella definizione di un modello standard dell'hardware di forwarding dei pacchetti che costituisce il nucleo dei diversi dispositivi di networking. Scopo del protocollo OpenFlow è quindi, in questo senso, quello di presentare all'esterno un modello di nodo generale e unificato, rendendo gli strati più alti dell'architettura di rete SDN indipendenti dall'implementa-

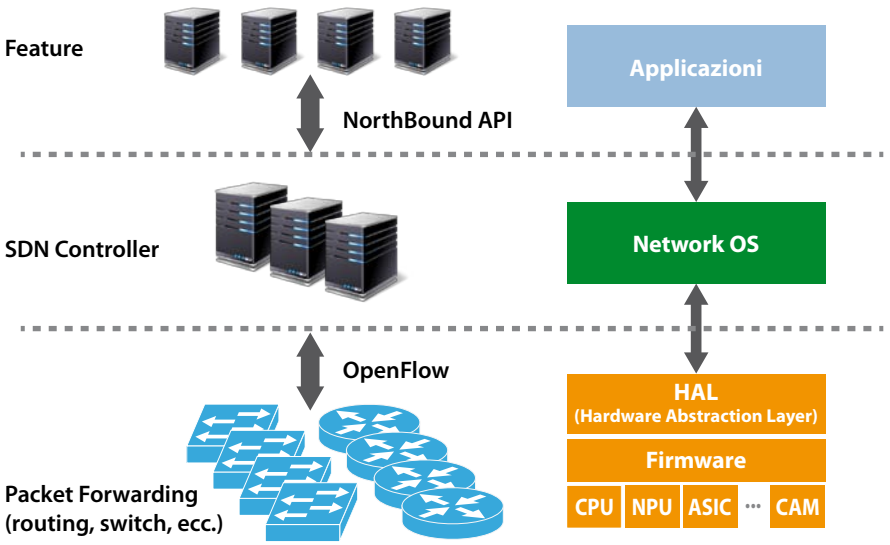


Figura 1 - Rappresentazione dell'architettura di rete SDN

zione del particolare vendor delle tecnologie impiegate nel piano di forwarding.

Risalendo alle origini della proposta, l'idea di base di OpenFlow è quella di rendere programmabili in senso generale le tabelle di classificazione ed instradamento dei pacchetti presenti negli apparati di networking (siano essi router o switch); in questo modo il contenuto (le cosiddette entry) può essere configurato dalle applicazioni, per il tramite di un piano di controllo esterno al dispositivo, mediante un'opportuna interfaccia. Quest'ultima, costituita appunto dal protocollo OpenFlow, permette di definirne in modo flessibile il contenuto, in funzione della logica di servizio da realizzare.

Le tabelle utilizzate per la classificazione del traffico a bordo dei router sono generalmente in grado di operare a velocità di linea e vengono sfruttate anche per realizzare funzioni aggiuntive al forwarding di base, quali: firewall, NAT, QoS, ecc. Nel modello del nodo OpenFlow, queste tabelle vengono denominate *flow table* e specificano le regole di trattamento associate a ciascun flusso di traffico. L'entità base con cui viene rappresentato e gestito il traffico in OpenFlow è per l'appunto il flusso di pacchetti (*flow*); quest'ultimo è definito da una regola di classificazione ottenuta specificando il contenuto di opportuni campi dell'intestazione tramite una *entry* della *flow table*. Il protocollo OpenFlow permette quindi al piano di controllo di definire in modo flessibile e dinamico le regole di instradamento e trattamento dei pacchetti appartenenti ai diversi flussi di traffico.

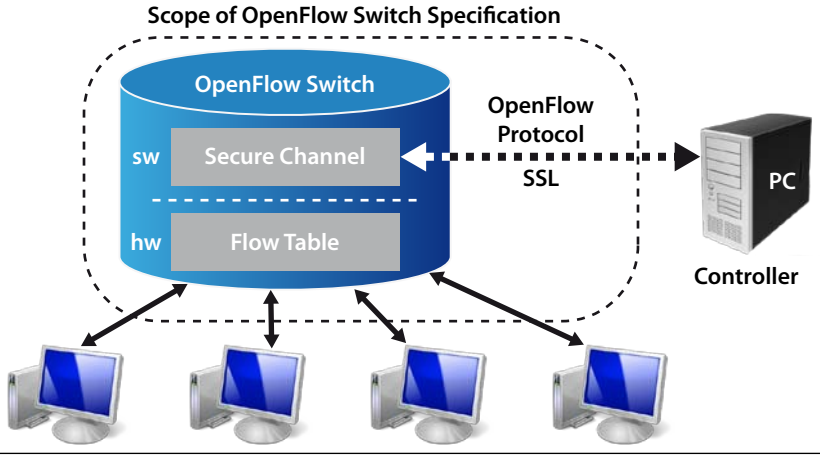
Normalmente l'implementazione delle tabelle di classificazione dei pacchetti, che presiedono alla definizione dei flussi e alla relative regole di inoltro, è una caratteristica proprietaria del particolare apparato di networking. Per superare questo modello, OpenFlow mira ad individuare e specificare ed a rendere accessibili attraverso il protocollo, un insieme di funzioni supportate dalla maggior parte dei router o switch commerciali. L'obiettivo principale consiste quindi nel definire un modello astratto dell'elemento che esegue il forwarding dei pacchetti, rendendolo programmabile attraverso un interfaccia aperta e standard.

Uno schema molto semplificato dell'architettura OpenFlow è riportato nella Figura 2 seguente. In particolare lo schema di principio fa riferimento alla versione base dell'architettura, come definita dalla specifica OpenFlow nella versione 1.0.

I principali elementi funzionali del sistema, come si osserva dalla figura, sono i seguenti:

1) una tabella (*Flow Table*) i cui elementi (*entry*) definiscono i

Figura 2 - Schema di principio di un nodo OpenFlow



flussi e le azioni associate, determinando il trattamento da applicare ai pacchetti appartenenti ai flussi stessi;
2) un canale sicuro (*Secure Channel*) tra il nodo ed un processo di controllo remoto (controller), che consente lo scambio di pacchetti e messaggi di comando;
3) il protocollo *OpenFlow*, come interfaccia di comunicazione standard ed aperta tra il nodo ed il controller.

In linea di principio si può distinguere un nodo nativo OpenFlow, in grado di svolgere tutte le sue funzioni unicamente tramite programmazione remota da parte di un controllore ed un nodo tradizionale (es. router o switch commerciale), che sia anche in grado di ricevere ed interpretare comandi mediante OpenFlow. Nel seguito, indicheremo questo tipo di apparati con il termine nodo OpenFlow ibrido, in uso in ambito ONF, ente incaricato dello sviluppo degli standard su SDN/OpenFlow. I nodi ibridi rappresentano infatti lo scenario più realistico, nell'ipotesi di un'introduzione in rete della tecnologia.

Gli elementi contenuti nella Flow Table (le versioni più recenti della specifica prevedono la presenza di più tabelle in cascata) specificano come devono essere gestiti i diversi flussi di pacchetti. Le azioni di base, che il nodo deve OpenFlow deve supportare sono:
1) inoltrare il pacchetto verso una determinata porta di uscita,
2) incapsulare il pacchetto e spedirlo al controller attraverso l'interfaccia di comunicazione; tipicamente questa azione viene applicata al primo pacchetto di un nuovo flusso, il controller potrà poi decidere di configurare un nuovo entry nella tabella per specificare il trattamento dei pacchetti successivi; infine, nulla vieta, in casi particolari, di inviare tutti i pacchetti di un flusso verso il controller per la loro elaborazione;
3) scartare i pacchetti appartenenti al flusso;
4) trattare i pacchetti secondo le normali procedure di forwarding del nodo (nel caso di nodi OpenFlow ibridi).

2.2 Gli sviluppi recenti

La definizione dell'architettura OpenFlow ha subito delle evoluzioni rispetto alla versione iniziale da quando è stata fatto oggetto di studio e specifica da parte di ONF ed ha visto parallelamente un sempre maggiore coinvolgimento da parte dell'industria. A differenza della semplice schematizzazione discussa in precedenza a titolo esemplificativo, il modello di nodo OF attualmente definito dalla versione più recente della specifica (Versione 1.3) prevede la presenza di una sequenza di *flow table* in cascata, al fine di consentire una maggiore flessibilità nel trattamento dei pacchetti.

Infine è bene notare che, se l'introduzione di un livello di interfacciamento aperto verso i dispositivi di forwarding rimane uno dei capisaldi dell'architettura SDN, comincia ad emergere, in seno alla comunità scientifica e industriale che lavora alla definizione di OpenFlow, l'idea che l'astrazione supportata dalle versioni di OpenFlow attualmente in corso di specifica (versioni 1.x) sia soggetta a limiti che possono ostacolare la piena applicabilità della tecnologia.

Il principale limite identificato, all'interno della stessa ONF, per il modello corrente, consiste nel fatto che la rappresentazione semplificata su cui si basa attualmente OpenFlow non è in grado di veicolare agevolmente le informazioni sulla logica di forwarding che l'applicazione intende implementare, rendendo difficile se non talora impossibile fare leva sulle funzionalità messe a disposizione dall'hardware. Anche nel modello corrente, la rappresentazione consiste in una sequenza di tabelle e obbliga l'applicazione a ragionare a basso livello, mancando in definitiva la possibilità di esprimere in termini concisi il comportamento (il cosiddetto *forwarding behavior*) end-to-end desiderato.

Questa è la ragione principale per cui in ambito ONF è stato istituito di recente un nuovo gruppo di lavoro incaricato della definizione del modello astratto del piano di forwarding del nodo. Sarà poi compito di un opportuno HAL (*Hardware Abstraction Layer*) presentare ai livelli superiori tale astrazione (Figura 1), interpretando i comandi provenienti dal controllo. Naturalmente, la definizione del livello HAL non rientra tra i compiti di ONF; trattandosi di un aspetto specifico legato alle diverse implementazioni tecnologiche dei vendor, spetta a questi ultimi sviluppare tale strato di adattamento sul loro hardware proprietario.

Parallelamente all'iniziativa di revisione di OpenFlow scaturita da ONF, si segnalano altre critiche mosse al modello corrente da parte di esponenti della comunità scientifica. Ad esempio, secondo un parere autorevole [5], il protocollo OF, così com'è definito oggi, sarebbe troppo complesso per un

impiego nel core della rete, a scapito della sua scalabilità, ed invece troppo semplificato per soddisfare i requisiti di maggiore ricchezza funzionale tipici dell'edge di servizio. Da questa critica consegue la proposta di differenziare le versioni del protocollo a seconda dell'ambito di applicazione; suggerendo un'implementazione software della versione destinata a controllare i nodi edge della rete, per una maggiore flessibilità ed evoluzione della tecnologia, mantenendo invece un profilo molto semplice per il core della rete a beneficio della scalabilità e del costo ma anche della compatibilità in ambiente multi-vendor.

2.3 Il livello dei controller come sistema operativo di rete

Come si nota nella Figura 1, uno degli elementi che compongono l'architettura SDN è costituito dallo strato di cui fanno parte i controller.
Vale la pena ricordare che tradizionalmente nelle reti a pacchetto le funzionalità del piano di controllo e quelle del piano dati sono strettamente accoppiate; ossia che sono gli stessi dispositivi che effettuano il forwarding del traffico a decidere come trattare e dove inoltrare i pacchetti.
Da questo punto di vista, il paradigma SDN/OpenFlow introduce invece, come già accennato, un principio di disaccoppiamento tra piano di controllo e di forwarding. L'approccio adottato prevede di scorporare le funzionalità del piano di controllo ed assegnarle ad elementi dedicati. Ciascuno dei controller, a sua volta, gestisce uno o più nodi che effettuano il forwarding dei pacchetti. Uno degli aspetti salienti della visione SDN è quindi la possibilità di disegnare le applicazioni considerando la rete come se fosse governata da un piano di controllo concettualmente centralizzato, invece che con un sistema complesso e distribuito. Le applicazioni possono quindi implementare le loro logiche di controllo astraendo dalla complessità fisica della rete, sarà compito dei controller presentare una vista unica, globale e logicamente centralizzata, gestendo la topologia fisica della rete e la distribuzione delle informazioni di stato necessarie ad implementare le logiche di servizio.
Lo strato di controllo dell'architettura SDN sarà generalmente composto da un ecosistema di moduli software, di cui il principale nucleo è costituito dal controller. Sebbene non vi sia una definizione completamente univoca e universalmente condivisa di controller, un punto fermo è rappresentato dal fatto che esso ha il compito di terminare l'interfaccia OpenFlow (vedi Figura 1). Inoltre questo modulo offre un'interfaccia di programmazione verso le applicazioni, siano esse interne o esterne allo strato di controllo stesso. È quella che in ambito ONF viene convenzionalmente indicata con il termine di "northbound" API, mediante la quale le applicazioni
possono fare uso delle funzionalità offerte dal controller. Questo strato dell'architettura SDN può essere visto più in generale come l'analogo di un sistema operativo di rete (Network OS), come tale deve offrire varie funzionalità di supporto, quali fra l'altro la gestione della comunicazione fra moduli e l'aggiunta di nuove componenti.
Se l'astrazione presentata dall'architettura SDN alle applicazioni è quella di un controllore logicamente centralizzato, dal punto di vista realizzativo sono possibili diverse scelte progettuali. In linea di principio, quella di un elemento di controllo fisicamente centralizzato è un opzione possibile, e forse adatta per ambiti molto circoscritti, quali una rete sperimentale o un campus universitario, ma certamente non adeguata per il dispiegamento in reti di produzione. La centralizzazione di un elemento così critico per il funzionamento della rete comporta infatti evidenti limiti dal punto di vista di: prestazioni, in particolare tempi di risposta, a causa dei ritardi di propagazione dovuti alle distanze geografiche, affidabilità, in termini di raggiungibilità e disponibilità dell'elemento e scalabilità. Questo significa che l'architettura del controllo dovrà in generale essere composta da elementi fisicamente replicati e distribuiti, ma capaci di comportarsi nel complesso come un piano di controllo logicamente centralizzato. Naturalmente un certo grado di distribuzione dei controller richiede la gestione delle usuali problematiche di consistenza delle informazioni di stato tipiche dei sistemi distribuiti. I vari controller dovranno poi essere in grado di dialogare tra loro, attraverso opportune interfacce "orizzontali", in particolare nel caso in cui essi appartengano a domini di rete differenti dal punto di vista geografico e amministrativo.
Quindi, riassumendo, dal punto di vista dell'organizzazione del piano di controllo la vera novità introdotta da SDN non sta nella sua centralizzazione, peraltro logica, bensì nella possibilità di svincolarne la topologia da quella dei nodi di rete che effettuano il forwarding del traffico.

2.4 La virtualizzazione di rete

Un ulteriore ingrediente che è parte integrante della visione SDN relativamente allo strato di Network OS è rappresentato dalla virtualizzazione di rete (si veda anche il riquadro di testo su questo argomento). Infatti, analogamente a come, nel mondo del computing, l'introduzione delle tecnologie di virtualizzazione ha consentito partizionare e condividere le risorse elaborative hardware, sotto forma di macchine virtuali, tra più istanze di sistemi operativi, si può pensare di applicare dei principi di virtualizzazione (*slicing*) anche alle risorse di rete.
L'obiettivo della virtualizzazione di rete, nel contesto OpenFlow/SDN, consiste dunque nel ricavare delle partizioni virtuali dell'infrastruttura di rete fisica, in modo da permettere a più istanze di controllo e rispettive applicazioni di utilizzare la *slice* di rete assegnata, come se fosse a tutti gli effetti dedicata e completamente isolata dalle altre reti virtuali che insistono sulla medesima infrastruttura hardware. Le tecniche di virtualizzazione dovrebbero consentire ai diversi soggetti che condividono l'infrastruttura ed alle relative applicazioni di implementare protocolli e schemi di indirizzamento totalmente indipendenti.
In questo senso, già oggi nell'ambito dei data center e delle architetture di cloud computing, le tecnologie di virtualizzazione, come ad esempio gli switch virtualizzati (vSwitch) realizzati all'interno dei moduli di gestione delle macchine virtuali, i cosiddetti *hypervisor*, giocano un ruolo chiave nell'evoluzione di queste soluzioni e rappresentano una realtà ormai affermata dal punto vista commerciale.
Naturalmente diversi e più articolati sono i requisiti ed i problemi da affrontare per esportare le tecnologie di virtualizzazione anche nell'ambito delle reti di telecomunicazione geografiche, tuttavia vi sono segnali di una possibile evoluzione proprio in questa direzione.
Ad oggi, invece, le tecniche per supportare dei principi di virtualizzazione in un ambiente generico di rete sono ancora in fase di sviluppo e le implementazioni disponibili sono limitate. Si tratta sostanzialmente di strumenti destinati ad applicazioni in contesti sperimentali e di ricerca, come il software FlowVisor [6], sviluppato nell'ambito del framework OpenFlow. Come le tecnologie di *hypervisor* si situano tra l'hardware di computing ed il sistema operativo, infatti, il FlowVisor si colloca tra il controller OpenFlow ed il piano di forwarding, introducendo nell'architettura un meccanismo di virtualizzazione (*slicing*) di rete.
Il FlowVisor si incarica di garantire che le diverse istanze di controllo siano in grado di vedere e gestire solo la *slice* a loro assegnata, assicurandone l'isolamento dalle altre *slice* configurate in rete. Da un punto di vista implementativo, il FlowVisor si inserisce in modo trasparente, in modalità *proxy*, tra l'interfaccia OpenFlow ed il controller, intercettando ed elaborando i messaggi scambiati. Il FlowVisor costituisce un'implementazione ancora embrionale dei principi di virtualizzazione e presenta alcune limitazioni, per esempio le topologie virtuali possono essere costituite solo da sottoinsiemi della topologia fisica.
Tuttavia si può sicuramente affermare che le tecnologie di virtualizzazione della rete costituiscono in prospettiva una componente qualificante dell'architettura SDN e potenzialmente in grado, quando mature, di abilitare nuovi ed efficaci modelli di condivisione delle infrastrutture di rete.

3 Alcuni scenari e possibili vantaggi per l'Operatore

L'interesse per il paradigma SDN è anche testimoniato dal crescente numero di iniziative internazionali di carattere industriale e da una serie di attività di sviluppo specifiche, prototipazione e prestandardizzazione, nonché dal sorgere di start-up.
In sintesi, se da un parte il paradigma SDN potrebbe permettere di attuare più facilmente azioni di configurazione e ottimizzazione delle risorse di rete e dall'altra parte, l'introduzione di diversi livelli di astrazione di rete coniugata con la virtualizzazione integrata delle risorse IT e di rete potrebbe permettere di estendere alle rete i paradigmi attualmente utilizzati all'interno dei Data Center.
La migrazione dell'intelligenza del piano di controllo dagli apparati ad un sistema logicamente centralizzati potrebbe favorire lo sviluppo di una nuova generazione di software router ad alte prestazioni (100 o più Gbps) basati su hardware standard. Il throughput di un router è fondamentalmente limitato dal routing processing (che detta il tradeoff tra numero di porte e relative banda per connessione): il paradigma SDN potrebbe permettere il superamento di questa limitazione, rendendo possibile attuare in rete delle ridondanze (ad es. over-provisioning della connettività virtuale) secondo schemi ad oggi impossibili, o introducendo un alto livello

di flessibilità e programmazione nell'utilizzo delle risorse di rete.
Nel seguito di riportano alcuni esempi di attività internazionali di ricerca e sviluppo.
Il progetto FP7 SPARC "Split architecture carrier class networks", finanziato dalla Comunità Europea e coordinato da Deutsche Telekom, ha portato allo sviluppo e sperimentazione di nodi di rete basati sul disaccoppiamento dei piani di controllo e forwarding. I prototipi di nodo sviluppati nel progetto SPARC si basano su piattaforme hardware fornite da Cavium, Broadcom ed Emerson. Inoltre, in linea con questi sviluppi, Deutsche Telekom sta sperimentando l'utilizzo di soluzioni alla OpenFlow/SDN nell'ambito dello sviluppo della rete greenfield TeraStream dispiegata in Croazia (figura 3). L'architettura punta a sfruttare la potenza di calcolo dei Data Centre dell'Operatore (attestati ai nodi R2) per la centralizzazione di alcune logiche di controllo di rete e per l'ottimizzazione di alcuni processi di gestione.

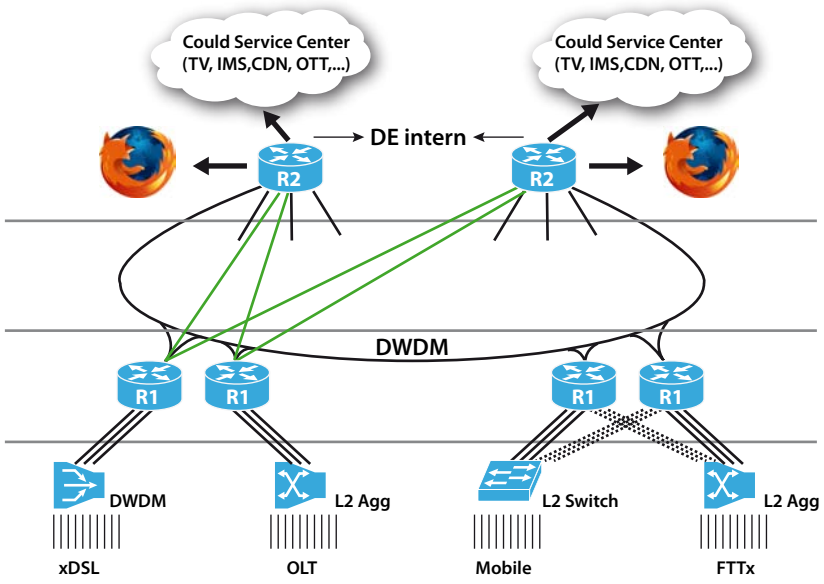
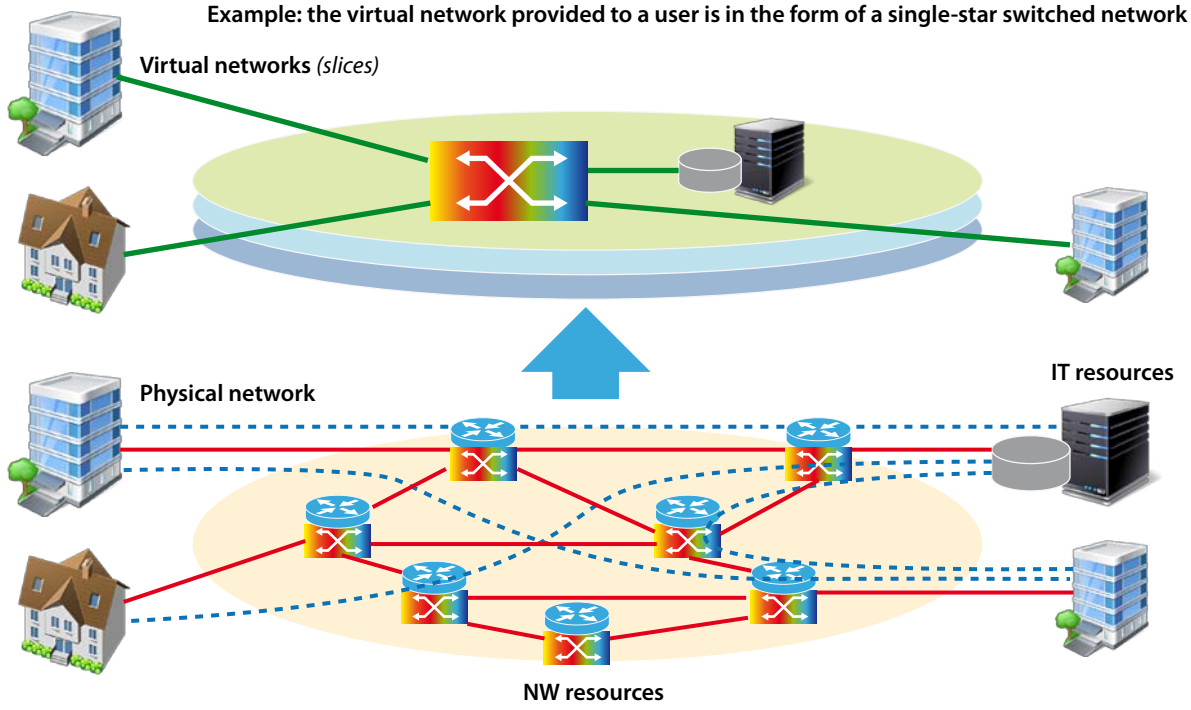


Figura 3 – TeraStream Architecture *(Fonte DT)*

Virtualizzazione, programmabilità e integrazione delle risorse di rete e IT sono le caratteristiche principali della visione di NTT per il futuro della rete. L'astrazione

Figura 4 – Visione di NTT sulla rete del futuro: astrazione e integrazione di risorse di rete e IT *(Fonte NTT)*



virtuale delle risorse permetterebbe l'esercizio di una molteplicità di reti logiche (overlay) coesistenti ma separate sulla stessa infrastruttura fisica.
La programmabilità ai diversi livelli di rete (con interfacce standard) aumenterebbe ulteriormente la flessibilità nella fornitura di servizi (Figura 4).
In figura 5 è illustrato un esempio di scenario di utilizzo di SDN per l'interconnessione di data centre in corso di sviluppo in Telefonica I+D.
Le applicazioni (attraverso l'SDN Orchestrator) potrebbero riservare le risorse IT e di rete in maniera integrata, secondo i requisiti richiesti e per il tempo necessario ad eseguire determinati task, o per attuare migrazioni tra diversi server. È il modello del sistema operativo di rete.
Un modello molto simile è il Dynamic Enterprise Cloud di Verizon (figura 6), dove nuovamente ricorrono i temi della virtualizzazione, programmabilità e integrazione delle risorse di rete e IT.

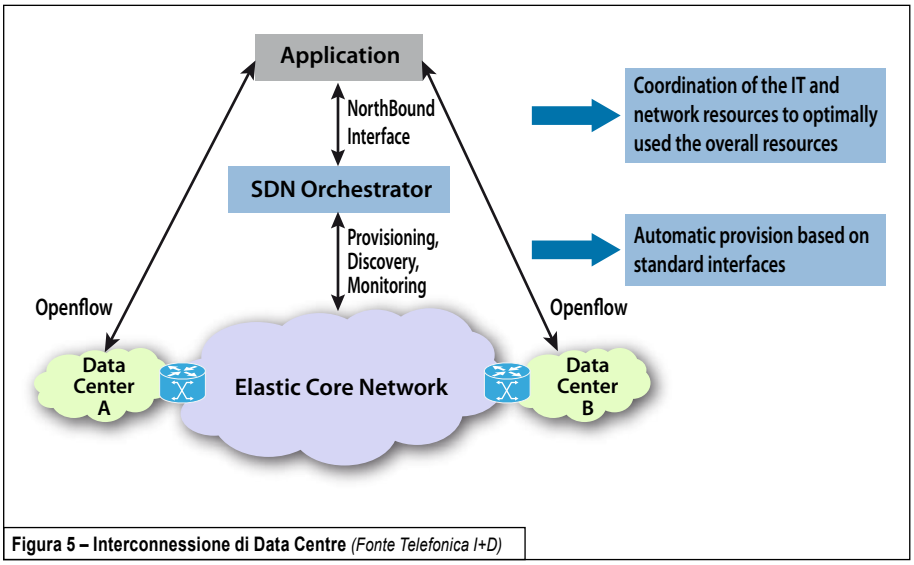
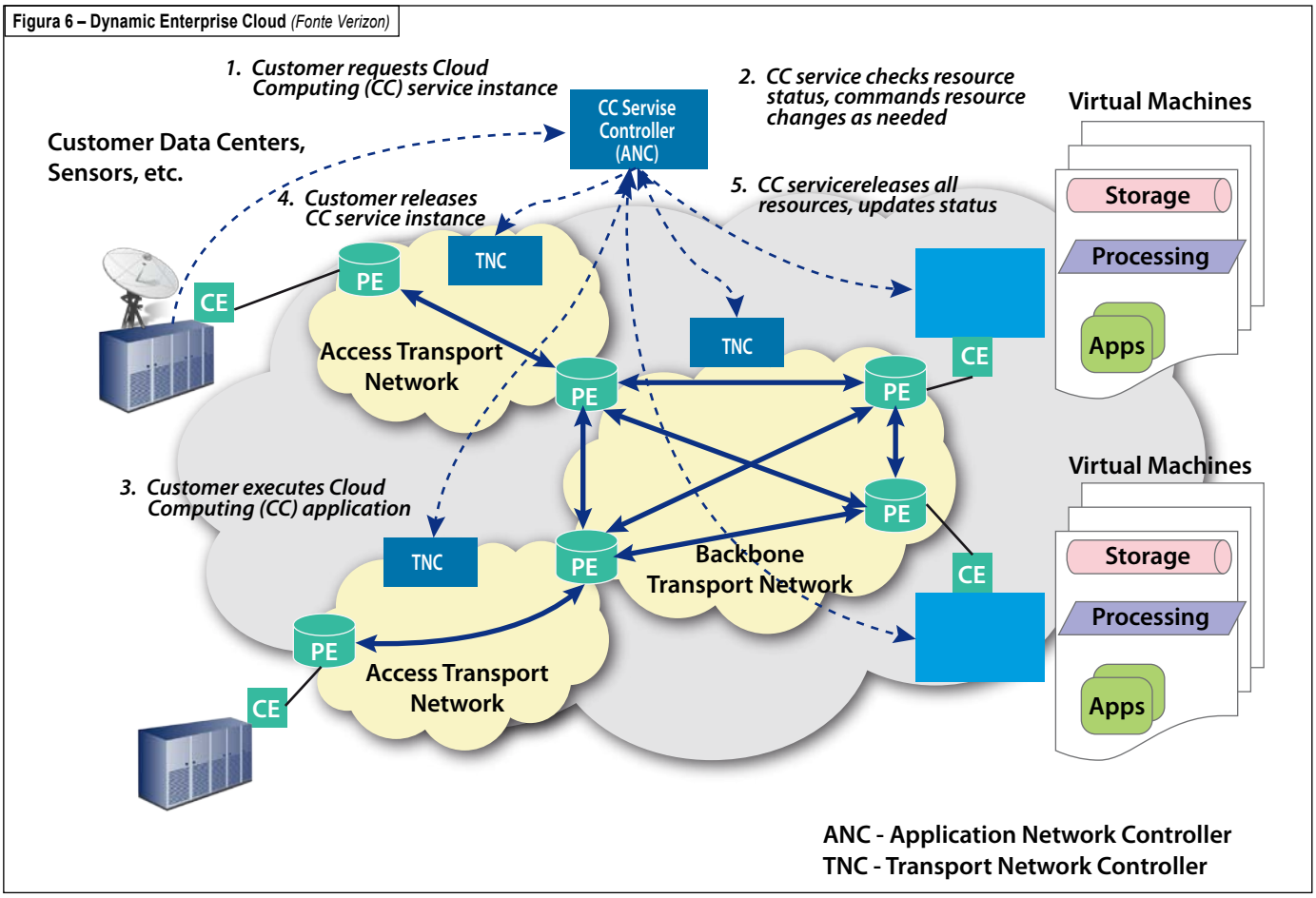


Figura 5 – Interconnessione di Data Centre *(Fonte Telefonica I+D)*

Figura 6 – Dynamic Enterprise Cloud *(Fonte Verizon)*



4 Posizionamento dei Vendor

L'architettura SDN ha mostrato la capacità di valicare i confini della ricerca accademica, all'interno della quale ha avuto origine il protocollo OpenFlow, e di affermarsi concretamente nell'ambito dell'industria come paradigma emergente di architettura di rete. Come ogni soluzione potenzialmente in grado di portare trasformazioni anche significative nel comparto industriale di riferimento, il paradigma SDN ha prodotto reazioni diversificate da parte dei soggetti del settore, ed in particolare dei vendor. Intendiamo riferirci qui in primo luogo ai vendor presenti nel segmento di mercato delle piattaforme di rete per i service provider, senza peraltro trascurare ciò che avviene in settori adiacenti, le soluzioni di networking per le reti enterprise e i data center. Per cominciare dalle realtà più pronte a muoversi nel mercato che le nuove opportunità tecnologiche sono in grado di creare, partiamo dal caso delle numerose startup che sono nate per esplorare questo filone.
Fra tutte, possiamo citare Nicira e BigSwitch, entrambe fondate da esponenti di primo piano dell'università di Stanford che, lo ricordiamo, è stata l'incubatore delle attività su SDN/OpenFlow. Entrambe hanno orientato i loro sviluppi verso uno sbocco commerciale nel segmento delle soluzioni di networking per il cloud computing ed i data center. In questo ambito, OpenFlow viene impiegato come elemento nell'ambito di tecnologie di virtualizzazione di rete. In particolare, Nicira, che ha sviluppato la piattaforma NVP (*Network Virtualization Platform*) basata sulla tecnologia Open vSwitch, è stata recentemente acquisita da VMware, leader nelle tecnologie di virtualizzazione. Altro gruppo di vendor è rappresentato da costruttori come HP, IBM e Brocade, che dispongono di linee di prodotto basate su apparati di networking destinati in primo luogo al segmento delle reti enterprise/campus e dei data center. Questi vendor hanno già annunciato la disponibilità commerciale di prodotti in grado di supportare il protocollo OpenFlow; essi sono inoltre tra gli esponenti più attivi in questo momento all'interno dei gruppi di lavoro di ONF.
Anche i tradizionali fornitori di tecnologie per le reti dei service provider stanno seguendo con attenzione questo filone ed elaborando le strategie per incorporare elementi della soluzione SDN nei propri prodotti. Si segnalano ad esempio vendor come NEC che proprio facendo leva sul tema SDN/OpenFlow stanno cercando di riposizionarsi sul mercato nel settore del networking. NEC è uno dei vendor particolarmente coinvolti nelle attività in ONF ed ha annunciato una soluzione, l'architettura denominata ProgrammableFlow, che introduce principi di programmabilità e di virtualizzazione nei dispositivi di rete. Anche altri costruttori affermati di apparati di networking, come ad esempio Cisco e Juniper, hanno inserito il tema SDN all'interno delle loro strategie evolutive di prodotto.
Generalmente viene prevista l'apertura di interfacce che consentono in qualche misura la programmabilità dei nodi di rete; di solito l'interazione con la piattaforma avviene a livello più alto rispetto a quanto prevede il protocollo OpenFlow, e talvolta sono presenti aspetti proprietari. In sostanza, la filosofia che in questo momento alcuni vendor propongono consiste in un approccio che potremmo definire ibrido. Il controllo rimane fondamentalmente a bordo dei nodi e distribuito, ma le piattaforme si aprono per veicolare informazioni e accettare anche comandi di configurazione, relativamente ad alcuni aree funzionali, da elementi (controller) esterni.
In questo senso, per esempio, molti si stanno orientando ad esportare verso le applicazioni informazioni sulla topologia e lo stato dei nodi, anche se ciò contrasta con la filosofia SDN, che prevede invece di creare livelli di astrazione progressivi, in modo da rendere trasparente la complessità sottostante allo strato applicativo. In ogni caso, l'introduzione di principi di apertura rappresenta una novità per le strategie dei vendor incombenti.

5 Attività internazionali

La notevole trazione che il tema SDN sta esercitando sull'industria ha fatto sì che siano state avviate diverse iniziative per cercare di definire delle soluzioni condivise e dei protocolli interoperabili. Prima fra tutte è l'ONF. Si tratta di una iniziativa relativamente recente, costituitasi nel marzo dello scorso anno sotto forma di consorzio industriale non-profit.
La missione principale di ONF è di promuovere un nuovo approccio al networking ispirato ai principi dell'approccio SDN. In questa prospettiva, il consorzio ONF si è assunto come compito principale quello di presiedere allo sviluppo degli standard fondamentali al riguardo, tra i quali, in primo luogo,

Network Virtualization

Ormai da anni una delle tecnologie dominanti nei Data Center è quella di virtualizzazione: Hypervisor commerciali (e.g. VMware vSphere [7]) o Open Source (e.g. XEN [8]) permettono di utilizzare un server fisico per realizzare istanze di server virtuali gestiti da organizzazioni differenti e che utilizzino eventualmente sistemi operativi diversi.

Le tecnologie di virtualizzazione possono essere potenzialmente impiegate nel dominio di rete con due diversi obiettivi:

- utilizzo di una stessa infrastruttura fisica per realizzare più reti virtuali, appartenenti a soggetti diversi;
- utilizzo di una stessa piattaforma hardware per realizzare più funzionalità di rete.

Il primo obiettivo è in realtà già indirizzato da anni attraverso l'impiego della tecnologia MPLS per realizzare reti private virtuali (Virtual Private Network) di livello 2 o livello 3, che utilizzano piani di indirizzamento eventualmente sovrapposti; attraverso le soluzioni Carrier Supporting Carrier è anche possibile condividere una stessa infrastruttura tra più operatori. I vincoli delle soluzioni attuali sono da una parte l'impossibilità di applicare alle diverse partizioni di rete soluzioni completamente disgiunte (tutte le reti virtuali condividono la tecnologia IP/MPLS), dall'altra alcune limitazioni quali la "granularità'" con cui è possibile associare il traffico ad una data rete virtuale (tipicamente una porta logica e non un singolo flusso) o la limitata dinamicità.

Il secondo obiettivo si inserisce nel dibattito su un dilemma tecnologico con cui da anni devono confrontarsi i costruttori di apparati delle reti dati: realizzazione delle funzioni in hardware o in software. Negli ultimi 10-15 anni si è osservato una progressivo spostamento di funzionalità negli apparati (forwarding, accodamento differenziato, filtraggio del traffico, …) da una realizzazione in software ad una realizzazione in hardware. Questo ha permesso la realizzazione di apparati con prestazioni via via crescenti in grado di contrastare la crescita del traffico mantenendo i costi contenuti. Il perdurare di questa tendenza è tuttavia oggi non così scontato:

- lo sviluppo di ASIC in grado di supportare sempre nuove funzionalità a velocità più elevata è sempre più complesso e costoso e richiede tempi molto lunghi (centinaia di risorse coinvolte, tempi nell'ordine di 18-24 mesi);
- le nuove funzionalità introdotte all'interno delle reti sono sempre più complesse;
- l'ingegnerizzazione di nuovi servizi in tempi relativamente brevi richiederebbe un'elevata flessibilità delle macchine;
- lo sviluppo tecnologico di server e schede di rete non specializzati può contare su un mercato molto più ampio.

Sulla base di questi fattori viene quindi proposto un ritorno al passato con l'utilizzo di hardware non specializzato per realizzare funzionalità di rete: in par-

la specifica del protocollo OpenFlow. ONF è governata da un board costituito da rappresentanti di Deutsche Telekom, Facebook, Google, Microsoft, NTT, Verizon e Yahoo. Anche Telecom Italia è recentemente entrata a fare parte del consorzio ONF, che annovera ormai oltre 70 membri, tra cui diverse altre aziende di rilievo come: Cisco, HP, Juniper, IBM, Ericsson, VMware, NEC, Orange e Comcast.

L'attività di specifica di ONF è organizzata in gruppo di lavoro. L'aspetto centrale del lavoro di definizione degli standard è rappresentato attualmente da OpenFlow, sia in termini di modello dell'hardware di rete che di protocollo. A questo riguardo sono al momento attivi principalmente due gruppi di lavoro: il *WG Extensibility* ed il *WG Forwarding Abstractions*, di recente costituzione. Il primo ha il compito di evolvere la specifica attuale, individuando ed introducendo estensioni volte ad incrementarne la flessibilità e la ricchezza funzionale. Mentre il secondo si propone di ripensare il modello astratto del nodo con un duplice obiettivo; da un lato, renderne più agevole l'implementazione sull'hardware piuttosto eterogeneo, per caratteristiche ed architettura, dei dispositivi di rete; dall'altro, permettere alle applicazioni di controllo di esprimere in modo più conciso ed efficace il cosiddetto *forwarding behavior* desiderato, senza dover ragionare in termini di compilazione di un numero imprecisato di singole *flow table*. Accanto ai due gruppi di lavoro citati ve ne sono poi altri i cui compiti riguardano per esempio la definizione del modello dei nodi ibridi (*WG Hybrid*), affrontando le problematiche di consistenza nella gestione delle risorse derivanti dalla presenza di piani di controllo distinti, oppure gli aspetti di configurazione

ticolare ad esempio le funzionalità ad oggi fornite da appliance (NAT, Firewalling, Deep Packet Inspection), quelle fornite dagli apparati di Core Network Mobile (GGSN, EPC, MME) o quelle fornite dagli apparati di edge della rete fissa (BRAS, PE). In questo contesto le funzionalità diventano istanze SW associate a macchine virtuali che condividono una infrastruttura di server fisici distribuiti sulla rete o concentrati in Data Center di rete.

Un interrogativo rispetto a questa proposizione è sicuramente quello delle prestazioni: è scontato che l'impiego di hardware non specializzato non permetta di ottenere le stesse prestazioni attuali per realizzare alcune funzionalità, quindi le risorse computazionali necessarie saranno quantitativamente maggiori; l'interrogativo diventa quindi se il costo complessivo di una architettura di rete basata sul paradigma "Network Virtualization" sia interessante rispetto alle soluzioni attuali come effetto delle economie di scala sul hardware general purpose e della maggiore concorrenza sulle componenti software, o se sia più conveniente un approccio meno innovativo che cerchi di coniugare hardware specializzato con funzioni virtualizzate, o se semplicemente, nel medio periodo, questa proposizione non sia ancora sostenibile.

I vantaggi legati all'impiego di questa architettura vanno tuttavia al di là del semplice risparmio economico: come all'interno dei Data Center la soluzione abilita un livello di flessibilità ad oggi impensato, permettendo di accendere le funzionalità a seconda delle esigenze nei punti di della rete più opportuni, realizzare ridondanze secondo schemi ad oggi impossibili, rinnovare le piattaforme hardware senza impatti sui servizi, …

Per poter avere questi vantaggi ci si trova tuttavia ad affrontare una problematica analoga a quelle che sta ad oggi diventando una criticità per i Data Center: come realizzare in maniera semplice e scalabile la mobilità delle Virtual Machine (su cui in questo caso sono istanziate le funzionalità di rete) sia all'interno di un dato sito tra più macchine fisiche, sia in un contesto Cloud tra siti diversi. Da qui il legame tra SDN e Network Virtualization che per altri aspetti potrebbero essere considerati temi ortogonali: la separazione del piano di controllo dal forwarding o l'apertura di API verso lo strato applicativo non sono necessari per realizzare un'architettura in linea con gli obiettivi della Network Virtualization; potrebbero tuttavia essere un elemento utile per gestire la mobilità delle Virtual Machine nello stesso modo come soluzioni basate su Openflow sono ad oggi considerate all'interno dei Data Center per risolvere lo stesso problema ■

Per approfondimenti
http://www.blog.telecomfuturecentre.it/

(*Configuration & Management*), di validazione (*Testing & Interoperability*) e di definizione dei principi architetturali (*Architecture & Framework*). Infine, merita di essere menzionata l'attività sulla definizione della cosiddetta *Northbound Interface*, che ha l'obiettivo di definire l'interfaccia esposta dallo strato di Network OS verso le applicazioni.

Anche in IETF il tema SDN ha stimolato il confronto sul coinvolgimento e sul possibile ruolo dell'ente da sempre preposto alla definizione degli standard per il mondo Internet nell'ambito di questo nuovo filone, dando origine ad alcune prime iniziative al riguardo. È stata proposta la creazione di un gruppo di lavoro su SDN, ma la discussione che si è sviluppata non è per il momento approdata ad una decisione finale. Tenendo conto del mandato precipuo di IETF, il dibattito è stato per lo più centrato sull'effettiva necessità di definire nuovi protocolli per rispondere ad esigenze specifiche in questo contesto. La discussione ha affrontato tra l'altro il tema dell'eventuale ruolo di protocolli esistenti, derivanti da attività IETF pregresse, in relazione al nuovo filone SDN. È questo il caso del WG NETCONF, che ha prodotto soluzioni per semplificare la configurazione degli apparati, oppure del già citato WG ForCES [4], che ha specificato un protocollo per separare piano di controllo e forwarding dei nodi di rete. In questo quadro, sono emerse anche nuove proposte per l'apertura della piattaforma di rete, come nel caso dell' IRS (*Internet Routing System*), che mira a consentire alle applicazioni di interagire con il sistema di routing della rete. Se la discussione in ambito IETF rimane comunque ancora molto aperta su questi temi, nel contesto della IRTF (*Internet Research Task Force*),

altro ente sponsorizzato da IETF e Internet Society, il cui mandato è di promuovere e condurre la ricerca su temi di riconosciuta importanza per l'evoluzione di Internet, è stato ufficialmente creato di recente un gruppo di ricerca su SDN (SDNRG). Parallelamente a queste iniziative, si sta registrando un crescente interesse da parte di alcuni Operatori (ad es. Telefonica e Deutsche Telekom) per lo sviluppo (in open source) di un sistema operativo (kernel OS) di nodo SDN.
In definitiva, lo stato delle attività internazionali su un tema così attuale e di crescente rilievo come il Software Defined Networking è in continua evoluzione ed è verosimile che accanto alle iniziative già in atto altre vedano la luce nei mesi a venire.

Conclusioni

Il potenziale impatto del paradigma SDN sulle reti del futuro potrebbe essere duplice: mentre da una parte SDN potrebbe portare vantaggi economici per gli Operatori in termini di riduzione costi, dall'altra potrebbe abilitare lo sviluppo di nuovi ecosistemi di servizi ICT, che costituirebbero potenziali opportunità di sviluppo per gli Operatori a patto in cui questi riescano a ritagliarsi un ruolo e inserirsi in un modello di business vantaggioso.
L'introduzione di diversi livelli di astrazione di rete coniugata con la virtualizzazione integrata delle risorse IT e di rete potrebbe permettere di estendere alla rete i paradigmi attualmente utilizzati all'interno dei Data Center. Le soluzioni SDN potrebbe permettere alle applicazioni di acquisire una vista astratta della rete, come se fosse governata da un piano di controllo concettualmente centralizzato: diventerebbe quindi possibile implementare logiche di controllo astraendo dalla complessità fisica della molteplicità di apparati. Il cuore della SDN assomiglia dunque ad un ecosistema di moduli software di controllo, interagenti fra di loro e capaci di attuare più facilmente azioni di configurazione e ottimizzazione delle risorse di rete: d'altro canto questa stessa centralizzazione logica potrebbe avere dei punti critici, quali ad esempio livelli di prestazioni, affidabilità, scalabilità e stabilità.
L'interesse verso il paradigma SDN è testimoniato dal crescente numero di iniziative di carattere industriale e da una serie di attività di sviluppo specifiche, prototipazione e pre-standardizzazione, nonché dal sorgere di start-up di un certo rilievo. Se verrà dimostrata la fattibilità tecnologica delle reti SDN, a valle di un processo di standardizzazione, le ricadute sull'evoluzione della rete degli Operatori potrebbero essere particolarmente innovative ■

Bibliografia

[1] A. Manzalini, N. Crespi "*Mitigating Systemic Risks in Future Networks*" in IEEE CAMAD, Barcellona, Settembre 2012.
[2] S. Shenker, "*The Future of Networking, and the Past of Protocols*", Open Networking Summit 2011.
[3] N. McKeown, "*How SDN will Shape Networking*", Open Networking Summit 2011.
[4] IETF RFC 5860 "*Forwarding and Control Element Separation (ForCES) Protocol Specification*".
[5] M. Casado, T. Koponen, S. Shenker, A. Tootoonchian, "*Fabric: A Retrospective on Evolving SDN*", Workshop HotSDN, Agosto 2012.
[6] R. Sherwood, G. Gibb, K. Yap, G. Appenzeller, N. McKeown, G. Parulkar, "*FlowVisor: A Network Virtualization Layer*", Technical Report, 2009.
[7] *http://www.vmware.com/products/datacenter-virtualization/vsphere/overview.html*
[8] *http://www.xen.org*

antonio.manzalini@telecomitalia.it
mario.ullio@telecomitalia.it
vinicio.vercellone@telecomitalia.it

Antonio Manzalini
ingegnere elettronico con certificazione PMI, è entrato in Telecom Italia nel 1990 ed ha partecipato a diversi progetti di ricerca riguardanti reti di trasporto SDH ed ottico (WDM), occupando varie posizioni di responsabilità. Ha inoltre partecipato a molte attività di standardizzazione, guidando alcuni gruppi di lavoro in ITU-T. Attualmente si occupa di tecnologie, sistemi ed architetture di reti auto-adattative e capaci di auto-gestione (quali Autonomic/Cognitive Networking e Self Organizing Networks). Recentemente le sue attività comprendono l'analisi e definizione di scenari riguardanti il paradigma Software Defined Network. È autore di alcune decine di pubblicazioni, di un libro sulla sincronizzazione delle reti di telecomunicazioni e di cinque brevetti internazionali.

Mario Ullio
ingegnere elettronico nel 1990 è entrato in Azienda dove si è inizialmente occupato di architetture e servizi per reti metropolitane. Dal 1993 al 1995 ha contribuito alla standardizzazione di reti e servizi ATM e ha partecipato alla realizzazione della rete pilota ATM italiana e pan Europea. Dal 1996 ha seguito le sperimentazioni di soluzioni di accesso IP basate su ADSL e le successive fasi di deployment della rete e dei servizi commerciali per utenza residenziale e business. Dal 2003 al 2005 ha lavorato su soluzioni per reti metro Ethernet ed ha contribuito al primo deployment di OPM. Dal 2006 è responsabile di un progetto in cui è studiata l'evoluzione tecnologica e architetturale di medio/lungo termine delle reti IP.

Vinicio Vercellone
ingegnere elettronico, nel 1984 è entrato in Azienda. Da allora opera nel settore innovazione di Telecom Italia, dove ha inizialmente lavorato nel campo dello sviluppo della tecnica ATM e delle sue applicazioni. Dal 1997 al 2000 ha ricoperto anche l'incarico di docente presso il Politecnico di Torino. Ha contribuito ad attività e progetti di ricerca nel settore del networking IP ed MPLS e nell'offerta dei relativi servizi di rete. In questi ambiti è autore di numerosi brevetti internazionali e pubblicazioni. Attualmente svolge la sua attività nell'area Data Networks Innovation, dove contribuisce a progetti di ricerca su soluzioni di networking innovative per le reti dati, ambito nel quale si colloca la sua partecipazione al progetto europeo FP7 SAIL. Recentemente le sue attività di ricerca hanno abbracciato anche il filone emergente del Software Defined Networking.

Usa il tuo smartphone per visualizzare approfondimenti multimediali

INTERCONNESSIONE IP: IL PERCHÉ ED IL COME DI UN CAMBIAMENTO

Gianfranco Ciccarella, Daniele Roffinella

Lo sviluppo di Internet e la diffusione di paradigmi "IP centrici" evidenziano i limiti dei modelli tradizionali di Interconnessione IP. Affinché i Clienti finali possano accedere, con una adeguata QoE (*Quality of Experience*), ai contenuti ed alle applicazioni su Internet, sono necessari nuovi modelli di interconnessione, capaci di abilitare nuovi modelli di business e la valorizzazione degli "asset" sia degli operatori di telecomunicazioni (Clienti finali ed infrastruttura di rete), sia degli Over-The-Top (contenuti, applicazioni, global reach).

1 Introduzione

In un articolo del 2005 [1], due studiosi, inserendosi in analisi e dibattiti iniziati alcuni anni prima, predicevano che Internet avrebbe potuto andare incontro ad una crisi, e scrivevano: *We find that, due to a phenomenon we call **capacity paradox**, the [internet] industry's future development is overshadowed by "dark clouds"*. Analizzando gli andamenti del business del trasporto dati, veniva spiegato come, al crescere del traffico e della domanda di capacità di rete, le marginalità per gli operatori si riducano. Cinque anni più tardi, analisi come quella di ATKearney [2] hanno confermato come, a livello mondiale, l'incremento dei volumi di traffico IP si sia accompagnato ad una riduzione di margini per i soggetti (gli operatori di telecomunicazioni, i cosiddetti *Telco*) che sviluppano e gestiscono le reti, a causa della *disconnessione* in atto fra il trend dei costi (legati al traffico, e quindi crescenti) ed il trend dei ricavi (l'ARPU per gli accessi ad internet resta al più costante, ed il mercato dei transiti ha subito un processo di "commoditization"). Questo processo è strettamente connesso ad altri cambiamenti, altrettanto evidenti e significativi, fra cui:

- modifiche radicali nell'utilizzo delle reti fisse e mobili. Il traffico dati mobile ha superato quello voce già nel 2009 [3]. I nuovi modi di comunicare di persone ed aziende, con l'esplosione delle applicazioni e la diffusione di terminali sempre più sofisticati, causano non solo una continua crescita del traffico dati (+29% CAGR 2011-2016 Worldwide, da stime Cisco 2012), ma anche variazioni nel mix delle tipologie di traffico (la componente "video" nel traffico complessivo è stimata da Cisco pari al 55% del consumer internet nel 2016), e più stringenti requisiti di qualità nel trasporto del traffico.
- uno spostamento di valore dai Telco ai cosiddetti *OverTheTop-OTT* (nel biennio 2010-2011 la crescita media dei primi 5 OTT è stata oltre 30 volte quella dei primi 5 Telco). D'altra parte l'impegno degli OTT nella competizione fra loro, per accrescere il proprio footprint (aumentando sia il numero degli utilizzatori sia la frequenza degli accessi alle applicazioni sui propri host), ha determinato una crescente necessità di qualità nella connettività IP verso i Clienti finali.

Questi cambiamenti a loro volta hanno favorito la comparsa di nuovi attori, che hanno risposto alla domanda di migliore qualità ed efficienza nel trasporto dei flussi IP; alcuni "aggregatori" e soprattutto Global Content Delivery Network Providers (come Akamai, Limelight...) hanno conquistato un'importante spazio di mercato, e per svilupparsi ulteriormente cercano di installare i propri apparati sempre più in prossimità dei Clienti finali. La stessa esigenza di qualità, a fronte di una eccezionale crescita del traffico ha spinto aziende di distribuzione come Netflix a dotarsi di proprie soluzioni CDN (*Content Delivery Network*), e Google a realizzare una propria rete backbone a livello mondiale.

L'insieme dei cambiamenti nello scenario ha posto con evidenza il problema della Sostenibilità di Internet; Enti sia nazionali che sovranazionali stanno incontrando difficoltà ad identificare percorsi praticabili per lo sviluppo dell'Ultra Broadband fisso NGAN (*Next Generation Acces Network*) e mobile LTE (*Long Term Evolution*), mentre l'intero settore delle Telecomunicazioni deve affrontare situazioni di criticità.

La maggior parte del traffico IP è oggi originato da pochi grandi OTT mondiali (i cosiddetti HyperGiants) ed attraversa diversi punti di interconnessione tra cui quelli con i Telco prima di giungere ai Clienti finali; è quindi evidente che le modalità con cui sono realizzate le interconnessioni IP hanno un'importanza fondamentale sullo sviluppo dell'ecosistema complessivo e sul posizionamento dei Telco, che hanno ruoli diversi proprio in funzione del tipo di interconnessione realizzato. Questo fatto è testimoniato anche da diversi contenziosi (fra Telco e OTT, aggregatori/CDN Providers internazionali) che vengono risolti introducendo nuovi modelli di interconnessione, talvolta solo dopo l'intervento delle Autorità. Governi e regolatori mostrano di essere consapevoli del problema; controversie come quelle Netflix-Level3-Comcast in USA [4] o Orange-Cogent-Megaupload in Francia [5] sono riconosciuti casi emblematici (es. dal regolatore UK OFCOM [6], dal parlamento Francese [7], ecc...) di come l'inadeguatezza dei modelli di interconnessione tradizionali sia causa di problemi e di instabilità.

L'articolo, dopo aver richiamato i cambiamenti nello scenario ed analizzato i problemi principali causati dai modelli di interconnessione tradizionali, indica come deve evolvere l'interconnessione IP, descrivendo i benefici attesi dalle nuove Policy di interconnessione definite dal Gruppo Telecom Italia.

2 I cambiamenti dello scenario dell'Interconnessione IP

2.1 L'interconnessione IP - elementi di base

La "Big Internet" consiste di una pluralità di reti interconnesse. Ogni rete (chiamata Autonomous System – AS) è direttamente connessa con: 1) Clienti finali; 2) siti Web (contenenti informazioni, applicazioni, ecc....); 3) altre reti IP (cioè altri AS). Le modalità con cui i pacchetti dati attraversano i punti di interconnessione e vengono trasportati a destinazione, e le relazioni business fra i soggetti interconnessi, definiscono i possibili "modelli di interconnessione IP".

I modelli di interconnessione tradizionali sono basati su accordi di transito e peering (free oppure paid) e sulla terminazione del traffico in modalità best effort.

- Il *Transito IP* è un servizio a pagamento fornito da un operatore (*transit provider*), che garantisce l'accesso a qualunque indirizzo IP a livello mondiale attraverso la propria rete ed attraverso interconnessioni con altri operatori.
  Tipicamente i Servizi di Transito sono acquistati da Operatori locali/regionali (i "Domestic Telcos") per garantire ai propri Clienti finali la possibilità di accesso a qualunque Server/Terminale IP al mondo.
  Lo scambio di dati tra i due operatori che hanno una relazione dei Transito è spesso *sbilanciato* e l'operatore che ha chiesto il transito, e che normalmente riceve più traffico di quanto ne invii, paga l'operatore che vende il Servizio di Transito.
- Il *peering* è un accordo non oneroso (free peering) o con un costo (che è normalmente più basso del transito); solitamente si realizza tra pari (*peers*), cioè tra operatori che hanno bacini di siti Web e/o clienti sostanzialmente confrontabili e che trovano pertanto reciprocamente vantaggioso realizzare l'interconnessione.
  Il peering consente di avere accesso agli indirizzi IP dei siti Web e/o clienti dell'operatore con cui si fa l'accordo. In genere lo scambio di dati tra i due operatori è bilanciato, ma se si superano prefissate soglie di sbilanciamento l'operatore che invia più traffico paga la terminazione per il traffico oltre soglia.
  Il *paid peering* è un servizio a pagamento per terminare traffico su una rete (AS). In genere si utilizza per terminare traffico sui Clienti finali di un operatore.
  È importante precisare che una relazione di peering non è "transitiva": attraverso un peering possono transitare solo pacchetti "provenienti e destinati" ad indirizzi IP appartenenti ai due AS interconnessi.

I pacchetti IP che vengono "ricevuti" da un AS attraverso un punto di interconnessione sono normalmente trasportati dall'AS in modalità "best effort" [8], ossia "al meglio", compatibilmente con le condizioni puntuali del traffico

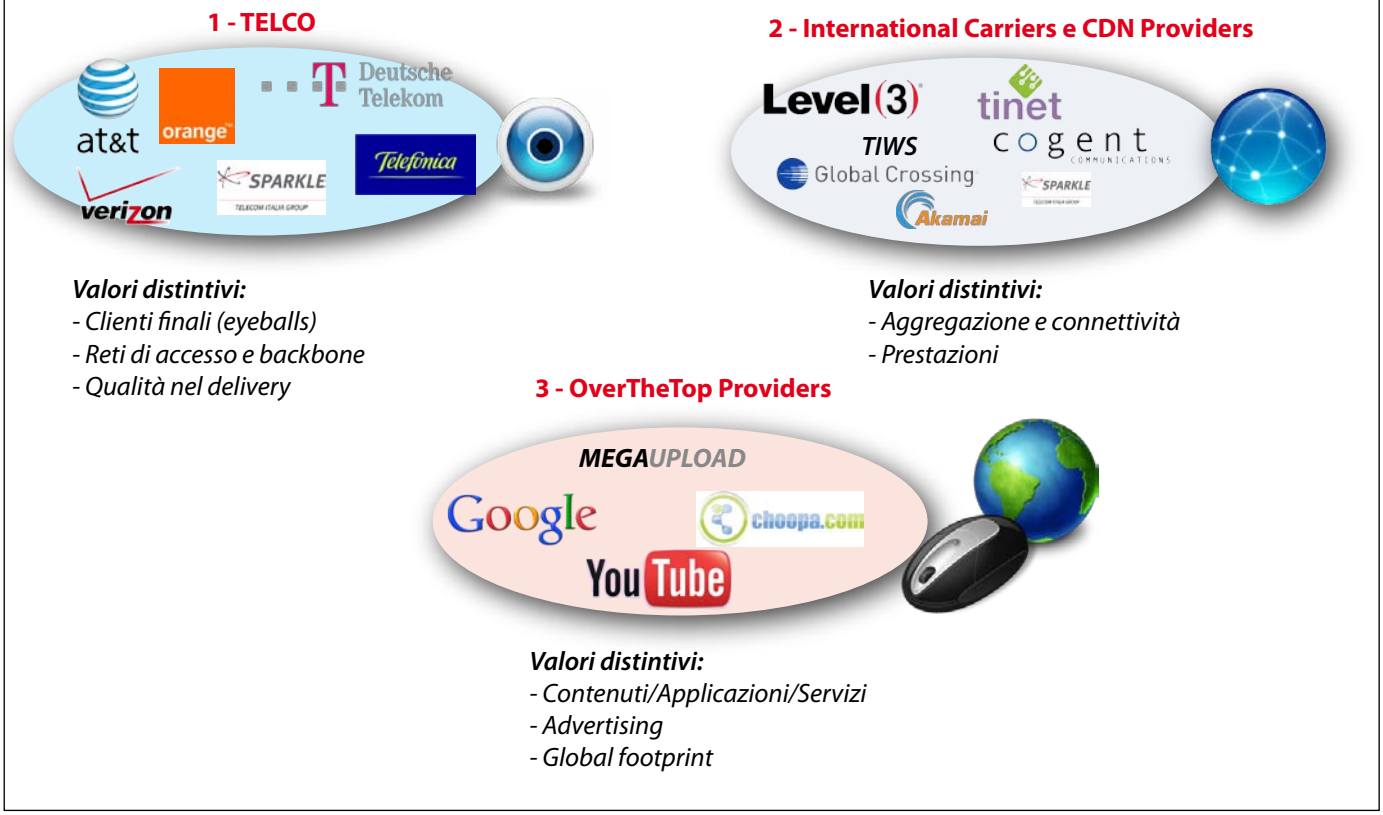
e della rete: non vi sono garanzie che i pacchetti dati arrivino a destinazione, oppure abbiano una certa priorità, o che siano trasportati con livelli minimi di qualità (ritardo, jitter, tasso di errore, duplicazioni, perdita, ecc...).
Oltre al best effort esistono altre modalità di trasporto dei pacchetti: si parla di servizi gestiti (managed services, o servizi specializzati o servizi prioritised). I servizi gestiti assicurano agli utenti il trasporto dei dati a destinazione con determinate caratteristiche e livelli di qualità. La Quality of Service (QoS) è definita mediante parametri tecnici relativi al trasporto dei pacchetti in rete, ed è legata alla Quality of Experience (QoE), che misura il livello di prestazione percepito nella fruizione di un servizio/applicazione [9].

I modelli di base sopra richiamati danno luogo a molte varianti e casistiche particolari. Ad esempio fra due AS ci possano essere allo stesso tempo un peering gratuito per flussi best-effort, ed un servizio a pagamento per un managed service con Qualità; se fra due AS vengono stabilite contemporaneamente relazioni sia di free peering sia di transito (offerto da un Tier1[1] solo sui suoi Clienti e non retribuito) si parla di accordo free-on-net; fra un Telco ed un OTT possono essere stabilite relazioni di peering gratuito oppure di paid peering, a seconda delle situazioni (e di quanto valore l'operatore e l' OTT sono disposti a riconoscersi a vicenda).
In tutti i casi, la realizzazione di uno specifico modello di interconnessione avviene mediante *negoziazione* fra i due soggetti direttamente coinvolti (rispettando criteri di non discriminazione, neutralità, trasparenza); l'esito della negoziazione riflette i rispettivi ruoli ed il valore che il traffico IP ha per ciascun soggetto (vedi Figura 1).

2.2 Lo sviluppo dei modelli di interconnessione tradizionali

I modelli di interconnessione IP tradizionali, basati su transito e peering e sulla terminazione del traffico in modalità best effort, si sono affermati in una precisa fase della "storia" di Internet (Figura 2): nella metà degli anni '90, la chiusura di NSF-Net[2] segna simbolicamente l'inizio dello sviluppo commerciale di Internet, e la crescita degli operatori Tier1, sui quali si determi-

Figura 1 – Interconnessione IP: gli attori principali



1 Le reti (AS) che possono raggiungere qualunque indirizzo IP senza dover acquistare Transiti da nessuno (ma che hanno solo relazioni di peering con altri AS, e vendono transiti a terzi), sono comunemente chiamate "Tier 1" (reti di primo livello).

2 La NSFNet (*National Science Foundation Network*), creata nel 1986 per collegare a 56Kbps i centri di supercomputing di università e centri di ricerca USA), crebbe sino a diventare un backbone a 45Mbps, sostituendo anche la famosa ARPANET. Nel 1995 le autorità eliminarono le residue restrizioni al trasporto di traffico commerciale su Internet; NSFNet fu chiusa e lasciò il campo ad una pluralità di reti gestiti da ISP (*Internet Service Providers*).

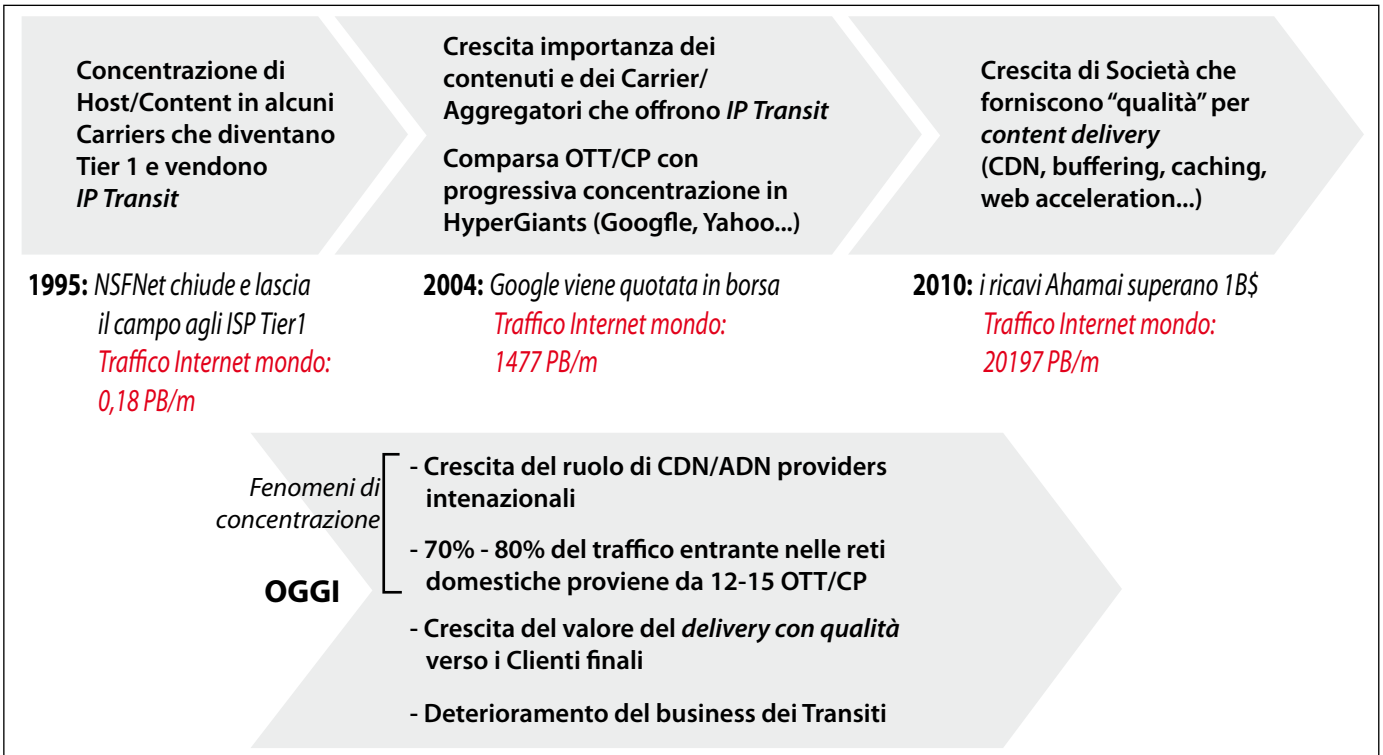
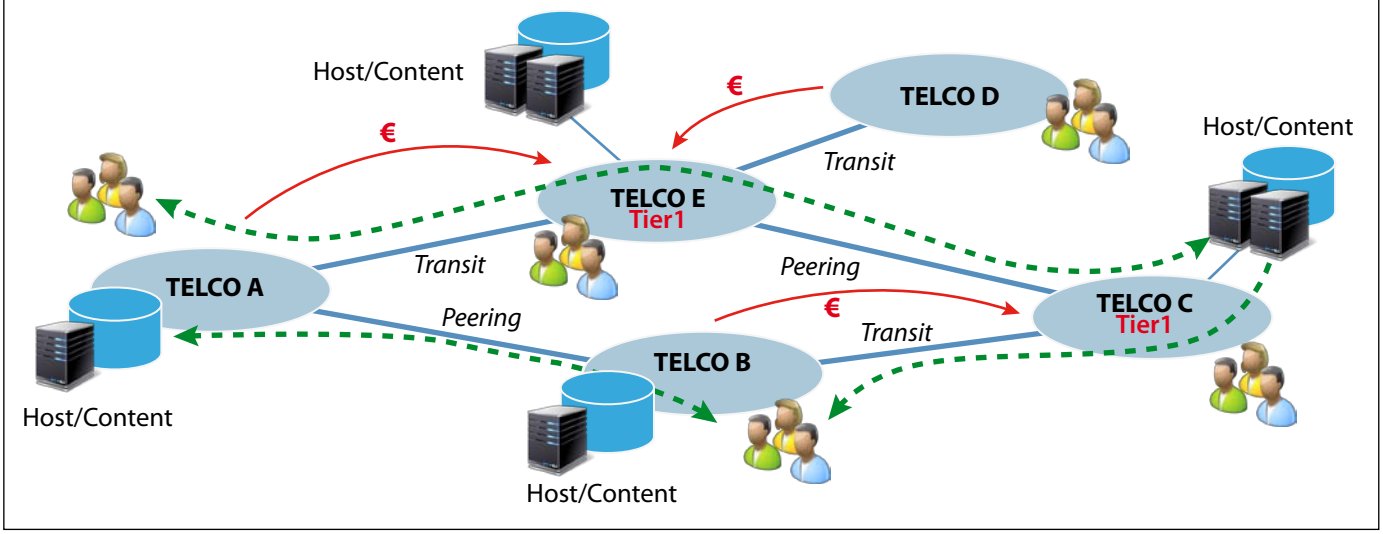


Figura 2 – I Cambiamenti nello scenario Internet

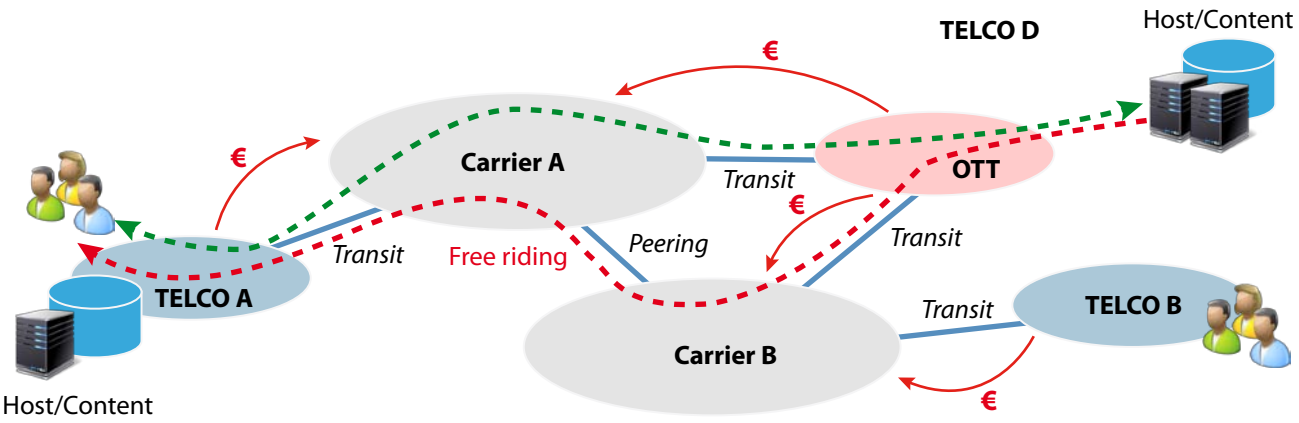
na una concentrazione di Host e Contenuti.
I *Tier1* stabiliscono relazioni di peering fra di loro, mentre vendono servizi di Transito ad altri operatori *non-Tier1* (vedi Figura 3).
In un decennio, lo scenario si modifica radicalmente; cresce enormemente l'importanza dei *contenuti* e cresce il ruolo di operatori che operano come Carrier/Aggregatori per il traffico. Il traffico IP mondiale, che nel 2001 era di 1 Exabyte all'*anno*, cresce esponenzialmente e diventa di 1 Exabyte al *mese* nel 2004 [10]. Compaiono e si sviluppano aziende (OverTheTop e Content Providers - OTT/CP) che non dispongono di proprie reti, ma forniscono servizi, applicazioni, contenuti "su" Internet, e possono raggiungere ed essere raggiunti dai Clienti finali grazie alla connettività mondiale

Figura 3 – Peering e Transit



garantita dalle reti interconnesse degli operatori nazionali ed internazionali. Nell'ecosistema degli OTT/CP si verifica una progressiva forte concentrazione in alcuni grandi player (fra cui Google che viene quotata in borsa nel 2004).
In questo contesto i Telco ricevono traffico generato da OTT/CP attraverso interconnessioni di tipo transito (pagate dai Telco) oppure di tipo peering e in ogni caso non hanno remunerazione. Solo in qualche caso i Telco ricevono cifre modeste (es. paid peering) per il servizio di delivery del traffico sino ai Clienti finali. Nell'esempio di Figura 4 si suppone che l'OTT utilizzi due diversi Carrier per accedere ad Internet (attraverso transiti a pagamento). Il traffico generato dall'OTT, per raggiungere i Clienti finali del Telco A, può seguire il percorso "tratteggiato verde", ma può seguire anche il percorso "tratteggiato rosso", transitando prima attraverso il Carrier B e quindi attraverso il Carrier A; questo percorso si configura come *free riding* in quanto sfrutta la relazione di peering fra i due Carrier (il Carrier A non riceve remunerazione per questo traffico). Se il Carrier A bloccasse il traffico proveniente dall'OTT lungo il percorso "rosso" (adottando modelli noti come *partial peering*) si esporrebbe al rischio di non poter più garantire al Telco A (a cui vende il servizio di transito verso tutti gli AS mondiali) la connettività completa con il Telco B (perché il Carrier B potrebbe reciprocamente applicare *partial peering* sui flussi in transito dal Carrier A al Carrier B). D'altra parte, si nota che in tutti i casi il Telco A non riceve alcuna remunerazione da OTT/CP o da altri operatori per il traffico che consegna ai Clienti finali (anzi paga il transito al Carrier A), ma incorre in costi crescenti per gli sviluppi di rete necessari ad evitare che la crescita del traffico entrante crei saturazione e degrado di prestazioni.
La fase successiva dello sviluppo di Internet ha visto l'affermazione di soggetti che offrono, a livello globale, servizi di delivery di traffico IP assicurando una qualità migliore di quella ottenibile dal puro best effort, ad esempio mediante soluzioni di Caching, Web Acceleration, Content Delivery Network – CDN e ADN (nel seguito si farà riferimento all'insieme di queste soluzioni con il termine CDN/ADN). In una CDN [11] il flusso dati che giunge al Cliente finale non proviene direttamente da un Host remoto, ma da una *cache* intermedia (i contenuti periodicamente sono distribuiti, memorizzati e aggiornati nelle cache secondo algoritmi proprietari); in questo modo diminuisce drasticamente il traffico che esce direttamente dall'Host remoto (e quindi diminuisce il traffico nelle reti intermedie lungo il percorso), ma soprattutto migliora la QoE perché il flusso IP deve compiere un percorso più breve e diretto, fra la cache ed il cliente finale. Si vedano gli esempi in Figura 5; i flussi di aggiornamento delle cache dei nodi CDN (linee "tratteggiate nere" in Figura 5) attraversano i peering ed i transiti; i flussi che arrivano sugli end-user sono invece originati dalle cache, seguendo percorsi molto più brevi (linee "tratteggiate verdi"). Le soluzioni basate su CDN, caching, ecc... hanno pesantemente cambiato il modo di realizzare le intercon-

Figura 4 – Inadeguatezza dei modelli tradizionali per il traffico da OTT/CP

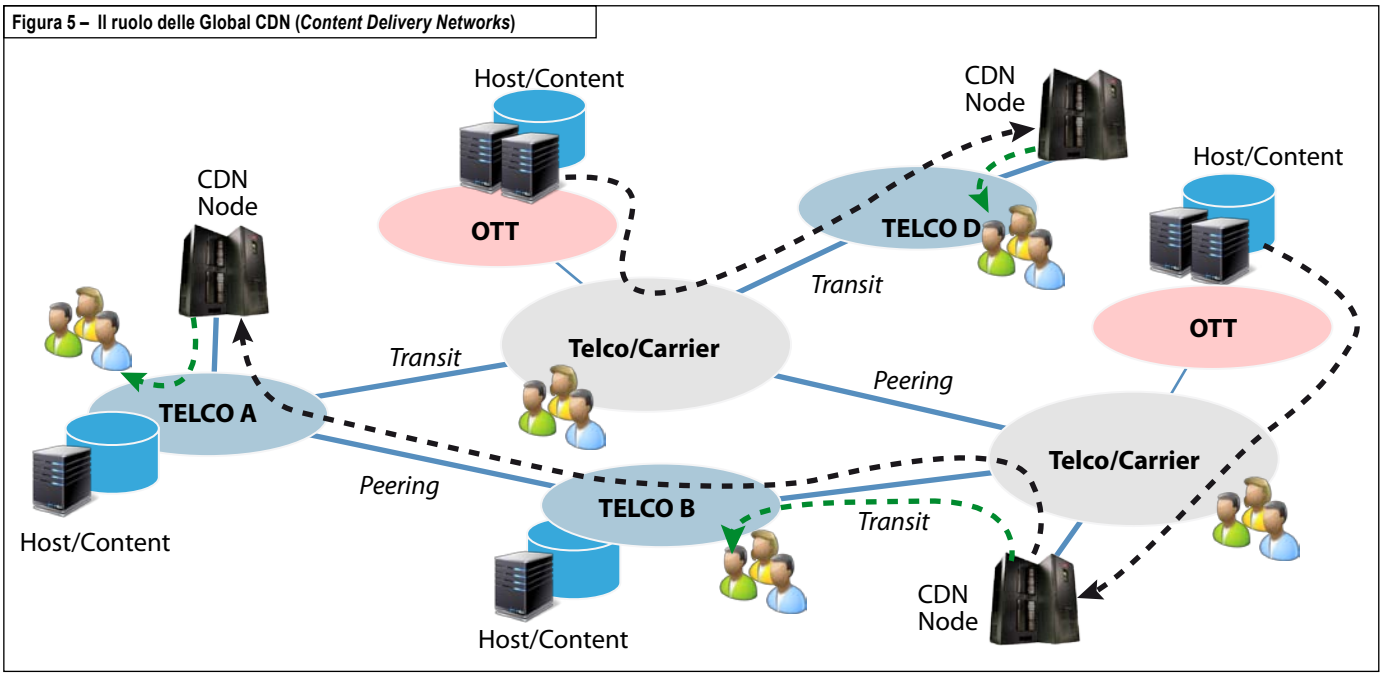


nessioni fra OTT, Carrier e Telco; ad es. nella Figura 5 la presenza di nodi CDN collegati alla rete di Telco A riduce drasticamente il traffico che attraversa le interconnessioni di transito e peering.
Va ricordato che queste soluzioni sono utilizzate non solo per servizi "bandwidth intensive" come il video streaming e il cloud computing, ma anche per migliorare la fruibilità di servizi Internet "tradizionali" come il Web browsing. Infatti, ad es., il "tempo di risposta al click" è un parametro fondamentale per qualunque business legato alla navigazione Internet e per qualunque OTT/CP che voglia migliorare la QoE ed incrementare i ricavi da advertising. Bassi tempi di risposta al click sono importanti per aumentare il numero di persone che accedono al sito, la durata si permanenza sul sito, la soddisfazione delle "frequentazioni" da parte dei Clienti finali)[3].
In questa fase dello sviluppo di Internet (di cui una data emblematica può essere considerata il 2010, anno in cui i ricavi di Akamai hanno superato la soglia di 1B$), il traffico IP mondiale ha continuato la sua corsa (diventando di 1 Exabyte alla *settimana* nel 2007) modificandosi anche nel mix, con una prevalenza di traffico di tipo video e content. Evidentemente i semplici modelli tradizionali sono inadatti al caso di interconnessione fra nodi CDN e le reti, in quanto ad es. non tengono conto del valore economico ne' del traffico scambiato a valle ed a monte delle cache, ne' della collocazione topologica in rete dei nodi CDN e del valore rappresentato dalla qualità con cui i flussi di traffico possono giungere ai Clienti finali.

2.3 Le criticità dello scenario attuale dell'Interconnessione IP

I forti cambiamenti dell'ecosistema Internet richiamati nel paragrafo precedente, non accompagnati da una adeguata evoluzione dei modelli di interconnessione IP, hanno determinato una situazione attuale di criticità.
I bisogni degli individui e delle aziende sono mutati, determinando una forte crescita della componente "video" nel traffico complessivo uno spostamento verso servizi Cloud e verso paradigmi di connettività always-on (con ubiquità fisso-mobile), fruizione in modalità social-net, alta interattività. I nuovi servizi richiedono, in molti casi, che la rete sia in grado di fornire QoS end-to-end (bassa latenza e jitter, bit-rate minimo garantito). La continua crescita del traffico IP, stimato pari ad 1 Exabyte al *giorno* dopo il 2013, comporta per i Telco forti incrementi di Capex/Opex per lo sviluppo rete, mentre i ricavi da Accesso Internet sono praticamente "flat". Questo porta, con gli attuali modelli di interconnessione IP, problemi di sostenibilità economica per gli operatori di telecomunicazioni.
In particolare i Domestic Telco acquistano transiti, per consentire ai loro end-user l'accesso a tutti gli indirizzi IP, e realizzano peering: in genere free peering con OTT/

Figura 5 – Il ruolo delle Global CDN (*Content Delivery Networks*)



3 Studi di Google, Bing, Aberdeen Group indicano ad es. che 1 sec. di ritardo nella risposta al click comportano perdite del 16% nella soddisfazione Clienti, dell'11% nel numero di pagine visitate, del 7% nella "conversione" del click in una azione concreta come un acquisto, un download, una digitazione di informazioni personali, ecc... Il tempo di risposta dipende da molti fattori, fra i quali in particolare la "distanza" dal Cliente finale ed i livelli di qualità con cui il traffico viene trasportato sulla rete.

CP e in alcuni casi paid peering con altri Telco. Gli accordi di transito e di peering sono solitamente definiti in base allo sbilanciamento dei volumi di traffico e senza tener conto del "valore commerciale" che il traffico ha per le due parti interconnesse.

Questo modello di interconnessione porta i Domestic Telco ad avere ricavi che sono essenzialmente relativi all'accesso internet pagato dagli end-user (secondo il modello *one side market*) ed a non avere praticamente ricavi da OTT/CP o da altri player, es. CDN Provider e Aggregatori (come invece avverrebbe applicando modelli *two sides market*). D'altra parte proprio questi soggetti:

- generano la maggior parte del traffico entrante (in media oltre l'80%) nelle reti dei Telco
- hanno ricavi da advertising e da servizi offerti agli end user. Ad esempio la terminazione di commercial movies ha un notevole valore per il fornitore dei contenuti, ma i Domestic Telco, che acquistano transiti o realizzano free peering, non ricevono ricavi per la terminazione di questo traffico sui loro end-user.

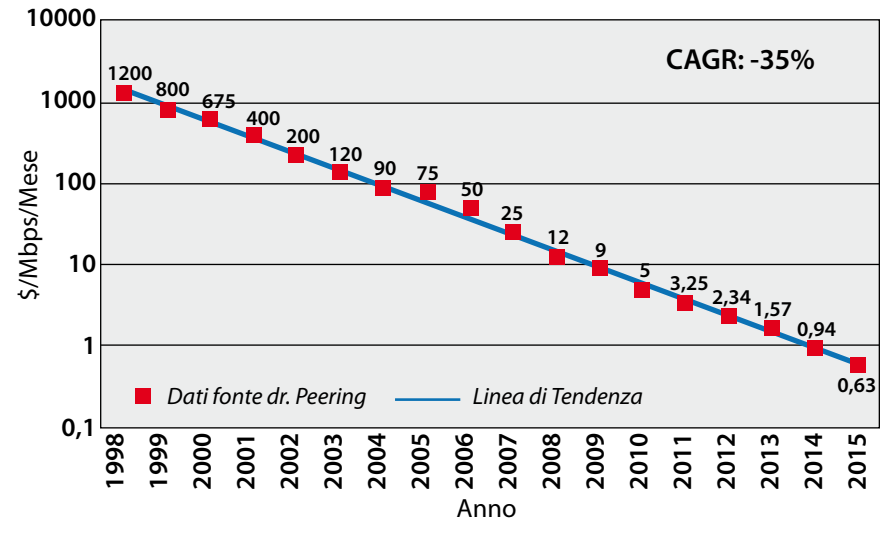
Il mondo degli OTT, accanto ad una miriade di soggetti medio-piccoli e piccolissimi, annovera pochi grandi player con un ruolo assolutamente dominante a livello globale. Il business model degli OTT è basato su un *reach* mondiale, garantito dalla rete internet, e su ricavi da advertising e da servizi/applicazioni offerti ai clienti dei Telco. In genere gli OTT, anche per motivi storici, non pagano la terminazione sulle reti degli operatori domestici, oppure pagano cifre molto basse rispetto al valore del loro business, mentre alcuni servizi offerti dagli OTT si pongono sempre più in competizione con quelli dei Telco (es. messaggistica, voce, servizi alle aziende, ...).

L'utilizzo da parte dei Telco di modelli di interconnessione IP tradizionali (ed in particolare il transito ed il *free peering* senza verifica sugli indirizzi per i quali è consentito il peering) rende possibile il *free-riding* sulle reti dei Telco. Per *free riding* si intende, in generale, qualunque situazione in cui il traffico attraversa le reti senza che i Telco ricevano un corrispettivo correlato al valore del traffico stesso. Il free riding si determina ogniqualvolta c'è disconnessione fra: 1) il traffico, 2) i ricavi del soggetto (OTT/CP/CDN Provider...) il cui business è legato a quel traffico, 3) la remunerazione che il soggetto (OTT/CP/...) riconosce a chi (Telco) consegna quel traffico a destinazione.

La modalità indifferenziata di gestione del traffico IP sulle reti dei Telco basata sul *best-effort* per la consegna del traffico, non permette di fornire le prestazioni richieste da alcuni servizi (ad es. video streaming real time), ed in alcuni casi non permettere di riconoscere differenze di valore nei flussi di traffico (ad esempio il valore dei bit associati ad un commercial movie è maggiore del valore dei bit associati al browsing). Inoltre il trattamento indifferenziato del traffico genera inefficienze nel dimensionamento delle reti, con maggiori costi di terminazione per i Telco. Se invece il traffico viene *caratterizzato*, sino da quando "entra" nell'AS del Telco, è possibile utilizzare, nelle reti del Telco, soluzioni quali caching, acceleratori, CDN/ADN che permettono di migliorare le prestazioni e ridurre, per alcuni servizi come ad es. il video streaming e cloud, i flussi di traffico nei backbone ed i correlati costi (secondo Akamai, con tecniche di caching si ottengono efficienze superiori all'80% per *media services*).

Anche il mercato dei transiti, basato sui modelli tradizionali di interconnessione, è stato caratterizzato da una costante e significativa riduzione dei prezzi (tipicamente i prezzi sono riferiti al traffico di

Figura 6 – Andamento dei prezzi dei transiti worldwide



Il punto di vista di ETNO

Nell'ambito dell'analisi sul futuro del settore delle telecomunicazioni in Europa, ETNO, l'associazione europea degli operatori di telecomunicazioni, sta attribuendo crescente importanza al tema dell'interconnessione IP. Lo stesso orientamento si rileva nelle Istituzioni comunitarie preposte alla definizione di policy regolamentari per il settore, in particolare la Commissione europea ed il BEREC (l'organismo dei regolatori europei).

La crescita dell'interesse nei confronti dell'interconnessione IP è una diretta conseguenza della transizione verso un mondo all-IP e delle sfide che esso comporta per le tradizionali fonti di ricavo sul traffico, come l'interconnessione wholesale. A livello europeo e non solo, ETNO ha contribuito ad alimentare il dibattito, ponendo particolare attenzione allo sviluppo delle prospettive di business legate al modello di interconnessione.

In particolare, come illustrato dalle anticipazioni di uno studio commissionato da ETNO ad ATKearney, due aspetti sono cruciali per i Telco. In primo luogo, un profondo cambiamento nelle strutture di pricing dei servizi offerti dall'industria europea delle telecomunicazioni, dovuto alla crescente competitività del settore; in secondo luogo, l'erosione dei ricavi derivante da nuovi servizi offerti in rete a costo zero per il consumatore, con la tradizionale tariffazione di chiamate e messaggi messa a rischio dalla concorrenza di sostituti OTT (*Over-the-Top*), basati su un modello di business del tutto diverso da quello della telefonia tradizionale.

Questo secondo punto è stato messo in luce da diverse analisi. A quella di ATKearney si aggiunge ad esempio quella di IDATE, su cui si basa l'ultima relazione economica annuale di ETNO (novembre 2012). Dalle elaborazioni di IDATE appare chiaro che il calo dei ricavi legati ai servizi tradizionali non è compensato dalla crescita dei ricavi derivanti dall'accesso alla banda larga (vedi Figura A). D'altra parte lo sviluppo dei servizi e del traffico comporta costi crescenti per gli operatori.

Le analisi ETNO evidenziano un sostanziale disequilibrio tra chi investe nelle infrastrutture necessarie allo sviluppo di Internet e chi trae i maggiori benefici dalla sua impressionante crescita. Tale scenario è reso ancora più difficile dalla frammentazione del mercato europeo delle telecomunicazioni, che contrasta nettamente con il livello di concentrazione dei mercati degli Stati Uniti e dei Paesi dell'Asia orientale. Tale frammentazione limita notevolmente lo spazio per innovare e razionalizzare i costi.

La transizione verso un sistema di reti all-IP rende quindi necessaria una riflessione approfondita sulla (non) sostenibilità dell'attuale ecosistema di Internet. Tale riflessione è resa ancora più urgente data la necessità di trovare fonti di finanziamento per investimenti in banda larga e ultralarga, come richiesto dagli obiettivi dell'Agenda Digitale Europea.

La domanda alla base di questa riflessione è la seguente: come fare evolvere l'ecosistema complessivo in modo che il valore del traffico IP, legato ai contenuti, applicazioni, servizi, advertising, ecc… possa generare ricavi sufficienti per una nuova fase di investimenti?

A questa domanda ETNO ha risposto evidenziando la necessità di passare da sistemi di charging tradizionali a nuovi meccanismi, basati sulla qualità del servizio. Le prime indicazioni in tal senso sono state presentate da ETNO nell'ambito di una consultazione pubblica lanciata dal BEREC nel maggio 2012.

Nella sua risposta alla consultazione, ETNO ha proposto di affiancare al modello di interconnessione IP basato sul best effort un modello basato sulla QoS (*Quality of Service*). La scelta di applicare il secondo modello dovrebbe essere lasciata alle libere negoziazioni

picco [Mbps] misurato al punto di interconnessione). L'entità della riduzione dipende dalle aree geografiche; alcuni analisti (Figura 6) indicano una decrescita per il periodo 2010-2015 con CAGR di -35%; altre valutazioni indicano un CAGR per il periodo 2008-2011 nel range -20% / -30% ed evidenziano riduzioni di oltre il 50% in alcune aree (es. Londra, NewYork) [12].

Dal momento che, come già ricordato, il traffico IP cresce, che i costi di rete aumentano con il traffico, e che i modelli di tradizionali mantengono una disconnessione fra il traffico e la remunerazione degli operatori, si potrebbero evidentemente determinare problemi per la sostenibilità; la rilevanza del problema è ormai riconosciuta a livello internazionale (vedi Box "*ETNO*").

3 Nuovi modelli di interconnessione

L'analisi dello scenario fa emergere chiaramente la necessità di nuovi modelli di interconnessione tra Telco e OTT/CP/CDN Provider/Aggregatori; i nuovi modelli devono essere capaci di:

1) permettere e promuovere il *delivery del traffico IP con qualità;*

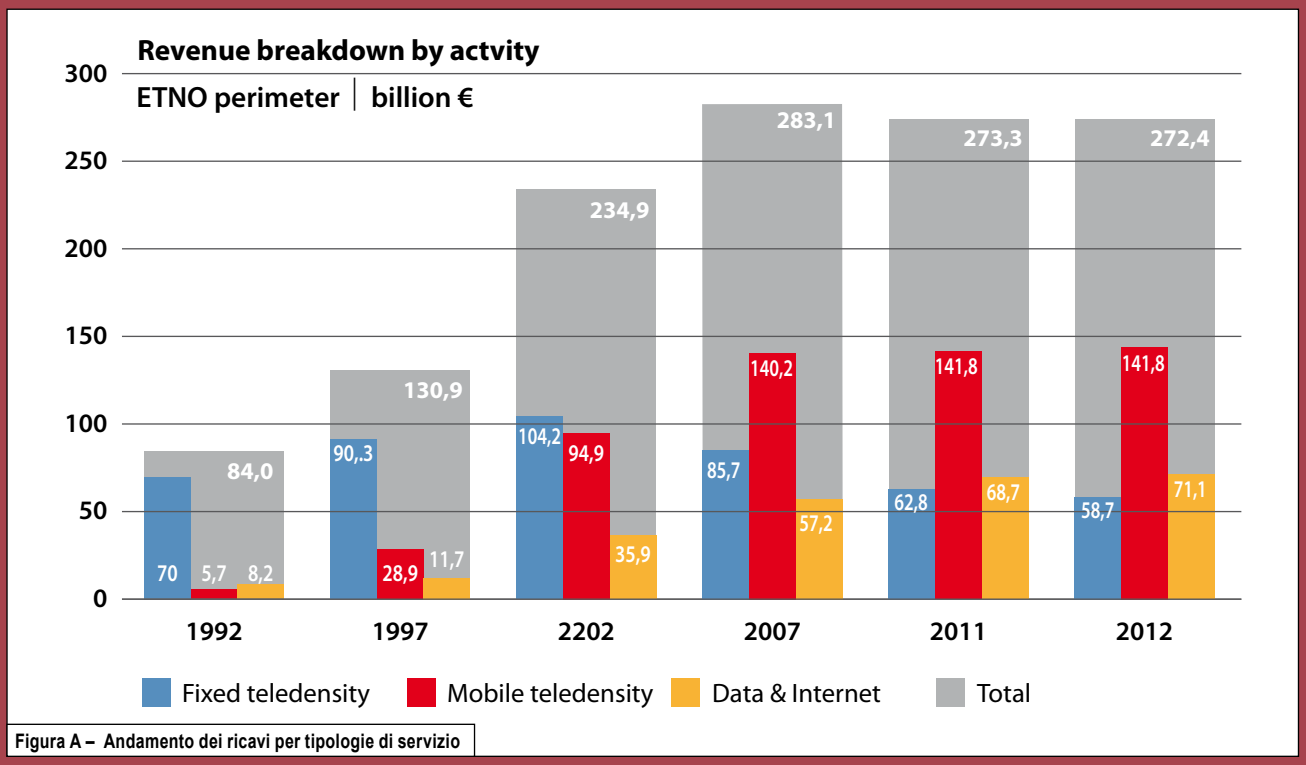


Figura A – Andamento dei ricavi per tipologie di servizio

commerciali fra gli attori della catena di valore digitale. Secondo l'associazione, l'introduzione di un modello di interconnessione basato sulla QoS e volto a migliorare la qualità dei contenuti, delle applicazioni e dei servizi forniti in rete, porterebbe benefici tanto ai consumatori quanto ai diversi attori dell'ecosistema Internet. Accanto alla QoS altri elementi importante nella definizione degli accordi di interconnessione IP sono i volumi del traffico scambiato (che possono essere simmetrici o no) e il valore associato al traffico.

In ultima analisi, ETNO sostiene che il regime di interconnessione IP debba evolvere in linea con i requisiti imposti dai nuovi servizi, dai comportamenti e dalle esigenze dell'utente finale e dai flussi di traffico IP che ne derivano.

La fornitura di servizi caratterizzati da QoS in aggiunta alla trasmissione best effort permetterà la creazione di nuovi modelli di business. Agli operatori non deve essere preclusa la possibilità di fornire tali servizi sia ai consumatori finali che ai provider di contenuti ed applicazioni OTT ■

luigi.gambardella@telecomitalia.it
michele.bellavite@telecomitalia.it

2) permettere la *valorizzazione dell'accesso ai clienti* dei Telco.

La qualità è necessaria sia per i Clienti finali, sia per OTT/CP; per lo sviluppo di Internet il maggior numero possibile di persone ed aziende deve poter fruire con l'adeguata QoE dei contenuti e delle applicazioni/servizi che OTT/CP rendono disponibili sul Web. Per garantire la QoE i Telco devono essere in grado di fornire QoS all'interno delle proprie reti.

OTT/CP sono consapevoli del *valore della qualità*, che da un lato estende il reach di servizi/applicazioni, e dall'altro permette di realizzare nuovi servizi rendendoli effettivamente fruibili in rete; i loro ricavi, da advertising e da servizi, dipendono dalla *soddisfazione* con cui gli end user possono utilizzare i contenuti e le applicazioni (la QoE influenza in modo determinante la frequenza e la durata degli accessi ai siti Web). Avere bassi valori di latency e jitter, ed alto bit-rate, è richiesto non solo per servizi video streaming, ma anche per il Web browsing. Proprio la necessità di migliorare la QoS ha consentito la crescita di soggetti (es. Akamai, Limelight,

L3) che forniscono servizi CDN, Web acceleration, cashing, ADN.
In sintesi, l'evoluzione di applicazioni e servizi in un mondo IP-centrico pone ai Telco la sfida di rendere possibili livelli di QoE adeguati alle nuove esigenze, in ogni condizione e su tutti i device fissi e mobili, e contemporaneamente di definire modelli di business e di customer relation sia verso i Clienti finali sia verso le terze parti fornitrici di applicazioni e contenuti.
Certamente i contenuti/servizi/applicazioni resi disponibili da OTT/CP costituiscono un importante valore per i Telco, che vendono accessi Internet ai Clienti finali, e sono interessati ad accrescere il numero dei clienti con accessi a larga banda fissi e mobili. D'altra parte le reti dei Telco rappresentano un valore per OTT/CP, che solo grazie alle reti di accesso ed al backbone possono essere raggiunti dai Clienti finali. Il "*valore della rete*" è testimoniato ad es. dal fatto che OTT e CDN Provider stanno chiedendo ai Telco di inserire i propri server 'dentro' le reti domestiche a partire dai Data Center per poi entrare nei POP e raggiungere la rete d'accesso (fino agli IP/DSLAM). I Telco quindi possono ottenere da OTT/CP il riconoscimento del valore della rete, e questo sta già avvenendo, in qualche caso dopo dispute anche legali (vedi Box "*Esempi in Europa e Stati Uniti*").
Stabilire nuove relazioni win-win fra OTT/CP e Telco richiede un'evoluzione dei modelli di interconnessione. I nuovi modelli di Interconnessione IP devono essere definiti partendo dalla considerazione che, oggi e sempre di più in futuro, il traffico IP è caratterizzato non solo dal "volume", ma da un "valore" commerciale che dipende dalla tipologia del traffico e dagli aspetti distintivi del soggetto che lo genera; in particolare va tenuto conto che:

- *OTT/CP* sono le principali "sorgenti" del traffico IP, originano traffico a cui generalmente sono associati ricavi da advertising, da servizi/applicazioni e da vendita di contenuti. Il valore nel caso di contenuti, servizi, applicazioni è in genere superiore a quello associato ad advertising.
- *CDN Providers/Aggregatori* distribuiscono il traffico generato da OTT/CP migliorando, nel caso dei CDN Provider, le prestazioni di delivery rispetto al best effort. Il valore di questo traffico è quindi anche legato ai ricavi che CDN Provider/Aggregatori ottengono offrendo servizi ad OTT/CP.
- I *Telco* hanno normalmente traffico entrante generato da OTT/CP e da CDN Provider/Aggregatori che è molto superiore rispetto a quello uscente. Il traffico "originato" dai Telco proviene tipicamente dagli end-users (incluso traffico da relazioni peer-to-peer) e ha un valore mediamente più basso rispetto a quello di OTT/CP "globali". Il traffico generato da OTT/CP "locali" e gestito dai Telco è certamente molto inferiore rispetto a quello degli *HyperGiants* globali come ad esempio Google e Netflix.

Per non compromettere la sostenibilità e lo sviluppo dell'intero ecosistema Internet, è necessario far evolvere sia la rete, sia i modelli di interconnessione IP con l'obiettivo di:

- abilitare nuovi modelli di business in grado di valorizzare correttamente sia gli asset degli OTT (applicazioni, contenuti, ...), sia gli asset dei Telco (reti, qualità, end-users...);
- generare valore dall'interconnessione IP, assicurando il *delivery con qualità* per le quote di traffico a cui è associato valore, in relazione alle prestazioni richieste dalle applicazioni ed alla QoE attesa dall'end-user;
- ridurre i costi di rete, gestendo il traffico con soluzioni efficienti (es. CDN, Caching, ADN).

Il superamento dei modelli tradizionali potrà avvenire soltanto mediante negoziazione diretta fra i soggetti coinvolti: i Telco devono relazionarsi con OTT, CP, CDN Providers secondo logiche di cliente/fornitore, offrendo servizi di delivery differenziati, adeguati ai requisiti dei diversi flussi di traffico e delle applicazioni. I nuovi modelli devono:

- tener conto non solo della *capacità* (bit/rate) all'interconnessione (e/o dei volumi di traffico) ma anche delle tipologie dei flussi di traffico, e quindi sia il *valore differenziato* che il traffico ha per l' OTT/CP/CDN Provider e per il cliente finale, sia gli specifici *requisiti di QoS;*
- facilitare, di volta in volta, la negoziazione diretta fra *i due soggetti portatori di valore*: ad es. l'OTT (che basa il proprio business su ADV e sulla vendita a Clienti finali di Applicazioni/servizi), ed il Telco (che serve i Clienti finali, ed incorre nei costi di rete legati anche ai volumi di traffico).

Conclusioni

I modelli di interconnessione IP tradizionali, basati su transito e peering e sulla terminazione del traffico in modalità best effort, sono stati importanti nelle fasi di

Cambiamenti nelle relazioni di interconnessione: esempi in Europa e negli Stati Uniti

La necessità di stabilire nuove relazioni di interconnessione, maggiormente rispondenti all'evoluzione dell'ecosistema ed ai ruoli dei diversi attori, ha già portato ad alcuni importanti accordi sia fra soggetti "Telco" e soggetti OTT, sia fra Telco ed aggregatori/CDN Providers, e questo è successo sia in USA sia in Europa.

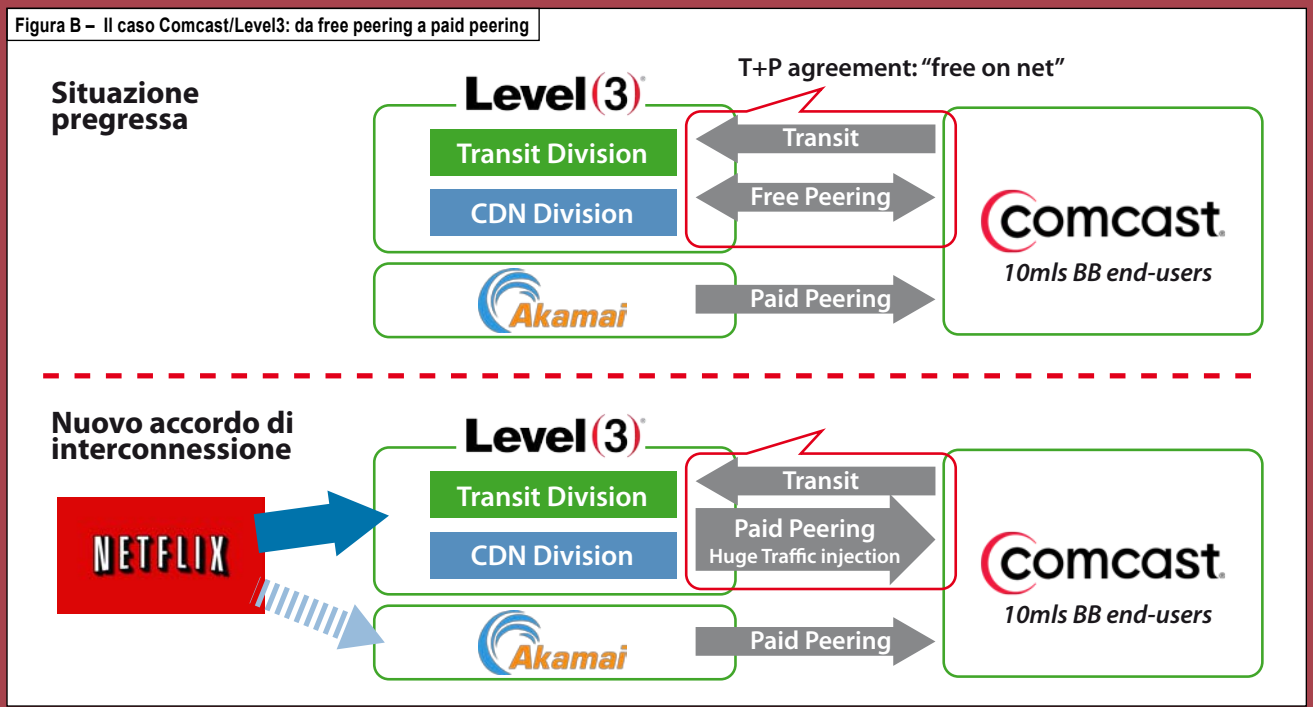
Ad esempio (vedi Figura B) Level3 (Tier 1 ISP) e Comcast avevano un accordo "free on net" (Transit + Free Peering); Level3 poteva raggiungere gratuitamente i clienti di Comcast, e Comcast poteva accedere gratuitamente alla Big Internet.

Quando Netflix selezionò Level3 come CDN provider, il traffico CDN di Level3 verso Comcast esplose: Comcast dovette trasportare, senza trarne ricavi, ingenti quantità di traffico (…proveniente da un competitor !). Comcast propose pertanto a Level3 un accordo a pagamento, inizialmente rifiutato, ma dopo un contenzioso (anche Legale), oggi Level3 ha un accordo di paid peering con Comcast. Il punto di forza di Comcast, che ha portato al nuovo modello di interconnessione, è stato il controllo dell' accesso verso i Clienti finali.

Un esempio in Europa è quello della disputa fra Cogent e France Telecom/Orange. Fra i due soggetti c'era una interconnessione di free peering; quando, al crescere del traffico, Cogent ha chiesto a FT di incrementare la capacità dell' interconnessione free, FT ha invece risposto con delle offerte a pagamento; le azioni intentate da Cogent contro FT per "rifiuto di accesso a risorsa essenziale per raggiungere i Clienti finali della rete domestica Orange" non hanno portato a decisioni in tal senso da parte dell' Autorità: ora Cogent paga FT per il traffico in eccesso. Anche in questo caso è stato riconosciuta la legittimità del Telco di valorizzare i propri asset (la rete ed i Clienti finali).

Esempi differenti, ma indicatori significativi del cambiamento in atto, sono gli accordi che soggetti come Akamai (che fornisce servizi di CDN/ADN a livello globale) hanno stipulato con Telco (es. Orange, AT&T). Questi accordi, di varia natura, hanno in comune la finalità di migliorare la QoE per alcune tipologie di flussi di traffico; i valori portati dal Telco in questi accordi sono l'accesso ai Clienti finali, ed il controllo della rete sino ai clienti, indispensabile per garantire la qualità del delivery ■

Figura B – Il caso Comcast/Level3: da free peering a paid peering



crescita di Internet, ma presentano limiti che li rendono non adeguati per lo scenario attuale e per i necessari sviluppi dell' ecosistema complessivo. Nell'evoluzione di Internet, l'interconnessione IP rappresenta un grandissimo valore sia per gli OTT/CP/CDN Provider che per i Telco; entrambi hanno infatti interesse a fare in modo che i Clienti finali possano accedere, con una adeguata QoE, ai contenuti ed alle applicazioni su internet. Sono quindi necessari nuovi modelli di interconnessione IP, capaci di abilitare nuovi modelli di business, idonei a garantire un equilibrio fra i diversi attori coinvolti, e la sostenibilità dell'evoluzione di reti, servizi ed applicazioni.

È importante ricordare che l'adozione, attraverso negoziazione fra i soggetti coinvolti, di nuovi modelli di interconnessione deve essere accompagnata da una trasformazione complessiva della rete [13]. Infatti i requisiti di delivery con qualità differenziata, previsti dai nuovi modelli di interconnessione, si traducono in requisiti architetturali e tecnici sia sui diversi segmenti di rete (accesso fisso e mobile, aggregazione, dorsale), sia per i diversi livelli funzionali (trasporto, controllo, intelligenza).

In termini generali, la trasformazione della rete deve realizzare una *intelligent pipe*, ottimizzata per uno scenario in cui la totalità del traffico sarà IP (di cui gran parte video) ed in cui una molteplicità di applicazioni e servizi avranno requisiti differenziati di qualità. Le scelte tecniche ed architetturali dovranno essere coerenti con il paradigma *network as a platform*: una piattaforma efficiente e flessibile, che utilizza tecnologie API, per il supporto di applicazioni e servizi anche forniti da terze parti, coerente con modalità di erogazione e fruizione *on the Cloud*.

Il Gruppo Telecom Italia ha definito nuove Policy di Interconnessione in linea con i modelli richiamati nell'articolo, ed ha piani di sviluppo di rete per l'Ultra Broadband fisso e mobile (FTTx ed LTE), mentre il "Backbone" evolverà con l'estensione dell' IP/MPLS in tutti i segmenti di rete a supporto della qualità E2E, con l'arricchimento e la convergenza delle funzioni di intelligenza ■

Bibliografia

[1] E.Jahn & J.Prüfer, "*Dark Clouds over the Internet?*", Social Science Electronic Publishing (2005) *http://papers.ssrn.com/sol3/papers.cfm?abstract_id=654442*

[2] ATKearney "*A Viable Future Model for Internet*", public report 2010

[3] Ericsson, "Traffic and Market Data Report", February 2012 Update, http://www.ericsson.com/res/docs/2012/tmd_report_feb_web.pdf

[4] Dr.Peering, "*Access Power Peering - The Netflix, Comcast and Level 3 Story*", September 2011, *http://drpeering.net/AskDrPeering/blog/articles/Ask_DrPeering/Entries/2011/9/6_Access_Power_Peering.html*

[5] [France Telecom, Cogent] Internet Traffic – Peering Agreements, Autorité de la Concurrence, Sept. 2011 *http://www.autoritedelaconcurrence.fr/user/standard.php?id_rub=418&id_article=1971*

[6] Huw Saunders "*IP Interconnection: trends and emerging issues*", OFCOM June 2012, *http://berec.europa.eu/files/news/ofcom_ipic.pdf*

[7] Report on "*Net and Network Neutrality*", April 2011, National Assembly FR, *http://www.assemblee-nationale.fr/english/dossiers/net_and_network_neutrality.pdf*

[8] La neutralità della rete: le risultanze della consultazione pubblica di cui alla delibera n. 40/11/CONS - Allegato A alla delibera n. 714/11/CONS

[9] Sul tema, per molti versi aperto, di QoS e QoE, si rimanda ai lavori di ITU-T SG12: "*Performance, QoS and QoE*" *http://www.itu.int/en/ITU-T/studygroups/2013-2016/12/Pages/default.aspx*

[10] Sito Visual Networking Index– VNI Cisco; Report "*The Zettabyte Era*" 2012, e dati periodicamente aggiornati *http://www.cisco.com/en/US/netsol/ns827/networking_solutions_sub_solution.html*

[11] F.Calonico "*Le Content Delivery Network di Telecomn Italia*", Notiziario Tecnico Telecom Italia n.2 – 2012

[12] TeleGeography, Global Internet Geography – Executive Summary *http://www.telegeography.com/page_attachments/products/website/research-services/global-internet-geography/0003/1871/GIG_Executive_Summary.pdf*

[13] G. Catalano, G. Ciccarella, D. Franceschini, D. Roffinella. "*Nuove reti per la nuova TV*", Notiziario Tecnico Telecom Italia n.3-2012.

Urlografia

http://www.youtube.com/watch?v=IPn0T1UacIA

gianfranco.ciccarela@telecomitalia.it
daniele.roffinella@telecomitalia.it

Gianfranco Ciccarella è attualmente Vice Presidente Technical Support Area Sudamerica del Gruppo. Dal 2011 al febbraio 2013 è stato Vice Presidente - Next Generation Access Networks and Partnership - in Strategy. Ha ricoperto dal 2009 all'inizio del 2011 il ruolo di Vice Presidente - Technical Support - in Technology & Operations ed è stato responsabile dei progetti sulla NGAN. Dal 1998 al 2009 è stato Executive Vice President -Network e IT- di Telecom Italia Sparkle ed ha avuto la responsabilità di realizzare e gestire la rete internazionale di Telecom Italia, una rete multi regionale, multiservizio e full IP. È stato anche membro del Consiglio di Amministrazione di alcune Società del Gruppo e Direttore della formazione presso la Scuola Superiore Guglielmo Reiss Romoli a L'Aquila. Ha svolto attività di ricerca e di insegnamento presso l'Università dell'Aquila e la New York Polytechnic University ed autore di due libri e di numerosi articoli.

Daniele Roffinella ingegnere in telecomunicazioni, attualmente responsabile per l'Evoluzione Tecnologica in Next Generation Access Networks & Partnership, nella Direzione Strategy del Gruppo TI.
Nella sua trentennale esperienza professionale nel settore telecomunicazioni, ha svolto attività in ambiti di innovazione, normativa, ingegneria, pianificazione, con responsabilità di funzioni aziendali e progetti relativi a reti metropolitane e geografiche, sistemi di commutazione, rete intelligente, reti Broadband Wireless. Ha guidato attività di Industrial Analysis a livello Gruppo TI e ha operato come Technical Support della Direzione Technology&Operations. È membro IEEE Society.

Usa il tuo smartphone per visualizzare approfondimenti multimediali

MOBILE SECURITY: QUALI SFIDE, QUALI PROSPETTIVE

Rosalia d'Alessandro, Roberta D'Amico, Marcello Fausti

Milioni di app, nuovi modelli di *smartphone* e *tablet* ogni pochi mesi, un accesso mobile sempre più veloce: è la *new mobile economy*. In questa fase di sviluppo e crescita che sembra inarrestabile non si possono trascurare gli aspetti di sicurezza dell'intero eco sistema: reti, terminali, applicazioni, identità e una miriade di dati personali da gestire e proteggere. Solo dalla collaborazione tra i diversi attori si possono trovare le risposte alle sfide poste dalla mobile security.

1 Introduzione

Parlando di mobile la mente corre veloce alle evoluzioni degli ultimi tempi con dispositivi dalle caratteristiche e prestazioni impensabili fino a qualche anno fa. Del resto l'idea di un telefono senza tastiera con funzionalità multimediali avanzate e servizi Internet sempre disponibili sulla punta delle dita è diventata una realtà solo da poco più di un lustro. Il mercato dei cellulari a livello mondiale è cresciuto con continuità dal 2009 e sebbene i dati relativi al 2012, appena pubblicati da Gartner, evidenzino, per la prima volta, una contrazione delle vendite (-1,7%) rispetto all'anno precedente, il volume complessivo dei dispositivi venduti è stato pari a 1,75 miliardi. La vendita degli *smartphone* tuttavia è ancora cresciuta, facendo registrare nel quarto trimestre un +38,3% per un totale, sempre nel trimestre, di quasi 208 milioni di unità. Leader di questo segmento di mercato si confermano Apple e Samsung. Anche le stime per i prossimi 5 anni vedono il mercato mobile in crescita: per la fine del 2017 si prevede che le connessioni mobili raggiungeranno 9,7 miliardi, rispetto agli attuali 7 miliardi, con un'utenza mobile che passerà da 3,2 miliardi ai 4 miliardi di unità. In particolare le connessioni mobili di tipo broadband, attualmente stimate in 1,6 miliardi, raggiungeranno quota 5,1 miliardi.

Un altro fattore che ha caratterizzato la nuova generazione di dispositivi, dando un notevole impulso alla loro diffusione, è stata l'affermazione degli *application store* e del modello di business che vede i big player quali Apple e Google proporre le applicazioni sviluppate da una pluralità di autori che hanno oggi a disposizione un modo semplice, veloce e "standardizzato" per offrire, pubblicizzare e vendere il prodotto del loro ingegno. Oltre 700.000 sono le app Android su *GooglePlay*, oltre 800.000 quelle su App Store di Apple, senza contare poi quelle per i dispositivi BlackBerry e Windows Phone in rapida crescita. "C'è un'app per tutti i gusti" recita uno slogan pubblicitario e, in effetti, è proprio così; per tutti i gusti e per tutte le necessità: dalle previsioni del tempo, agli orari dei treni, dalle ultime notizie, all'acquisto dei biglietti per il cinema, dai giochi all'intrattenimento, solo per fare qualche esempio.

È evidente come i dispositivi mobili, in questo nuovo contesto, si ritrovino a gestire, oltre al tradizionale credito telefonico, enormi quantità di dati sensibili, account per accedere ai servizi forniti tramite le app, identità digitali, diventando nei fatti l'obiettivo preferito di attaccanti e frodatori.

Lo scenario tecnologico e di mercato è diventato molto articolato e complesso e gli aspetti di sicurezza sempre più rilevanti.

Il tema della protezione dei dati e delle identità digitali degli utenti gestiti da questi dispositivi, può rappresentare un'opportunità di business importante per gli operatori mobili.

Sviluppare a tutto tondo il tema della mobile security in un singolo articolo è tutt'altro che bana-

le. Per provare ad accompagnare il lettore negli approfondimenti che questo articolo propone, partiremo da una schematizzazione del dominio di riferimento. La schematizzazione più semplice è quella che prevede di sviluppare il tema security a livello di:

- rete, in particolare della rete di accesso, sia per la coesistenza di tecnologie, protocolli, algoritmi di sicurezza diversi, sia per l'attenzione che occorre porre al dispiegamento delle reti di ultima generazione;
- terminali, in particolare per le caratteristiche di sicurezza dei diversi sistemi operativi e i relativi modelli di gestione dei rischi;
- applicazioni (app), includendo in quest'ultima sezione anche il tema della protezione dei dati personali dell'utente e l'uso dei mobile honeypot per rilevare il nuovo malware.

2 Sicurezza della rete d'accesso

Per un operatore mobile la sicurezza della propria rete di accesso è un importante requisito sia per garantire la sicurezza delle comunicazioni dei propri clienti, sia per proteggere la propria infrastruttura e salvaguardare la propria immagine.
Occorre evidenziare che lo scenario di rischio delle reti mobili è cambiato radicalmente negli ultimi due anni. Infatti la disponibilità di tool open source che girano su dispositivi a basso costo fa sì che molti degli attacchi in passato noti solo da un punto di vista teorico, ma molto complicati da attuare, oggi siano realizzabili con sforzo e costi decisamente inferiori, rendendo quindi fattibili scenari di attacco una volta impensabili. Per stimolare l'attenzione dei media sul tema, a partire dallo scorso anno, è addirittura disponibile un sito in cui sono pubblicati, e continuamente aggiornati, i risultati di attività di analisi effettuate da ricercatori tedeschi, col contributo della comunità Internet, sulle reti mobili 2G dei principali operatori [2]. Si tratta di dati che paragonano le misure di sicurezza dispiegate in campo rispetto a tre principali categorie di minaccia:

- la possibilità di impersonare un utente, effettuando ad esempio chiamate voce oppure inviando SMS per suo conto;
- l'intercettazione del traffico voce e dati;
- il tracciamento dell'utente, nell'ottica di identificare i suoi spostamenti.

Tale attività testimonia come alcuni algoritmi deboli dal punto di vista della sicurezza, in quanto ormai superati dai progressi tecnologici raggiunti, siano ancora oggi usati in molte reti 2G. Altro aspetto da rimarcare riguarda la presenza di configurazioni in campo che penalizzano la messa in sicurezza delle comunicazioni, ad esempio a causa di apparati datati o sottodimensionati. Infine alcune vulnerabilità sono proprio intrinseche negli algoritmi e nei protocolli 2G (ad esempio l'assenza della mutua autenticazione apparato-rete) e non eliminabili.
Come Security Lab abbiamo di recente effettuato un'attività di analisi e test, anche in campo, per comprendere il reale livello di difficoltà nel riprodurre gli attacchi noti in letteratura, usando tool e informazioni disponibili pubblicamente. I risultati di tale attività sono stati condivisi anche con il GSMA Security Group e sono stati utilizzati come base per effettuare un security assessment sistematico della nostra rete, e delle reti di Telecom Argentina e Tim Brasile.
Uno studio approfondito è stato inoltre rivolto agli aspetti di riservatezza ed integrità dei dati sulle reti mobili GSM, GPRS/EGPRS, UMTS e LTE. L'analisi ha considerato le pubblicazioni scientifiche, le informazioni reperibili in rete, i vincoli e le vulnerabilità degli algoritmi utilizzabili. Molti di questi algoritmi sono standardizzati dal 3GPP. Alcuni sono ancora segreti oppure specificati in termini di parametri e strutture dati dai singoli operatori mobili nell'ambito di generiche linee guide.
Si ricorda che nelle reti GSM/GPRS/EGPRS non esiste autenticazione della base station al terminale mobile e non c'è protezione dell'integrità dei dati. Nelle reti UMTS/LTE invece tale autenticazione esiste e viene assicurata la protezione dell'integrità dei dati (over-the-air) con i MAC)*Message Authentication Code*).
La riservatezza dei dati (over-the-air) è invece disponibile in tutte le reti GSM/GPRS/EGPRS/UMTS/LTE ed è assicurata applicando algoritmi di cifratura, diversi e con differenti livelli di sicurezza a seconda della tecnologia di accesso.
Le seguenti tabelle schematizzano la mappa degli algoritmi utilizzabili rispettivamente nelle reti 2G e in quelle 3G/4G, sintetizzandone caratteristiche e proprietà di sicurezza. In particolare il codice colore utilizzato nelle tabelle prevede il rosso per indicare un livello di sicurezza nullo o molto basso, l'arancio per un livello di sicurezza basso, il giallo per un livello di sicurezza medio e il verde per un livello alto.

Mobile Network Protection	Encryption Integrity Algorithm	Key Bitsize	Key Generation Algorithm	Security of Key Generation Algorithm
GSM-2G Confidentiality	A5/0 No encryption			
	A5/1 (64-bit state, known next-state function)	64	A8: COMP128-1, COMP128-2, COMP128-3, UMTS MILENAGE type algorithm (e.g., based on AES-128)	Master key reconstruction attacks on COMP128-1; require either fake base station or possession of SIM card. In 2006, GSM recommended not to use COMP128-1.
	A5/2 (64-bit state, known next-state function)	64		
	A5/3 Based on KASUMI Counter/CBC mode (64-bit state, key-dependent next-state function	64		
	A5/4 Same* as A5/3	128	MILENAGE f3	Secure if based on AES-128. Theoretically proven that MILENAGE algorithms are jointly secure if the kemel block cipher is secure.
GPRS-2.5G Confidentiality	GEA0 No encryption	64		
	GEA1 Secret (96-bit state)	64	A8: COMP128-1, COMP128-2, COMP128-3, UMTS MILENAGE type algorithm (e.g., based on AES-128)	Master key reconstruction attacks on COMP128-1; require either fake base station or possession of SIM card. In 2006, GSM recommended not to use COMP128-1.
	GEA1 Secret (125-bit state)	64		
	GEA3 Same* as A5/3	64		
	GEA4 Same* as A5/3	128	MILENAGE f3	Same as above
EGPRS-2.75G Confidentiality	GEA0 No encryption			
	GEA3 Same* as A5/3	64	Same as above	Same as above
	GEA4 Same* as A5/3 or A5/4	128	MILENAGE f3	Same as above

Figura 1 - Algoritmi per reti GSM e GPRS

Mobile Network Protection	Encryption Integrity Algorithm	Key Bitsize	Key Generation Algorithm	Security of Key Generation Algorithm
UMTS-3G Confidentiality	UEA1 Same* as A5/3	128	MILENAGE f3	Same as above
	UEA2 Snow 3G (608-bit state)	128	MILENAGE f3	Same as above
UMTS-3G Integrity	UIA1 32-bit MAC based on KASUMI Enhanced CBC-MAC	128	MILENAGE f4	Secure if based on AES-128. Theoretically proven that MILENAGE algorithms are jointly secure if the kemel block cipher is secure.
	UIA2 32-bit MAC based on Galois MAC and Snow 3G Universal hashing and one-time pad masking (64-bit state)	128	MILENAGE f4	Same as above
LTE-4G Confidentiality	128-EEA1 Same ad UEA2	128	MILENAGE f3	Same as above
	128-EEA2 Based on AES-128 Counter mode	128	MILENAGE f3	Same as above
	128-EEA3 ZUC (560-bit state)	128	MILENAGE f3	Same as above
LTE-4G Integrity	128-EIA1 Same ad UIA2	128	MILENAGE f4	Same as above
	128-EIA2 32-bit MAC based on AES-128 CMAC mode	128	MILENAGE f4	Same as above
	128-EIA3 32-bit MAC based on ZUC Uniform universal hashing and one-time pad masking (32-bit state)	128	MILENAGE f4	Same as above

Figura 2 - Algoritmi Reti 3G e 4G

3 Sicurezza dei terminali

I dispositivi mobili sono esposti sia al rischio di furto o smarrimento sia alla possibilità di essere violati attraverso l'installazione di app non sicure e tutto ciò può determinare la compromissione delle informazioni in essi memorizzate, sia di tipo personale che legate al mondo lavorativo. Occorre inoltre evidenziare la scarsa adozione di strumenti di protezione anche se ormai ampiamente disponibili sul mercato e in grado di offrire diverse funzionalità tipo anti-*malware*, anti-theft, cifratura dei dati, ecc.

Un altro aspetto da considerare ai fini della sicurezza dei dispositivi è che, nel mondo mobile, la catena di produzione, certificazione e rilascio delle *patch* è molto più articolata e complessa rispetto a quanto accade ad esempio in ambito fisso. Gli attori coinvolti sono, infatti, molteplici: il fornitore del sistema operativo (OS), il produttore del dispositivo ed infine l'operatore mobile. Ciò comporta quindi un allungamento dei tempi di disponibilità degli aggiornamenti, a vantaggio degli attaccanti che mediamente possono sfruttare le vulnerabilità per un periodo più lungo.

Sul tema della sicurezza dei terminali mobili dallo scorso anno, come Security Lab, abbiamo avviato un processo sistematico di analisi e valutazione del livello di sicurezza offerto dai diversi sistemi operativi mobile. In particolare uno degli obiettivi è quello di analizzare i framework di sicurezza delle diverse piattaforme, sia da un punto di vista teorico, come modello di base, sia da un punto di vista pratico, effettuando dei veri e propri security assessment sui dispositivi, scelti tra quelli certificati TI (*Telecom Italia*).

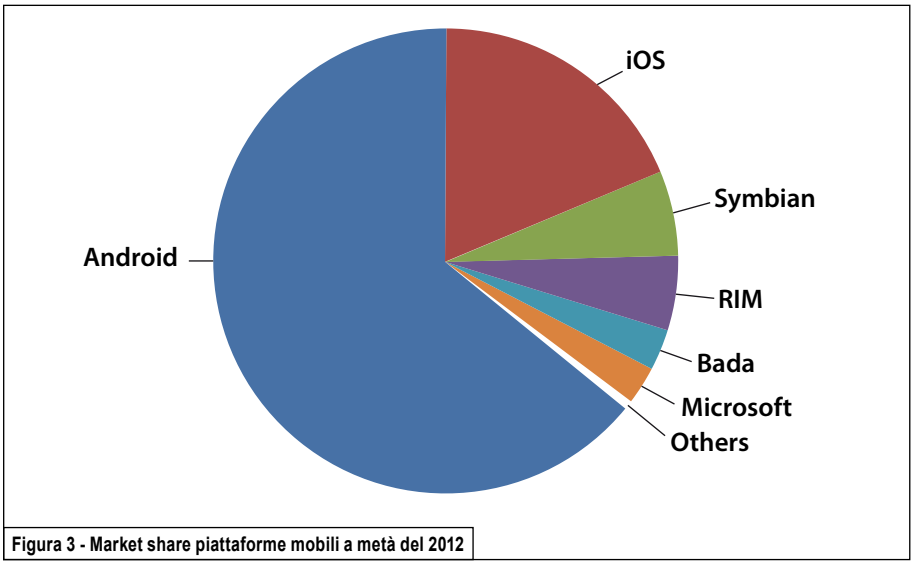


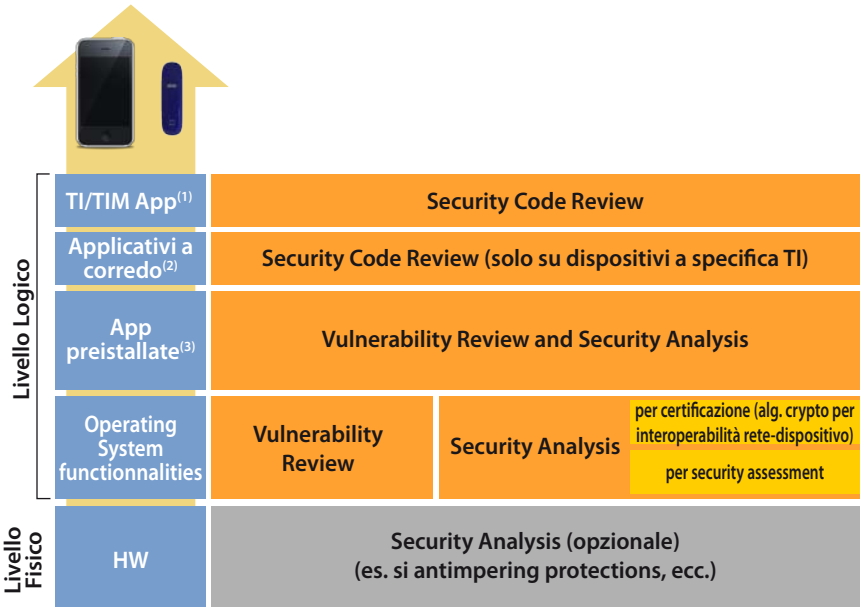
Figura 3 - Market share piattaforme mobili a metà del 2012

L'analisi è in questo momento focalizzata sulle piattaforme maggiormente diffuse che, come mostrato anche dalla Figura 3 sono Android con il 64,1%, seguito da iOS con il 18,8%, Symbian con il 5,9% e RIM con il 5,2% [12].

In quest'analisi abbiamo incluso anche la piattaforma WindowsPhone, considerata la previsione di crescita del relativo market share [13].

In Figura 4 è schematizzato il processo di sicurezza per i dispositivi mobili introdotto in TI che vede coinvolti, oltre al Security Lab, la

Figura 4 - Processo di assessment dei dispositivi mobili



(1) la sicurezza delle App e brand TI/TIM contribuiscono al livello di sicurezza complessivo del dispositivo smartphone/tablet
(2) es. sw applicativo di gestione es. per utilizzo/aggiornamento Internet Key
(3) App standard incluse nel sistema operativo di base

funzione Certificazione E Sviluppo Terminali del Marketing e l'Ingegneria Device Mobili di Tilab.
Facendo riferimento allo schema riportato in questa figura, al livello più basso si collocano le analisi di sicurezza del livello fisico (HW), previste nel caso sia utile misurare, ad esempio per specifici dispositivi, l'efficacia delle misure di protezione di tipo anti-tampering. Questo tipo di analisi richiede competenze e strumenti disponibili presso pochi laboratori a livello internazionale; pertanto, se necessarie, vengono realizzate con un supporto esterno.
Sopra il livello HW si collocano le attività di verifica delle funzionalità offerte dal sistema operativo. Queste, insieme all'analisi di sicurezza e di vulnerabilità delle app di base, sono eseguite tramite:

1) l'analisi dei modelli di sicurezza delle piattaforme mobili;
2) l'esecuzione dei security assessement.

Da tale attività scaturisce anche l'identificazione dei requisiti di sicurezza, classificati in mandatori, piuttosto che raccomandati o opzionali, per i terminali a marchio TI.
Per i dettagli relativi ai due livelli superiori, security code review e analisi delle app pre-installate nei dispositivi certificati TI, o disponibili sugli store e pubblicate a marchio TI, si rimanda al capitolo successivo.
Entrando invece un po' più nel merito dei Device Security Assessment si può dire che ci permettono di stimare il livello di rischio associato all'uso di un determinato dispositivo attraverso l'analisi del livello di maturità delle funzionalità di sicurezza.
Le verifiche sono raggruppate in 4 categorie principali, ciascuna delle quali comprende specifiche funzionalità di sicurezza: AC (*Access Control*), DP (*Data Protection*), NS (*Network Security*) e AS (*Application Security*), intesa quest'ultima per gli aspetti di valutazione del modello di sicurezza adottato per le app. La valutazione di ciascuna funzionalità di sicurezza è eseguita in base ad una scala di valori da 0 a 3 ed indicano rispettivamente se la funzionalità non esiste (0), esiste ma non è operativa (1), è parzialmente supportata (2) o è correttamente implementata (3). La media dei risultati di ciascuna categoria concorre a calcolare il valore finale di stima affidabilità del SO, detto Average Score (Avg Score). La seguente tabella riassume l'esito dell'assessment effettuato su alcuni dispositivi nel corso dello scorso anno.
A seguito degli *assessment* abbiamo sviluppato delle linee guida di *hardening dei dispositivi* ovvero delle configurazioni sicure che possono essere utilizzate come riferimento.
Sempre sul fronte sicurezza dei dispositivi mobili forniamo poi i requisiti di sicurezza, da considerare per i terminali che seguono l'iter di certificazione Telecom Italia, confrontandoci con Marketing Device per la determinazione del livello di obbligatorietà.

4 Sicurezza delle applicazioni

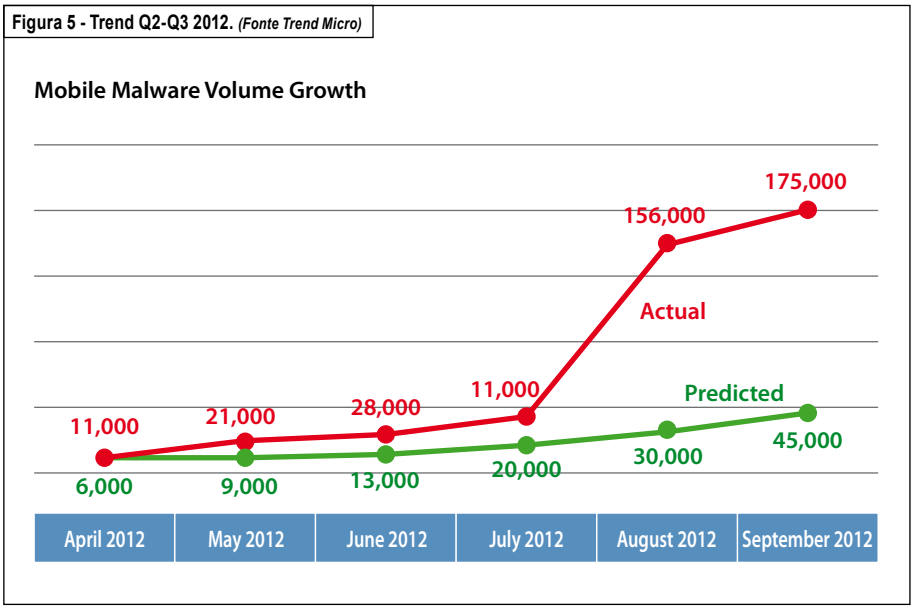
Infine analizziamo il tema della sicurezza delle mobile app. Abbiamo visto come l'affermarsi dei dispositivi di tipo smartphone sia legato all'affermarsi di sistemi operativi aperti e in grado di mettere a disposizione ambienti di sviluppo utili per codificare applicazioni in grado di sfruttare tutte le funzionalità dei dispositivi.
In virtù dell'elevato tasso di penetrazione degli *smartphone*, delle funzionalità offerte e dei

Tabella 1 Esito security assessment di alcuni dispositivi

Produttore	Modello	Sistema Operativo	AC	DP	NS	AS	Avg Score
APPLE	iPhone 4S	iOS 6.0	2,4	2,6	1,93	2	2,23
APPLE	iPhone 4	iOS 5.1.1	2,4	2,6	1,93	2	2,23
RIM	BlackBerry Torch 9800	RIM OS 6.0.0.570	3	2,79	2,28	2,6	2,67
RIM	BlackBerry Bold 9900	RIM OS 7.1.0.190	3	2,8	2,31	2,6	2,68
NOKIA	LUMIA 710	WINDOWS PHONE 7.5	1,4	1,87	1,7	2	1,74
SAMSUNG	GT-S5660	ANDROID 2.3.6	1,4	1,24	1,93	2	1,64
NOKIA	LUMIA 610	WINDOWS PHONE 7.5	1,4	1,87	1,7	2	1,74
SONY ERICSSON	XPERIA ST21i	ANDROID 4.0.3	1,4	1,25	2,04	2	1,67
HTC	WILDFIRE S A510e	ANDROID 2.3.6	1,4	1,19	1,93	2	1,63
HTC	DESIRE C	ANDROID 4.0.3	1,4	1,41	1,89	2	1,68
SAMSUNG	GT-I5500	ANDROID 2.1.1	1,25	1,31	1,82	2	1,59

nuovi sistemi operativi, l'interesse da parte delle comunità di sviluppatori verso le nuove piattaforme è cresciuto sempre di più e parallelamente anche quello degli ideatori e sviluppatori del *mobile malware*.
Il primo campione di *malware* per *smartphone* risale al 2004, si chiamava Cabir ed era un *worm* per il sistema operativo Symbian sviluppato per dimostrare come il fenomeno dei virus potesse riguardare anche il mondo mobile. Nel corso di tutto il 2004 e 2005 furono poi rilevati altri malware sostanzialmente sempre per la piattaforma Symbian. Successivamente cominciarono a diffondersi i primi *malware* per ambienti J2ME (*Java Micro Edition*). Questa piattaforma permetteva di superare il problema della frammentazione dei sistemi operativi, consentendo così di creare *malware* eseguibili su piattaforme diverse. In particolare nel 2009 si assistette a una vera e propria esplosione di malware per J2ME capaci di inviare SMS a numerazioni premium, di sottoscrivere le vittime a servizi a pagamento ecc. senza che l'utente ne fosse consapevole. Dal 2010 il fenomeno del *malware* ha subito una rapida crescita [Figura 5] grazie al fatto che nel solo 2010 il tasso di penetrazione degli *smartphone* era cresciuto del 70% rispetto all'anno precedente e in quell'anno fu rilasciata sul mercato la piattaforme aperta Android.
I trend più recenti relativi al fenomeno del *mobile malware* evidenziano come il sistema operativo maggiormente preso di mira sia oggi Android e che l'89% del malware sia di fatto collegato al cosiddetto *repackaging* di applicazioni note per questa piattaforma (fonte RSA).
Le ragioni di questi numeri sono da ricondurre principalmente alla mancanza di vincoli stringenti per l'installazione di applicazioni sui dispositivi Android (al contrario di Apple che permette l'installazione di applicazioni solo da iTunes, a meno di non avere un dispositivo *jailbroken*, in cui tutte le applicazioni sono eseguite come root e i controlli tipici di iOS sono stati rimossi). Questa politica scelta da Google ha favorito la proliferazione di mercati alternativi attraverso cui gli sviluppatori di *malware* possono veicolare facilmente le proprie applicazioni malevole.
Quali sono le caratteristiche e le frontiere del *mobile malware*? Questi nuovi *malware* combinano le vecchie funzionalità quali ad esempio l'invio di SMS a nuove funzionalità che permettono di recuperare dal dispositivo una quantità di dati, prima non disponibili o difficilmente accessibili, il cui valore commerciale sui mercati underground è considerevole e tale da suscitare l'interesse di vere e proprie organizzazioni criminali. Ad esempio le liste di IMEI validi possono essere particolarmente allettanti per le associazioni criminali che devono rimettere sul mercato dispositivi rubati e che altrimenti, grazie ai controlli messi in campo dagli operatori, potrebbero essere inutilizzabili; i dati personali degli utenti possono essere sfruttati per la pubblicità; i numeri di telefono per lo SPAM via SMS; i numeri di carte di credito per le frodi su Internet e così via. L'industria che gravita intorno al *malware* per le piattaforme mobili è divenuta matura e rappresenta oggi una fonte redditizia per gli attaccanti, con veri e propri modelli di business.
In termini di sofisticazione del *malware*, si sta assistendo ad un replica di quanto è accaduto in ambito fisso, ma con tempi di evoluzione decisamente più rapidi.
Le tecniche di distribuzione del mobile *malware* sono molteplici; si adottano meccanismi di tipo "*Drive by download*", per cui una pagina web viene appositamente compromessa per avviare il

Figura 5 - Trend Q2-Q3 2012. *(Fonte Trend Micro)*



download di una app malevola quando visitata; altra tecnica è la pubblicità malevola (*Malvertising*), per cui lo sviluppatore di un *malware* compra della pubblicità legittima per indirizzare gli utenti a scaricare copia del *malware* su market leciti oppure su market di *phishing* creati appositamente per imitare quelli leciti; altra pratica molto comune è il già citato *repackaging*; in questo caso l'attaccante decompila un'applicazione legittima (tipicamente gioco, utility o porno), include nella nuova versione il codice malevolo e infine la pubblica nuovamente su un market, per lo più di terze parti, o su un sito. Quest'ultima tecnica risulta abbastanza efficace in quanto è difficile per un utente identificare la differenza tra un'app legittima e quella contraffatta.

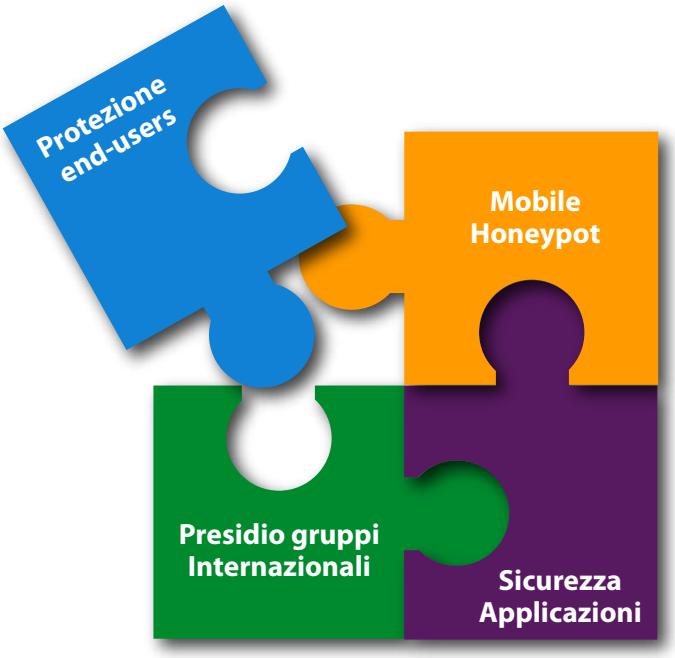


Figura 6 - Attività Telecom Italia sul tema mobile malware

Quali sono invece i problemi derivanti dalla propagazione del *malware* per un operatore mobile? Dal punto di vista di un operatore mobile, il fenomeno della propagazione del *malware* può avere degli impatti importanti che vanno dalla gestione dei reclami al Customer Care da parte degli utenti, per erosione del credito o per malfunzionamento dei dispositivi, alla riduzione dei ricavi a causa di frodi, all'overload sulle proprie infrastrutture, in termini di segnalazione e dati scambiati, alla possibilità di attacchi di *denial of service* verso specifici servizi. Come esempio può essere citato il virus Guardian0.95/HatiHati [5] per dispositivi Symbian S60 che nel 2009 creò un disservizio all'infrastruttura di messaggistica di molti operatori nel *Middle East*.

Come Security Lab stiamo approcciando in modo sistematico il problema del mobile *malware* con una serie di attività e iniziative che spaziano dal presidio dei gruppi internazionali attivi su questo tema quali il MMG (*Mobile Malware Group*) della GSMA, alla definizione di strumenti per valutare la sicurezza delle applicazioni mobili, alla distribuzione di bollettini sui nuovi campioni di *malware* individuati di volta in volta presso i nostri stessi laboratori o da altri esperti del settore, al dispiegamento di un'infrastruttura di *honeypot* specifica per il mondo mobile.

Nell'ambito della partecipazione al MMG, collaboriamo invece attivamente con altri operatori mobili e vari produttori di dispositivi e antivirus per la condivisione di informazioni sui *malware* quali ad esempio le modalità di infezione, i numeri premium usati per defraudare il credito, le url connesse al funzionamento del *malware*, le tecniche di rimozione. Tali informazioni spesso si rivelano molto utili sia alle funzioni del *Customer Care* per garantire un adeguato supporto ai propri clienti sia alle funzioni Antifrode per rilevare e tracciare eventuali azioni fraudolente a danno di utenti i cui dispositivi siano stati infettati.

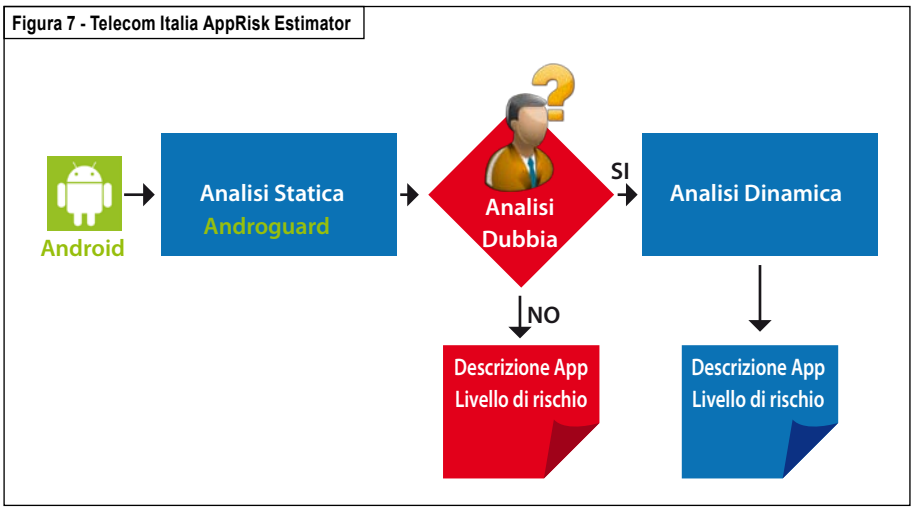
Un altro ambito di intervento è quello collegato allo sviluppo, sempre in ambito GSMA, di linee guida [11] utilizzabili dai vari operatori per ridurre sia gli impatti sulle proprie infrastrutture che le eventuali perdite economiche derivanti dalle frodi che possono essere collegate al fenomeno del mobile *malware*.

4.1 Sviluppo di applicazioni sicure

Sul fronte della sicurezza delle applicazioni mobili abbiamo attive diverse iniziative.

In particolare, abbiamo reso disponibili a tutte le funzioni aziendali che sviluppano applicazioni mobili delle linee guida per lo sviluppo di app mobili più sicure. Inoltre si sta lavorando con la funzione Marketing Device affinché anche le terze parti ingaggiate per lo sviluppo di app per conto di TI seguano processi di sviluppo sicuro.
Parallelamente, abbiamo sviluppato un sistema denominato *Apps Risk Estimator* che permette di analizzare, in ottica sicurezza, applicazioni Android. Il sistema è costituito da due moduli principali: il primo implementa l'analisi statica, mentre il secondo quella dinamica [Figura 7].
Per l'analisi statica, è stato sviluppato, in collaborazione con il Politecnico di Torino, un software basato sul tool open-source Androguard [6]. Questo strumento analizza automaticamente i permessi richiesti dall'applicazione, i file presenti nell'archivio *apk*, ricerca dei pattern di comportamento classificati come rischiosi e, infine, ne determina un livello di rischio globale. Tale livello è calcolato usando un algoritmo in logica *fuzzy* che elabora 12 differenti categorie di rischio individuate, ad esempio, sulla base dei permessi dichiarati nel file *manifest* e utilizzati implicitamente, sull'eventuale caricamento dinamico di risorse esterne (librerie, classi), sul rischio che l'applicazione possa eseguire un exploit e ottenere i permessi di root, sull'utilizzo di API pericolose quali quelle che permettono di intercettare e/o inviare SMS, fare chiamate, cambiare la configurazione del dispositivo.
Oltre all'analisi statica, è utilizzato anche lo strumento open-source denominato DroidBox [10] che permette invece di effettuare un'analisi dinamica delle applicazioni. Questo tool è costituito da un emulatore di Android che ha al suo interno un kernel opportunamente modificato e nel quale viene installata l'applicazione da analizzare. Il sistema intercetta, classifica e salva in un report tutte le operazioni eseguite dall'app (es. connessioni di rete, cifratura/decifratura, invio SMS ecc.).
Il sistema Apps Risk Estimator è stato anche utilizzato per condurre un *assessment* di circa 82000 applicazioni gratuite scaricate dal market ufficiale di Android per capire la qualità, in ottica sicurezza, delle applicazioni pubblicate e quali eventuali rischi potevano rappresentare per gli utenti finali. Il risultato ottenuto è stato che circa il 33% delle applicazioni analizzate comportavano potenzialmente un rischio, in termini di violazione privacy ed eventuale danno economico, per l'utente che le avesse installate, confermando i trend pubblicati da alcuni enti di ricerca internazionali quali la Carnegie Mellon University [7, 8, 9].
Inoltre durante l'analisi sono state direttamente rilevate una decina di applicazioni, successivamente rimosse dallo store, che nascondevano al loro interno dei veri e propri componenti malevoli.

Figura 7 - Telecom Italia AppRisk Estimator



4.2 Il progetto internazionale NEMESYS per il contrasto del mobile malware

Sul fronte del monitoraggio e del contenimento della propagazione del malware sulle nostre reti, abbiamo iniziato ad utilizzare la tecnologia dei mobile honeypot e stiamo partecipando ad un progetto finanziato dalla Comunità Europea denominato "*Enhanced Network Security for Seamless Service Provisioning in the Smart Mobile Ecosystem*" o *NEMESYS*.
Il principale scopo del progetto è proprio quello di sviluppare nuove tecnologie di sicurezza per i dispositivi di tipo smartphone e realizzare strumenti innovativi di monitoraggio e sicurezza, che possano essere utili sia all'utente finale, sia agli operatori mobili, Figura 8. In particolare all'interno di questo progetto si realizzerà un'infrastruttura (hardware e software) che, a partire dall'osservazione di specifici eventi sul

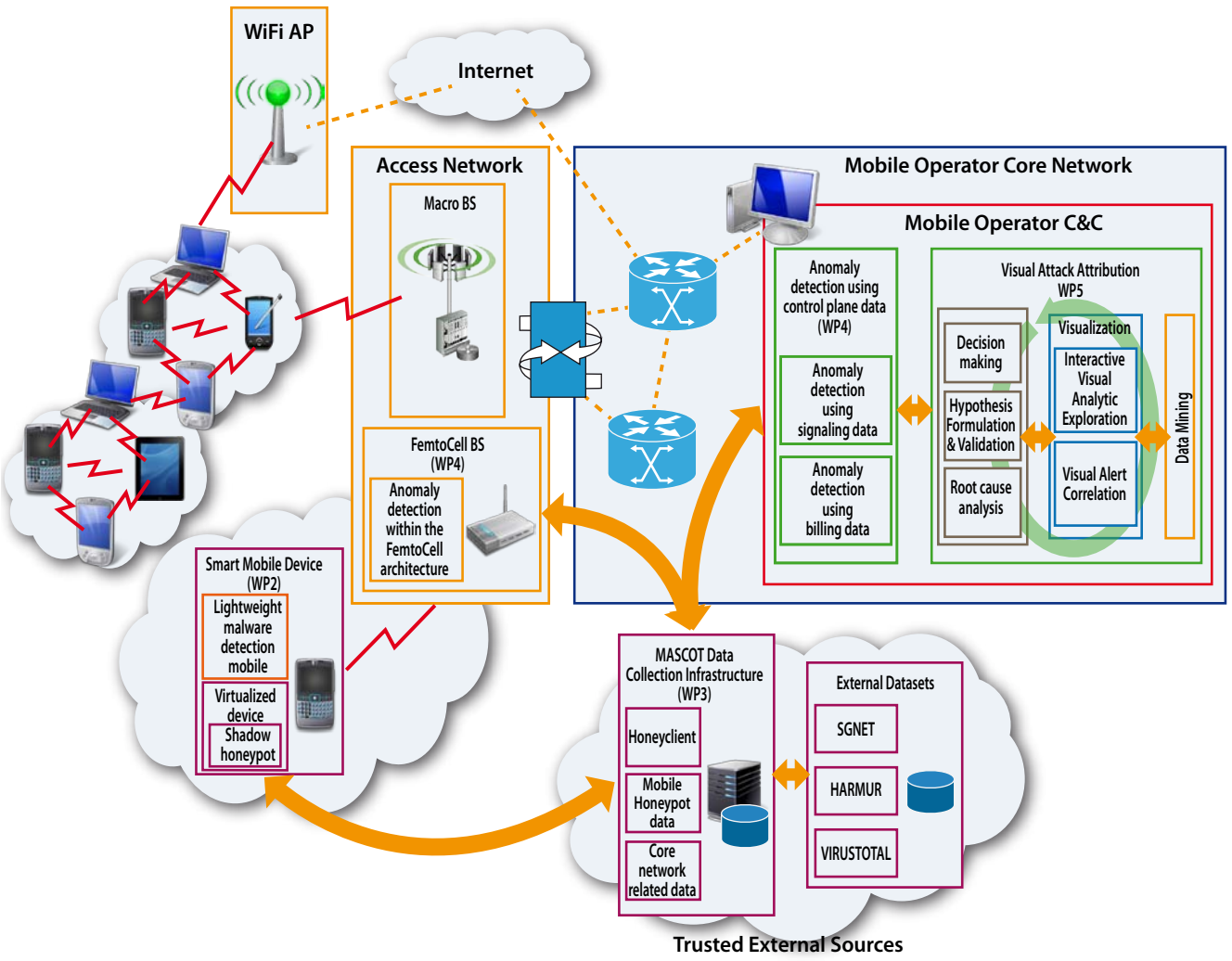


Figura 8 - Architettura piattaforma NEMESYS

traffico raccolto (es. attacchi indirizzati ai dispositivi e alle reti mobili), cercherà di predire nuove minacce (es. DoS sulla segnalazione, propagazione malware, ecc.). Le attività del progetto sono partite lo scorso novembre e vedono coinvolti sei partner: Imperial College London (i coordinatori), Centre for Research and Technology Hellas – Informatics and Telematics Institute (Grecia), COSMOTE Mobile Telecommunication S.A. (Grecia), la società spagnola Hispsec (creatori di Virustotal), la Technische Universitat Berlin (Germania) e Telecom Italia Information Technology con il Security Lab.

Conclusioni

L'eco-sistema mobile, in continua evoluzione e trasformazione, dal punto di vista della sicurezza rappresenta oggi per l'operatore una sfida che va combattuta su diversi fronti, ma anche una grande opportunità. Il perimetro della sicurezza mobile è infatti molto ampio e tecnologicamente articolato: esso spazia dalla sicurezza della rete, ai modelli di sicurezza dei diversi sistemi operativi e alla sicurezza delle app. Telecom Italia è fortemente impegnata in questa sfida e contribuisce costantemente al monitoraggio e all'analisi dei nuovi trend di minaccia, ma anche all'elaborazione e alla sperimentazione di nuove tecnologie e servizi che possano garantire, ai

nostri Clienti, un livello di protezione sempre maggiore ■

Bibliografia

[1] *http://countermeasures.trendmicro.eu/wp-content/uploads/2012/02/History-of-Mobile-Malware.pdf*
[2] *http://gsmmap.org/cgi-bin/gsmmap.fcgi?risk=1*
[3] *http://www.itu.int/ITU-D/ict/statistics/at_glance/KeyTelecom.html*
[4] *http://mobithinking.com/mobile-marketing-tools/latest-mobile-stats/b#mobilebroadband*
[5] *http://www.binyahya.com/books/book_manager/?p=20*
[6] *http://code.google.com/p/androguard/*
[7] *http://tecnologia.ondenews.it/android/41-applicazioni-android-mettono-a-rischio-privacy-utenti/3916/*
[8] *http://www.webnews.it/2013/01/17/applicazioni-android-e-rischi-per-i-dati-personali/#ixzz2KhFkSV9s*
[9] *http://www.androidworld.it/forum/applicazioni-17/come-proteggersi-dai-permessi-delle-app-47170/*
[10] *http://code.google.com/p/droidbox/*
[11] Operator Guide to Mobile Malware, v3.0, May 2012
[12] Gartner "Market Share: Mobile Devices, Worldwide, 2Q12."
[13] *https://www.strategyanalytics.com/default.aspx?mod=reportabstractviewer&a0=7834*

roberta.damico@it.telecomitalia.it
rosalia.dalessandro@it.telecomitalia.it
marcello.fausti@it.telecomitalia.it

Rosalia d'Alessandro
Senior Security Engineer nel gruppo Security Lab della struttura Technical Security, si occupa dal 2004 della sicurezza dei dispositivi mobili. Dal 2011 si è dedicata anche alla sicurezza delle reti mobili con attività di analisi delle vulnerabilità e testing. In ambito internazionale, partecipa al Security Group della GSMA e ai suoi sottogruppi. In passato le sue attività si sono concentrate anche sulla sicurezza delle reti fisse e in particolare sulla sicurezza del traffico DNS, sui sistemi di strong authentication basati, ad esempio, su autenticazione biometrica e one time passwords, su intellectual properties. È autrice di articoli e brevetti nelle aree di interesse. Ha conseguito la laurea in Ingegneria delle Telecomunicazioni presso l'Università Federico II di Napoli nel 2000.

Roberta D'Amico
laureata in Scienze dell'Informazione presso l'Università degli Studi di Torino e ha conseguito il Master COREP in Telecomunicazioni nel 1996. È entrata in CSELT (Centro Studi E Laboratori di Telecomunicazioni) nel 1994 e dal 1996 fa parte del gruppo dedicato alla sicurezza dell'informazione, oggi Security Lab in Telecom Italia Information Technology. Inizialmente si è occupata di sistemi di pagamento elettronici e firma digitale, successivamente di autenticazione biometrica e ricerca e sviluppo per la sicurezza delle applicazioni e dell'accesso alle reti di nuova generazione. Negli ultimi anni ha affrontato prevalentemente la tematica della sicurezza delle reti mobili e della diffusione e contrasto dei malware. È attualmente responsabile del gruppo Cyber Security Threat Evolution.

Marcello Fausti
VP Technical Security dal 2009. Inizia la sua carriera nel 1983 in società di software, impegnato nella conduzione di progetti presso grandi clienti pubblici e privati. Dal 1993 al 1998 è in Olivetti SpA come Marketing Manager della divisione PA. Dal 1998 al 2000 è in GFI-OiS SpA come VP Marketing & Business Development. Entra nel Gruppo Telecom Italia nel 2000 e fino al 2005 è in Telecom Italia Mobile SpA come VP e-Company, con l'incarico di sviluppare le attività di e-business nel rapporto con partner, fornitori, canali distributivi ed employee. Dal 2005 al 2008 è in Telecom Italia come VP HR Information Systems. Ha conseguito la laurea in Economia Aziendale (ICT Management for Business) e il master EMIT in IT Governance & Management presso la LUISS Guido Carli di Roma.

Usa il tuo smartphone per visualizzare approfondimenti multimediali

CYBERSECURITY E LOTTA ALLE BOTNET

Stefano Brusotti, Luciana Costa, Paolo De Lutiis

La cybersecurity ha nel contrasto del malware e delle botnet, cioè i mezzi più usati dalla criminalità informatica per sferrare i suoi attacchi, uno degli obiettivi principali. Operatori e ISP possono svolgere un ruolo chiave nell'identificazione e nella mitigazione di questi fenomeni. La UE crede fortemente in un'iniziativa comunitaria e stanzia oltre 7 milioni di euro per dimostrare, attraverso appositi esperimenti, l'efficacia a livello continentale, di modelli di azione coordinata e congiunta.

1 Introduzione

Negli ultimi anni le attività compiute dai criminali informatici si sono contraddistinte per una crescita costante e inarrestabile, caratterizzata da una duplice trasformazione: da una parte l'affermarsi di un modello di crimine informatico, differente rispetto al passato, in quanto organizzato. Dall'altra nuove minacce tecnologiche, sempre più insidiose e avanzate.
In effetti, si è in presenza di vere e proprie reti criminali gestite da soggetti motivati da profitti importanti e duraturi, derivanti, ad esempio, dalla vendita di dati personali, dalle truffe online o dalle estorsioni e ricatti. L'obiettivo non è più la notorietà degli attaccanti, ma l'implementazione di un vero modello di business, il più possibile stabile ed in grado di sopravvivere nel tempo. Queste reti criminali riescono, spesso anche facilmente, ad eludere i sistemi di difesa basati sul riconoscimento di firme di attacco note o su analisi comportamentali. Il più delle volte il *malware* viene ideato in modo da imitare le applicazioni di rete legittime e riprodurre modelli di traffico riconducibili a condizioni di normalità. Inoltre, il codice malevolo viene modificato molto più rapidamente di quanto i produttori di soluzioni di sicurezza tradizionali siano in grado di fare.
In questo scenario, le botnet (reti di dispositivi compromessi da *malware* e controllate da remoto) rappresentano l'infrastruttura preferenziale utilizzata dai cybercriminali per lanciare praticamente ogni tipologia di attacco: dallo spionaggio industriale al furto di dati e identità, dallo spam agli attacchi DDoS, ed altri ancora. Mediante l'impiego di risorse computazionali ottenute in modo illecito, molto spesso personal computer compromessi, e distribuite a livello mondiale, i cyber criminali sono, infatti non solo in grado di amplificare significativamente l'impatto e la portata dei loro attacchi, ma anche di occultare la loro vera identità e posizione.
Accanto alla crescente sofisticazione del *malware* e delle botnet in genere, un altro fattore che non va trascurato è quello dell'*ingegneria sociale* che rimane uno degli strumenti più utilizzati dai gestori delle botnet e dalla criminalità in genere. Questa tecnica si rivela decisamente efficace nel riuscire ad ottenere informazioni sensibili facendo leva sul fattore umano, molto spesso l'anello debole per la sicurezza. Inoltre, ha il vantaggio di non poter essere facilmente contrastata. Occorre infatti identificare da un lato soluzioni che minimizzino la possibilità, per gli utenti, di divenire vittime di questi attacchi, dall'altro agire sul piano della formazione, per sensibilizzare gli utenti stessi sulle problematiche della sicurezza informatica, promuovendo comportamenti consapevoli e conservativi.

2 Malware e botnet

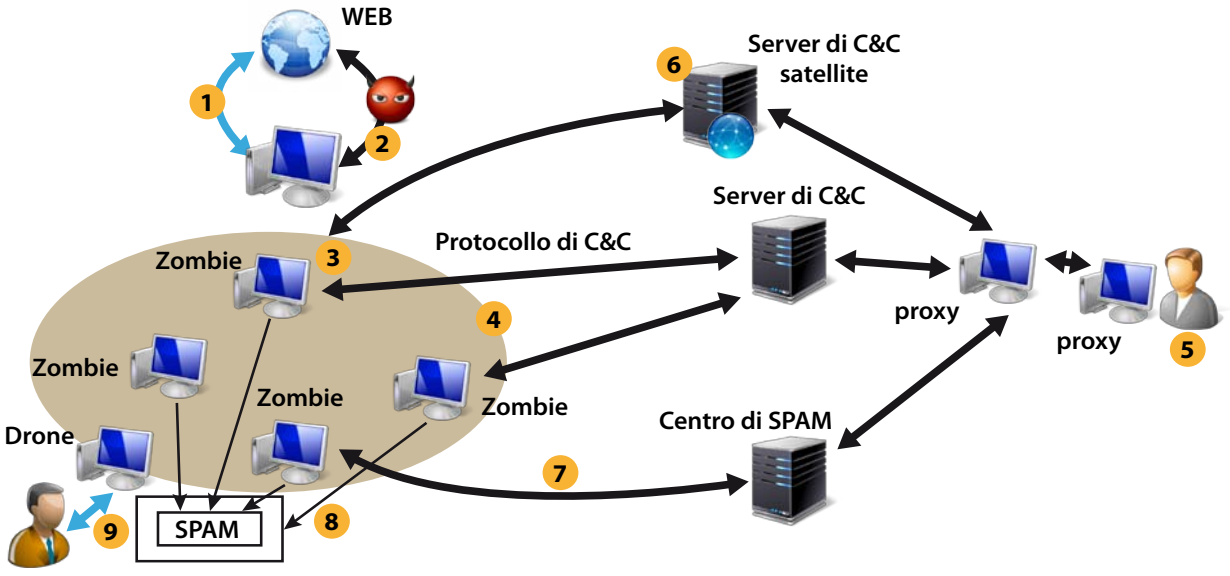
Una *botnet* si configura come una rete di dispositivi compromessi, la cui principale peculiarità è la pos-

sibilità di comandarla da remoto per mettere in atto svariate attività illecite.
Il processo di compromissione è finalizzato all'esecuzione di codice malevolo, spesso riferito con il termine di *malware* o *bot*, sul dispositivo vittima per trasformarlo in una sorta di *zombie* a completa disposizione di un controllore esterno. Il *malware* può essere distribuito attraverso svariate modalità; inserito direttamente come allegato, o indirettamente come link, all'interno di mail malevole il cui contenuto, costruito sfruttando tecniche di *social engineering*, induce gli utenti al download e all'esecuzione. In altri casi, invece, l'esecuzione del *malware* avviene automaticamente sfruttando vulnerabilità presenti nei sistemi operativi o in applicativi di largo utilizzo, quali i browser o i loro plug-in, all'insaputa dell'utente.
In Figura 1 viene presentata una tipica sequenza di infezione da bot finalizzata ad illustrare le interazione tra i diversi componenti di una botnet e la comunicazione con il centro di C&C (*Command&Control*), propedeutica per la preparazione di un'attività malevola.

2.1 Come rilevare una botnet?

Il rilevamento di una botnet non è un obiettivo facilmente perseguibile. Le tecniche adottabili possono, in generale, essere classificate in tre principali categorie: *host-based, network-based* e tecniche incentrate sull'analisi del protocollo DNS.
Le tradizionali tecniche di rilevamento puramente *host-based* (ad esempio gli strumenti anti-virus) seppur possono essere efficaci nel riconoscimento del *malware* e dei comportamenti anomali a livello di host (ad esempio l'invocazione di specifiche sequenze di chiamate di sistema o la creazione di particolari chiavi di registro), presentano alcuni limiti nel contesto delle botnet. In primo luogo, basandosi sull'uso di firme di attacco (*signature*) richiedono frequenti aggiornamenti, al fine di ridurre la finestra temporale di esposizione degli utenti. In secondo luogo,

Figura 1 - Sequenza di infezione da bot



1. Un utente seleziona un URL segnato in un messaggio di spam
2. Raggiunge un sito, compromesso ad-hoc, da cui scarica involontariamente un malware di tipo bot
3. La macchina viene compromessa e trasformata in zombie, divenendo parete di una botnet
4. Le macchine zombie comunicano con il server di C&C attraverso un protocollo di C&C
5. Il server C&C e amministrato e comandato dal botmaster, o bot herder, attraversouno o più proxy intermedi
6. Il server C&C satellitare fornisce un sito web da cui gli zombie scaricano aggiormamenti del malware
7. Gli zombie ricevono informazioni aggiornate dal Centro spam per una nuova campagna di spam
8. Gli zombie inviano lo spam, in base alle istruzioni ricevute
9. Tramite un drone, spacciato per un reale bot, è possibile analizzare una botnet dal suo interno

questi strumenti possono essere elusi semplicemente aggiornando il codice maligno con una frequenza maggiore rispetto alle stesse firme. Sono, infatti, sempre più numerosi i *malware* in grado di replicarsi creando una nuova istanza a ogni infezione, così come i server in grado di distribuire binari malevoli "personalizzati" per ciascuna vittima. Infine, i bot tendono a nascondersi all'interno delle macchine infette, in modo silente, senza comportare un consumo significativo della memoria o delle altre risorse. Spesso possiedono, sull'host infettato, gli stessi privilegi di un sistema di rilevamento *host based* con la possibilità pertanto di disabilitare il sistema anti-virus in uso o di utilizzare tecniche di *rootkit* per offuscare la propria presenza.
Questi fattori rendono pertanto necessaria l'ideazione di nuove strategie di rilevamento da affiancare a quelle più tradizionali. In tal senso, le tecniche di tipo *host-based* emergenti per il contrasto delle botnet sono pressoché incentrate sull'adozione di un approccio di tipo "semantico". Esse mirano all'identificazione dei comportamenti tipici del *malware* senza fare uso di database di *signature* e comunque minimizzando, o eliminando laddove possibile, la necessità di disporre di informazioni "a priori" sul *malware* da rilevare. Alcune riprendono il paradigma dell'*anomaly detection* e sono finalizzate a monitorare i processi in esecuzione su di un particolare host al fine di rilevare quelle sequenze tipiche associabili a bot. Questo richiede ovviamente la definizione di un modello di comportamento del *malware* su cui poi incentrare il monitoraggio.
Le tecniche *network-based* possono essere viste come misure complementari rispetto alle precedenti soluzioni. Esse mirano ad individuare sulla base dell'osservazione del traffico di rete, l'esistenza di un'infrastruttura malevola, dei relativi bot e/o dei server di C&C. Anche in questo caso i classici metodi di rilevamento richiedono comunque un affiancamento di strategie di nuova concezione. I tradizionali sistemi IDS

Sequenza di infezione da bot

Il passo 1 si riferisce al momento in cui un utente viene, a sua insaputa, infettato, visitando, ad esempio, un sito web, preventivamente compromesso, referenziato ad esempio all'interno di un messaggio di spam. Un classico esempio è rappresentato dagli attacchi di tipo drive by-download in cui un'utente viene indotto a scaricare ed eseguire del malware da siti web senza esserne consapevole (passo 2). Una volta compromesso, il dispositivo dell'utente si trasforma in uno zombie (passo 3) e diviene parte della rete di bot. L'entità preposta al comando dell'infrastruttura malevola è spesso riferita come botmaster o anche bot herder. Questa si avvale di efficienti meccanismi di Comando e Controllo (C&C), per distribuire i comandi da eseguire, ricevere informazioni sullo stato dei bot e delle loro attività, aggiornare i componenti software del malware, raccogliere i dati sottratti agli utenti e così via. Nello specifico, gli elementi alla base di questi meccanismi sono il server di C&C e il protocollo con il quale i bot ed il server comunicano (passo 4). Per mascherare e proteggere la propria identità, il botmaster spesso si avvale di uno o più livelli di intermediazione (passo 5), prima di arrivare ad amministrare e pilotare la macchina su cui è ospitato il centro di C&C. Il fine è proprio quello di aumentare la resilienza della botnet ossia la sua capacità di resistere a tentativi, da parte delle forze dell'ordine, di blocco e di tracciamento del server di C&C con l'impossibilità, per quest'ultimo, di impartire comandi e distribuire gli aggiornamenti software. In alcuni casi, l'architettura di C&C prevede anche il cosiddetto server di C&C satellite, ossia un host remoto il cui ruolo è quello di fornire un supporto all'attività di gestione e comando degli zombie; in genere questi server mettono a disposizione una risorsa web dalla quale gli zombie possono scaricare aggiornamenti software o nuove istruzioni da eseguire (passo 6). Le botnet spesso possono essere specializzate anche in funzione del tipo di attività malevola perpetrata. Un esempio rilevante è dato dalle botnet focalizzate sullo spam; in tal caso è presente un centro di spam (passo 7), ossia un host preposto a fornire istruzioni agli zombie su come preparare i messaggi da inviare (template) e a fornire gli indirizzi di posta elettronica dei destinatari delle campagne di spam (passo 8), tipicamente recuperati mediante tecniche di harvesting (raccolta). Infine, al passo 9 è rappresentato il caso in cui un drone viene infiltrato all'interno di una botnet. Spacciato come reale bot al servizio del botmaster, esso viene invece usato per analizzare il comportamento della botnet dal suo interno, con l'intento di raccogliere informazioni preziose per supportare l'identificazione e la realizzazione di specifiche contromisure ■

sono, infatti, incentrati nel monitorare il traffico in ingresso alla rete e sono, in questo contesto, efficaci nell'individuare iniziali tentativi di intrusione. Essi, tuttavia, difficilmente permettono di decretare il successo di un tentativo d'infezione solo sulla base degli allarmi relativi a scansioni e tentativi di intrusione; numerose sono infatti le attività di scansione da parte di macchine zombie alla ricerca di nuove vittime, che si rivelano il più delle volte non fruttuose. Viceversa, è molto più probabile la presenza di un problema quando sono rilevati tentativi di scansione oppure comportamenti riconducibili a bot da parte di host attestati sulla rete interna. Sulla base di queste considerazioni i paradigmi che si vanno affermando ribaltano il punto di osservazione e mirano a identificare quegli host, interni alla rete, intenti a propagare un'infezione verso l'esterno, oppure alla ricerca di un controllo da un'entità remota. Le diverse soluzioni si distinguono sostanzialmente sulla base del meccanismo di monitoraggio adottato (attivo o passivo), sulla dipendenza da specifici protocolli e architetture di rete, sulla tecnica di correlazione utilizzata con il fine di catturare elementi di similitudine nel comportamento delle botnet.

Infine ci sono le tecniche incentrate sull'analisi del protocollo DNS. Nonostante la rapida evoluzione che ha caratterizzato le botnet negli ultimi anni, in termini ad esempio di protocolli di C&C e meccanismi di cifratura, il protocollo DNS continua a rappresentare un elemento basilare per l'organizzazione di una rete di bot, in quanto necessario a localizzare il server con il quale i bot devono comunicare. In aggiunta il protocollo DNS è spesso impiegato dai botmaster per scopi malevoli, finalizzati ad aumentare la resilienza della botnet occultando i server preposti alla distribuzione dei contenuti malevoli (*mothership*) o addetti al coordinamento dei singoli nodi (server di C&C). Questa tecnica che va sotto il nome di *fluxing* in generale prevede la protezione del dominio malevolo, assegnato al server da proteggere, mediante una rapida rotazione degli indirizzi IP che lo risolvono. Questi IP di fatto corrispondono a macchine compromesse (altri bot), in quel momento attive e raggiungibili, ed agiscono da proxy verso la vera *mothership*, nascondendone quindi il reale indirizzo IP. In questo modo lo stesso contenuto verrà acceduto nel tempo mediante indirizzi IP differenti, rendendo sostanzialmente inefficaci eventuali contromisure basate su *blacklist* di IP. Una variante alla tecnica descritta (*single flux*) è il *double flux* dove viene introdotto un secondo livello di protezione mediante l'applicazione di una rotazione anche ai server autoritativi per lo specifico dominio malevolo. Infine una valida alternativa all'IP flux è rappresentata dal *domain flux*. In questo caso invece di far variare rapidamente nel tempo gli indirizzi IP che risolvono uno specifico dominio, viene fatto variare il dominio stesso. Questo obiettivo viene tipicamente raggiunto richiedendo ai bot di collegarsi, a domini differenti ma sempre associati alla stessa infrastruttura di C&C. In questo modo, il blocco preventivo di tutti i domini utilizzati dal botmaster è molto complicato a causa della numerosità stessa dei domini coinvolti nell'operazione.

Ritornando alle tecniche di rilevamento basate sul DNS, molte di queste sono espressamente ideate per identificare botnet di tipo fast flux. La logica su cui si basano è proprio l'analisi del traffico DNS per l'individuazione di quelle peculiarità intrinsecamente legate alla logica di funzionamento delle reti fast flux con il fine di discriminare domini legittimi da domini malevoli. Ovviamente queste non sono le uniche a disposizione; esistono svariate altre tecniche di analisi del traffico DNS che ad esempio mirano all'identificazione dei nodi di una botnet attraverso l'analisi delle query alle *blacklist* DNS.

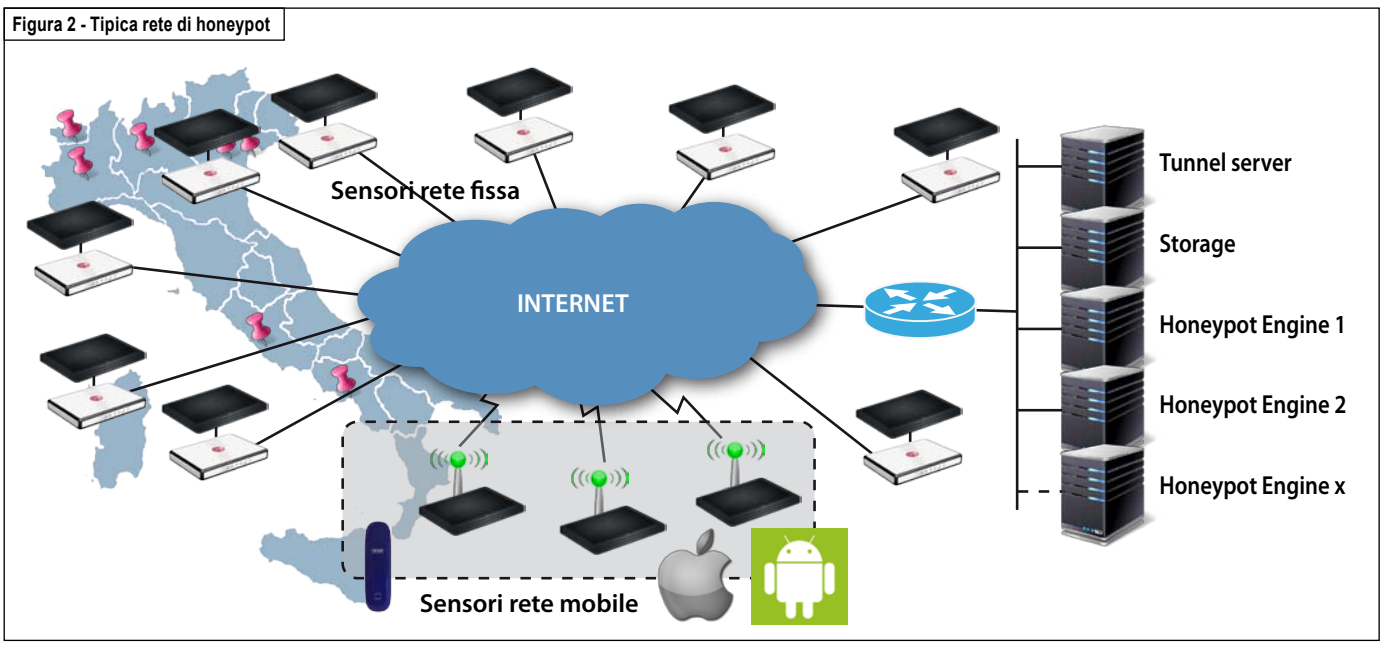
2.2 Il ruolo di un operatore

Sebbene le botnet affondino le proprie radici in minacce e tecniche in parte note, esse sono state recentemente oggetto di una profonda evoluzione, sia legata al raffinamento del modello di business criminale che le sfrutta sia soprattutto in termini tecnologici. Le proporzioni raggiunte da questo fenomeno e la facilità con la quale è oggi possibile divenirne vittime inconsapevoli, sono solo alcune delle ragioni che ci spingono a comprenderlo meglio, insieme alle sue reali potenzialità e ai rischi correlati.

Le botnet, per quanto tecnologicamente già molto avanzate, sono state recentemente ridisegnate e riprogettate proprio per allargare la base della loro potenziale "clientela". Oggi molte botnet sono alla portata anche di organizzazioni criminali povere dal punto di vista delle competenze tecniche. Grazie alla disponibilità di servizi di noleggio e di *kit* di sviluppo, è possibile creare e personalizzare botnet per ogni esigenza.

In tale contesto un ISP può svolgere un ruolo importante aiutando i propri Clienti ad identificare le compromissioni da bot e fornendo eventualmente informazioni e supporto per le operazioni di bonifica.
I benefici sono molteplici: da un lato la protezione della propria infrastruttura d'altro un maggior accreditamento verso i clienti, che attraverso operazione di bonifica dei propri PC, possono limitare l'esposizione al rischio di furto di dati riservati e di identità.
Occorre notare che già diversi ISP, a livello mondiale, si stanno attrezzando per fornire servizi simili ai propri clienti.
In quest'ottica anche Telecom Italia potrebbe offrire un servizio di notifica ai clienti che risultano coinvolti nella propagazione di *malware* per informarli che la loro macchina potrebbe essere infetta. La notifica potrebbe essere utilizzata per fornire indicazioni e linee guida su come evitare future infezioni.
L'implementazione di tali servizi richiede ovviamente l'uso di una componente di rilevamento, l'approccio che in molti casi si sta seguendo a livello internazionale, è basato sull'impiego di reti di *honeypot*, che per loro natura non richiedono di analizzare il traffico di rete ma solo quello terminato sull'*honeypot* stesso.
Un *honeypot* infatti è un sistema in grado di essere rilevato, attaccato e compromesso, simulando di essere un server parte della rete e contenente informazioni preziose. In realtà è isolato dalle altre macchine e non contiene nessun dato sensibile o critico. L'attaccante viene attratto a entrare in queste "trappole" perché l'*honeypot* mette a disposizione dei servizi aperti e visibili da Internet che risultano facilmente violabili. Il valore derivante dall'uso di un *honeypot* risiede principalmente nei dati che esso permette di raccogliere, oltre che nella semplicità con cui questi dati sono collezionabili. Trattandosi di sistemi destinati esclusivamente a essere attaccati, da una parte ogni connessione verso l'*honeypot* può rappresentare una scansione o un tentativo di attacco, dall'altra ogni connessione originata dall'*honeypot* può suggerire la compromissione del sistema. In altre parole, tutto il traffico, in ingresso o in uscita da una *honeypot*, deve essere considerato sospetto e meritevole di ulteriori approfondimenti. Concettualmente, non essendo basato su algoritmi di rilevamento o firme note, un *honeypot* è un sistema relativamente semplice da implementare e, soprattutto, da amministrare; inoltre, catturando solo traffico malevolo, non richiede tipicamente grandi risorse computazionali.
Nell'ottica di un servizio di notification, l'impiego di reti di *honeypot* consente di identificare gli host dai quali provengono le infezioni che verosimilmente risultano essere stati a loro volta compromessi. Per questa finalità è stato già predisposto presso il Security Lab, Figura 2, un primo sistema di monitoraggio attacchi su reti pubbliche basato proprio su una rete di honeypot. Per il rilevamento viene utilizzato un sistema open source e una molteplicità di *honeypot*.

Figura 2 - Tipica rete di honeypot



3 Le iniziative della comunità europea per la cybersecurity e la lotta alle botnet

Le tecnologie ICT e la cybersecurity rivestono un ruolo chiave per il successo economico e sociale della EU, e giustamente la Commissione Europea le ha inserite nel suo piano strategico per affrontare con successo le sfide di questo decennio (Europa 2020). Partendo da queste considerazioni, nel contesto del programma europeo del 2012 ICT Policy Support Programme (CIP-ICT PSP), a sua volta posto sotto l'ombrello del CIP, o Competitiveness and Innovation Framework Programme, la Comunità europea ha pubblicato un bando per la "cybersecurity/ fighting botnets objective". Lo strumento utilizzato per il finanziamento è definito come Pilot-B, cioè in grado di sostenere una robusta azione "pilota" per quasi 8 milioni di euro di contributo comunitario.
È importante sottolineare che con il Pilot la EU non intende supportare attività di ricerca, anche se può coprire, quando necessario, l'adeguamento tecnico e il necessario lavoro di integrazione al fine di raggiungere gli obiettivi prefissati. Lo scopo principale di questa iniziativa è quello di stabilire, a livello europeo, una piattaforma pilota per la rilevazione, la misurazione, l'analisi, la mitigazione ed eliminazione delle minacce informatiche, le botnet in particolare, ma possibilmente anche altre tipologie di malware, in modo da creare una serie di strumenti a livello europeo per la lotta contro le minacce informatiche emergenti, il tutto basandosi sulle attuali iniziative degli Stati membri o altri soggetti europei (es. Telco, LEA, ecc.). Le botnet sono quindi l'obiettivo primario di questa azione, riconoscendo a queste tipologie di malware una particolare dannosità e pericolosità per l'intero cyberspazio.
Il valore aggiunto di un approccio globale europeo è ampiamente riconosciuto per una riduzione efficace delle minacce informatiche e per aumentare il livello di sicurezza e di fiducia nel cyberspazio europeo. Le botnet, come abbiamo visto, sono infatti fenomeni globali e, quindi, un efficace meccanismo di difesa non può essere limitato ad un approccio nazionale o meno ancora a livello di una singola organizzazione, per quando multinazionale possa essere. L'enfasi viene quindi posta sull'integrazione di strumenti distribuiti in aree geografiche differenti, nonché lo sviluppo di buone pratiche per la fornitura di soluzioni innovative, efficaci e user-friendly.
Telecom Italia con il Security Lab, già membro dell'EP3R(*European Public Private Partership for Resilience*) ha aderito all'iniziativa del bando EU collaborando fin da subito alla costruzione del consorzio Advanced Cyber Defence Center che ha presentato la domanda poi risultata vincente.

4 Il progetto ACDC (*Advanced Cyber Defence Center*)

4.1 Il consorzio ACDC

Al consorzio ACDC, Figura 3, partecipano 28 partner provenienti da 14 paesi (Germania, Austria, Spagna, Bulgaria, Croazia, Romania, Repubblica Ceca, Francia, Regno Unito, Italia, Portogallo, Belgio, Olanda, Slovenia) con competenze diversificate in modo da coprire tutto il know-how necessario:

- Operatori di telecomunicazioni e ISP (tra cui TI, Telefonica ed ECO, l'associazione dei provider tedeschi, che opera da prime contractor del progetto).
- Associazioni industriali e di settore (tra cui Microsoft).
- Consulenza legale.
- Centri di ricerca.
- CERT.
- Le autorità pubbliche (LEA).

4.2 Il framework ACDC dalla rilevazione alla protezione

Partendo dall'analisi dei limiti delle attuali misure anti-botnet il progetto ACDC propone un approccio che mira ad integrare le attuali best-practice e tecnologie esistenti in un unico framework end to end (Figura 4) che incorpora il rilevamento degli abusi di rete, l'archiviazione, l'analisi dei dati, la distribuzione dei risultati di tali analisi e infine la fase di mitigazione dei malware con particolare attenzione ai dispositivi client infetti.

4.2.1 *Rilevamento (Detect Botnets)*

Come descritto nel paragrafo 2.1 "*Come rilevare una botnet?*" la lotta contro le botnet presuppone inevitabilmente di partire dall'individuazione degli abusi di rete, cioè dei comportamenti fondamentali delle botnet: il diffondersi o replicarsi e l'attaccare determinati obiettivi ad esempio con DDoS o campagne di SPAM massive. La diffusione è il processo attraverso il quale le botnet cercano di infettare altri computer. Il progetto ACDC mira ad identifi-

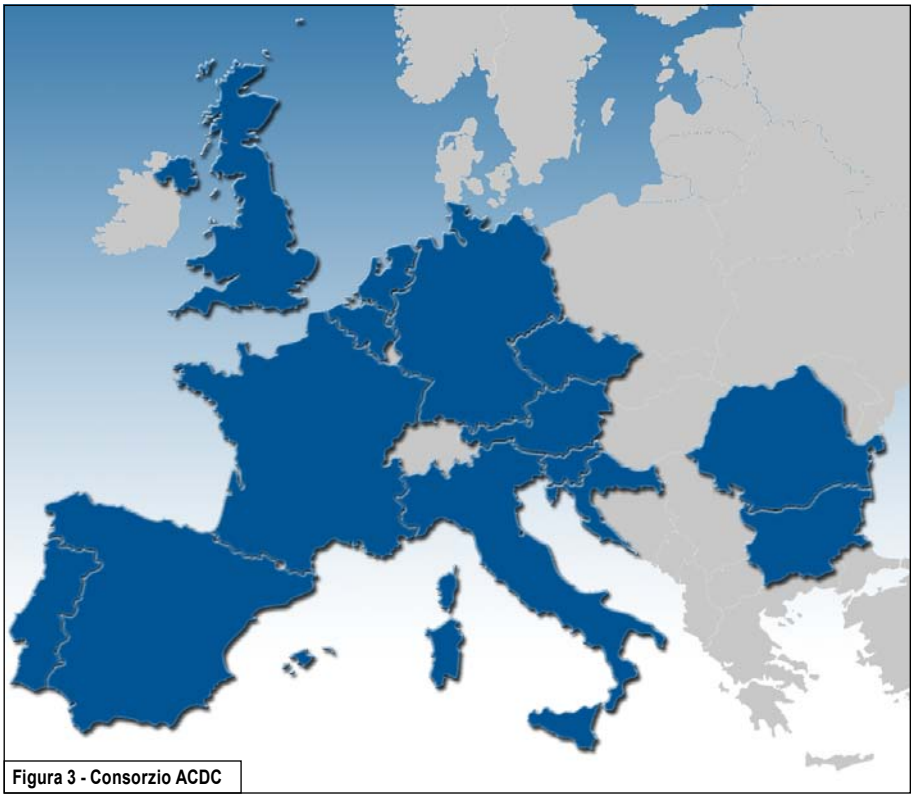


Figura 3 - Consorzio ACDC

care e rintracciare botnet mentre stanno cercando di espandersi, quindi prima che lancino attacchi su larga scala (prevention) attraverso:

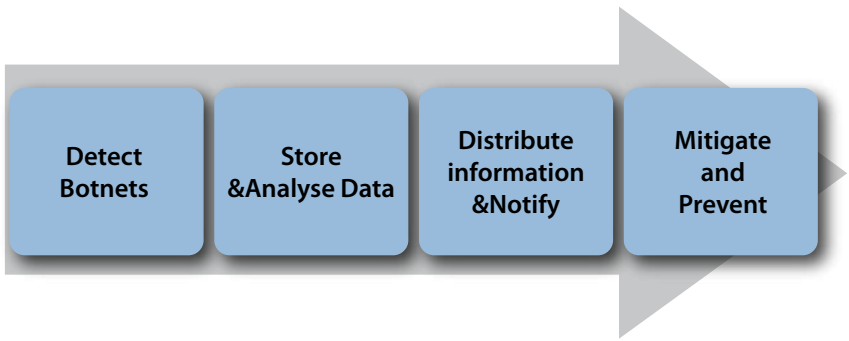
- L'installazione di plug-in su PC "amici" (come ad-on di antivirus, ad esempio).
- L'impiego di reti di sensori (es. honeynet).
- L'Analisi di siti Web infetti.
- L'Utilizzo di Droni, cioè sistemi che si fingono infetti che cercano di agganciarsi a botnet esistenti.

4.2.2 *Memorizzazione e analisi dei dati*

La sola raccolta dei dati non è sufficiente per capire cosa sta avvenendo realmente. Per dedurre esattamente quali fenomeni si stanno verificando e quali misure adottare per un efficace contrasto, i dati raccolti devono essere analizzati in modo opportuno. L'idea è di avere un unico centro sul quale far convergere tutte le informazioni necessarie: più dati sono disponibili, maggiore è la probabilità che le analisi e le contromisure individuate siano efficaci.
ACDC prevede di realizzare una "Clearing-House" centralizzata dei dati (ovviamente mantenuti ed elaborati secondo le norme di legge vigenti) finalizzata a fornire:

- Grandi quantità di informazioni anche per organizzazioni piccole o locali.
- Una gestione centralizzata delle informazioni secondo le norme di legge, sgravando tale incombenza alle singole organizzazioni che hanno interesse ad analizzarle.
- Funzioni di reporting omogenee e comparabili.
- Un Early Warning System per individuare tempestivamente trend di attacco da contrastare con misure di prevenzione.

Figura 4 - Framework ACDC



4.2.3 *Distribuzione delle informazioni*

I dati analizzati e le informazioni elaborate devono essere distribuite in modo efficace ai corretti destinatari in modo che possano prendere per tempo le contromisure necessarie.
La Clearing House centralizzata dei dati sarà basata su tecnologie esistenti e metodologie per lo scambio di dati utilizzati in progetti precedenti che abbiano dimostrato di essere efficaci per la condivisione delle informazioni sugli incidenti e le vulnerabilità,

sempre nel rispetto dell'anonimato e delle norme vigenti. Una comunicazione corretta e completa porterà ad una reazione più rapida ed efficace contro le minacce informatiche.

4.2.4 *Prevenzione e contenimento*

Mentre la maggior parte delle attuali iniziative anti-botnet hanno come obiettivo principale il solo server C&C trascurando il problema degli utenti dei PC infetti, l'approccio ACDC si concentra anche sugli utenti finali, come giustamente richiesto dal bando EU.
Con i principali ISP in qualità di partner del consorzio, ACDC è nella posizione di sviluppare azioni di mitigazione contro le botnet ben oltre il solo lato server. Grazie alle analisi della Clearing-House centralizzata è possibile individuare puntualmente i siti Internet e gli host infetti. L'ISP può essere messo in condizione di contattare il proprietario del PC infetto al fine di comunicargli lo stato di sicurezza del PC ed aiutarlo a risolvere il problema indirizzandolo verso siti nazionali dove può trovare un aiuto su misura per il suo caso personale. Questo è infatti l'approccio già seguito con successo in Germania dall'iniziativa Bot-Frei o in Giappone con l'iniziativa CCC (*Cyber-Clean-Center*). Infine, la soluzione ACDC sarà ovviamente messa alla prova con esperimenti che ne dimostrino l'efficacia. Gli esperimenti si concentreranno essenzialmente sugli aspetti più rilevanti delle botnet, quali ad esempi la capacità di condurre massive campagne di SPAM o di attacchi di tipo Denial of Service oppure quella di modificarsi e nascondersi agli strumenti di detection (es. tecniche fast-flux).
La Figura 5 illustra il ciclo di vita dell'insieme delle soluzioni proposte dal progetto.

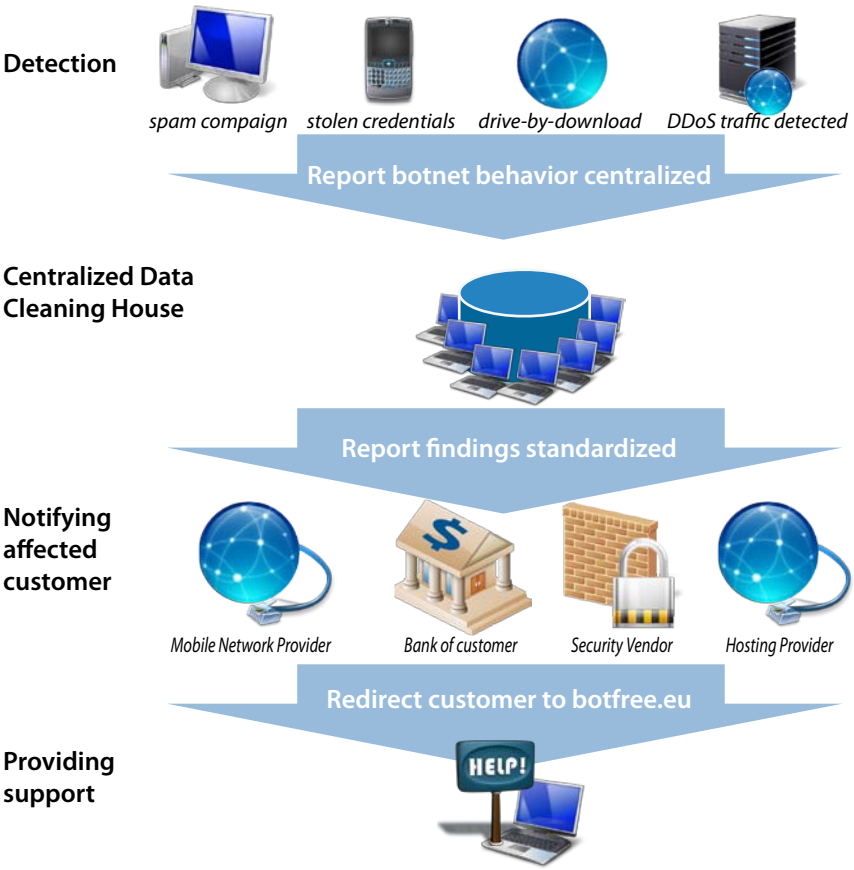


Figura 5 - Ciclo di vita delle soluzioni per ACDC

Conclusioni

Il contrasto della cyber criminalità non può prescindere come visto da una risposta coesa ed allargata con l'attivazione di una stretta collaborazione tra i diversi attori coinvolti a vario titolo, quali ISP, operatori di telecomunicazione, enti governativi e, ultimi ma non meno importanti, gli utenti.
Le attività che si stanno sviluppando hanno come fine di mantenere alta l'attenzione sul fenomeno delle botnet e del malware e rispondere in modo proattivo e preventivo, laddove possibile, alla diffusione delle infezioni sulle nostre reti e sui terminali dei nostri Clienti, o limitarne quantomeno gli effetti.
Questo è in corso di realizzazione non solo attraverso il dispiegamento di apposti sensori per il monitoraggio ma, come descritto, anche con la partecipazione attiva al consorzio internazionale ACDC ■

stefano.brusotti@it.telecomitalia.it
luciana.costa@it.telecomitalia.it
paolo.delutiis@it.telecomitalia.it

Stefano Brusotti
dottore in Scienze dell'Informazione con master COREP in Telecomunicazioni entra nel Gruppo Telecom Italia nel 1996 dove, nell'allora CSELT (Centro Studi E Laboratori di Telecomunicazioni), inizia ad occuparsi di moneta elettronica partecipando al progetto di sperimentazione del primo borsellino elettronico italiano e all'introduzione delle carte a chip in telefonia pubblica. Nel 2000 è nominato responsabile del Centro di Competenza e Servizio "Security" e si occupa dei primi progetti del Gruppo sulla sicurezza delle informazioni e dello sviluppo della prima offerta di servizi di sicurezza per il mercato. Dal 2001, in Telecom Italia Lab, è responsabile dell'Area di Ricerca "ICT Security" dove si occupa di nuove tecnologie per la sicurezza delle reti e dei servizi. Nel 2006 passa in Telecom Italia come responsabile Security Innovation. Attualmente in Information Technology è responsabile delle attività di cyber-security, prototipazione, scouting e testing guidando il Security Lab di Telecom Italia.

Luciana Costa
laureata presso il Politecnico di Torino in Ingegneria delle Telecomunicazioni. Lavora in Telecom Italia dal 2001 e si occupa di sicurezza informatica e di protezione dell'Informazione, nell'ambito della funzione Security Lab di Technical Security. Ha maturato esperienza sugli aspetti di sicurezza delle reti mobili, in particolare UMTS ed LTE, con attività di analisi delle vulnerabilità dell'infrastruttura di rete e di security assessment dei terminali mobili, contribuendo anche alla specifica dei requisiti di sicurezza, in ottica certificazione. Attualmente partecipa alla definizione di una possibile metodologia da applicare ai prodotti delle reti 3GPP per certificarne il loro livello di sicurezza e robustezza, attività del gruppo di sicurezza SA3 del 3GPP. Continua ad occuparsi dei temi legati all'evoluzione del malware, ed in particolare delle botnet, dell'analisi dei nuovi modelli di infezione e delle possibili tecniche di contrasto.
È coautrice del libro "Il fenomeno delle botnet" e di diversi articoli e domande di brevetto

Paolo De Lutiis
ha un solido background in informatica ed è specializzato in sicurezza informatica. Lavora in Telecom Italia dal 2000 ed è impegnato direttamente nel progetto finanziato ACDC.
Partecipa attivamente in diverse attività di normativa ed è stato chairman del gruppo ETSI TISPAN WG7 fino al 2012. Inoltre ha collaborato con vari Enti internazionali ed ha contribuito alla stesura delle specifiche ITU-T per la sicurezza delle reti di accesso G-PON e XG-PON. Si interessa di Governance, Risk Management e Compliance (GRC), e partecipa ai lavori del gruppo ETSI ISG "Indicatori della Sicurezza delle Informazioni" (ISI) in qualità di rapporteur. È autore di diversi articoli e domande di brevetto legati alla sicurezza delle TLC.

Usa il tuo smartphone per visualizzare approfondimenti multimediali

VERSO UNA NUOVA GOVERNANCE GLOBALE DI INTERNET

Lorenzo Maria Pupillo

Sin dalla sua nascita Internet è stata gestita attraverso un processo *bottom up* chiamato *multi stakeholder* e caratterizzato da un coinvolgimento paritario da parte dei governi, del settore privato e della società civile. Storicamente però la società civile e il settore privato hanno svolto i ruoli maggiori. Poiché Internet è diventata parte sempre più centrale dell'economia e della vita quotidiana dei cittadini, i governi di molti stati ritengono necessario riaffermare la loro giurisdizione diretta su Internet soprattutto sui temi della privacy, della sicurezza e della protezione dei diritti di proprietà.
Questo processo non è però senza contraddizioni perché sfida una cultura di Internet aperta e senza confini e pone con forza la necessità di nuove istituzioni globali per la *Governance* di Internet. Il punto di partenza deve essere un ICANN profondamente riformata, un processo multi stakeholder migliorato e che evolva nel tempo verso un processo multi istituzionale in cui ci sia un rapporto più stretto tra sfida da governare e istituzione più adatta al suo governo.

1 Introduzione

Dopo la Conferenza di Dubai che, per la prima volta nella storia dell'ITU, ha visto i paesi membri dividersi sulla firma di un trattato in aree geopolitiche diverse, evocando, secondo alcuni osservatori, l'inizio di una guerra fredda digitale[1], è quanto mai necessario aprire una riflessione sul futuro della *Governance* Globale di Internet.

Il trattato approvato a Dubai presenta miglioramenti rispetto al testo del 1988 e solo nelle risoluzioni, non vincolanti, sollecita un'attività specifica sui temi della *governance* di Internet. La reazione negativa da parte degli USA e di alcuni paesi occidentali rischia tuttavia di caratterizzare come una frattura geopolitica le divisioni sull'opportunità di un maggiore coinvolgimento dell'ITU, polarizzando politicamente le divisioni sulle idee di governance globale di Internet[2]. Perché la governance di Internet oggi appare più importante che nel passato? Internet è sempre più presente nella vita quotidiana e sarà sempre più pervasiva, perché più accessibile in ogni momento e in ogni luogo, attraverso l'internet mobile, il cloud computing e l'ubiquitous computing: *we will live in the Internet, rather than go on the Internet*!

Internet è, infatti, sempre più considerata una risorsa essenziale per lo sviluppo dell'attività economica e sociale della nostra società, ma è soprattutto la sua dimensione globale che la rende ormai un fenomeno sempre più centrale, per lo sviluppo economico e sociale di ogni paese. Da questo punto di vista, per esempio, quello che è successo in Egitto, durante la Primavera Araba, è particolarmente significativo. L'Egitto è uno stato che sta puntando molto alla diffusione dell'ICT per promuovere il suo sviluppo economico. Durante le rivolte di piazza del Febbraio del 2011, il governo egiziano ha deciso di interrompere per cinque giorni le comunicazioni internet e quelle dei telefoni cellulari con il resto del mondo. Secondo l'OECD[3], quest'operazione ha comportato un danno diretto di circa 90 milioni di USD, circa 18 milioni di dollari il giorno, quindi su base annua qualcosa come 3-4% di Prodotto Interno Lordo. Questo testimonia come Internet sia diventata parte sempre più centrale dell'economia e come le implicazioni legate alle interruzioni delle connessioni Internet abbiano conseguenza rilevante non

1 *A digital cold war ? The Economist*, 14 Dicembre 2012

2 Secondo l'Economist, la posizione degli USA è dettata anche dalla difesa dei propri interessi: "*... no other country benefits as much from the status quo in the online world. Since much of the internet infrastructure is based in America and most of its traffic zips through it, America is in a unique position to eavesdrop, should it be so inclined. America's internet firms also capture most of the profit pool of the online industry". Id.*

3 Vedi OECD (2011) : http://www.oecd.org/document/19/0,3746,en_2649_201185_47056659_1_1_1_1,00.html

WCIT 2012:la Conferenza di Dubai

Il 14 Dicembre scorso si è conclusa a Dubai la *World Conference on International Telecommunications* che, dopo due settimane d'intenso dibattito tra circa 1600 delegati presenti alla Conferenza, ha approvato le nuove ITRs (*International Telecommunications Regulations*), che entreranno in vigore nel 2015. I paesi presenti alla Conferenza si sono divisi tra quanti hanno accettato di firmare il trattato e quanti invece non l'hanno fatto. 89 paesi su 144 presenti alla Conferenza hanno firmato mentre i restanti 55 non l'hanno fatto o si sono riservati di decidere in un secondo momento. La conferenza di Dubai si è chiusa con un risultato clamoroso per la storia dell'ITU, cioè una divisione, geo-politicamente netta, nell'adesione al trattato tra gli Stati Uniti, il Regno Unito, il Canada, l'Australia da una parte e il blocco dei paesi Africani, Arabi e la Russia e Cina dall'altra.

1 I contenuti del nuovo trattato

È opportuno distinguere l'analisi degli articoli del trattato da quella delle risoluzioni che lo accompagnano. Infatti, mentre i primi, per loro stessa natura, sono vincolanti per gli Stati che accettano di firmare il trattato, le risoluzioni allegate al trattato non hanno invece natura vincolante ed esprimono indicazioni ed esigenze espresse nel dibattito durante la conferenza o molto spesso svolgono un ruolo di mediazione per raggiungere un consenso più ampio o garantire equilibri più avanzati tra gli stati membri.

2.1 Gli Articoli

Le novità rispetto alle ITRs del 1988, ovvero gli elementi completamente nuovi di cui cioè non esisteva nessuna traccia nella versione precedente del trattato, sono:

Nel preambolo:

- L'impegno a implementare le ITRs in modo da **rispettare e migliorare i diritti umani**.
- Il **diritto all'accesso** degli stati membri ai servizi internazionali di telecomunicazione.

Negli articoli:

- **Roaming Internazionale** (Art. 4.4 - 4.7 e 5.4) In *materia di trasparenza*, l'Art. 4.4 del trattato prevede che gli Stati Membri promuovano misure per assicurare informazioni accurate, gratuite e trasparenti. Non è previsto però, nessun obbligo in materia ma solo un invito agli Stati Membri a operare in tal senso.
- **Security** (Art. 5A) L'articolo 5A - "*Security and robustness of the network*" - chiama gli Stati Membri a impegnarsi per assicurare la sicurezza e robustezza delle reti internazionali per garantirne l'uso effettivo ed evitare danni tecnici alle reti.
- **Spam** (Art. 5B) La nuova formulazione degli ITRs prevede un nuovo articolo in materia di spam (art. 5B: "*Unsolicited bulk electronic communications*") il quale, **escludendo ogni possibile obbligo**, afferma che gli Stati Membri devono impegnarsi - anche attraverso forme di cooperazione internazionale - a prevenire la diffusione dello spam minimizzandone l'impatto sui servizi internazionali di telecomunicazione.
- **Energy efficiency/*e-waste*** (Art. 8A). Quest'articolo incoraggia gli Stati Membri ad adottare le best practices sull'efficienza energetica e sull'*e-waste*, facendo riferimento alle Raccomandazioni ad hoc dell'ITU-T.
- **Accessibility** (Art. 8B). L'art 8B invita gli Stati Membri a promuovere l'accesso ai servizi di telecomunicazioni internazionali per le persone con disabilità, in accordo con le raccomandazioni ITU-T.
- **Risorse di numerazione internazionale** (Art 3.5). Si richiede agli Stati Membri di assicurare che le risorse di numerazione siano utilizzate solo dai soggetti cui sono assegnate e per lo scopo previsto.
- **Calling Line Identification** (CLI) (Art 3.6): Si richiede che gli Stati Membri offrano il CLI seguendo le raccomandazioni previste dall'ITU-T.
- **Regional Telecommunication Traffic Exchange Points** (Art. 3.7) Si raccomanda che gli Stati Membri creino l'ambiente migliore dal punto di vista delle regole, per lo sviluppo dei punti di scambio regionale del traffico, per migliorare la qualità e l'affidabilità della connessione tra le reti di telecomunicazioni, sostenendo la concorrenza e riducendo il costo delle interconnessioni internazionali.

I cambiamenti che fanno riferimento invece agli articoli esistenti hanno portato a emendare alcune parti del testo esistente relativo ai seguenti temi:

- **Obiettivo degli ITRs**: (Art.1) il testo del trattato non contiene modifiche alla definizione di telecomunicazioni e non riconosce il valore vincolante delle raccomandazioni ITU-T. Invece, si specifica che il testo del trattato non fa riferimento ai *content related aspects of telecommunications*.
  Per quanto riguarda l'entità cui va applicato il trattato, il testo nell'art. 1.1 abis) parla di "***authorized operating agencies***" come quelle "*operating agencies, authorized or recognized by a Member State"*. In altre parole si lascia agli stati membri la facoltà di definire a quali società si applica il trattato.
- **Charging and Accounting**: le modifiche all'art. 6, riconoscono, in linea generale, l'obiettivo di sostenere gli

accordi commerciali e il principio di valorizzazione del traffico (pricing) da parte degli operatori per il traffico trasportato sulle reti.

- **Tassazione**: Gli atti finali degli ITRs introducono un nuovo articolo (art. 6.3: "Taxation") che non prevede alcun espresso divieto di doppia imposizione.
- **Routing**: Gli atti finali degli ITRs non prevedono alcuna nuova disposizione in materia di routing né alcun obbligo in capo agli operatori di fornire informazioni in materia di direttrici internazionali di traffico.
- **Network management**: La nuova versione degli ITRs pur non prevedendo nulla in merito a compensazione per il traffico IP ovvero in merito a differenti livelli di qualità del servizio, prevede un aggiornamento dell'art. 3.1 finalizzato ad evidenziare come gli Stati Membri debbano adoperarsi per cooperare al fine di garantire un "soddisfacente" livello di qualità del servizio. Cosa si intenda per "soddisfacente" non è stato chiarito in dettaglio.

Questo esame dell'aggiornamento degli articoli del trattato, cioè della parte vincolante del trattato stesso, evidenzia come nel trattato siano adesso presenti significative e importanti novità sul tema del roaming, dell'estensione dell'accesso ai servizi di telecomunicazione ai disabili, del riferimento all'efficienza energetica e all'e-waste nonché miglioramenti del testo preesistente.
L'elemento che appare più importante è tuttavia che il tema di Internet non sia presente esplicitamente all'interno del trattato.

2.2 Le risoluzioni

La parte che invece ha destato più polemiche sia nel metodo in cui è stata gestita (l'uso del voto invece che del consenso) che nel merito dei contenuti è quella che fa riferimento ad alcune risoluzioni allegate al trattato che però, come abbiamo evidenziato in precedenza, non rappresentano nessun obbligo per i paesi firmatari del trattato stesso.
Due sembrano essere quelle più rilevanti per capire la natura della dialettica sviluppatasi a Dubai: le risoluzioni numero 3 e la numero 5. La numero 3 ha il titolo "*To foster an enabling environment for the greater growth of the Internet*" e nel complesso invita gli Stati Membri a svolgere un ruolo attivo nel dibattito sull'Internet Governance utilizzando prioritariamente l'ITU.
La risoluzione 5 "*International telecommunication service traffic termination and exchange*", invita gli Stati Membri a collaborare affinchè "*their regulatory frameworks promote the establishment of commercial agreements between authorized operating agencies and the providers of international services in alignment with principles of fair competition and innovation*". Sotto il profilo operativo, la Risoluzione 5 delega lo Study Group 3 dell'ITU-T a predisporre una specifica raccomandazione, se appropriata, e comunque delle apposite guidelines. Nel complesso la Risoluzione 5 deve essere considerata come un risultato significativo nella direzione di approcci regolamentari che promuovano (e dunque almeno sicuramente non ostacolino), lo sviluppo degli accordi commerciali tra Telco e OTT, come con forza richiesto dall'ETNO.

3 Valutazioni e commenti

La posizione oltranzista degli USA ha giocato un ruolo fondamentale nel determinare il risultato finale della conferenza. Quest'atteggiamento unilaterale è stato però rimarcato da autorevoli quotidiani e osservatori americani ed anche dall'Economist. Il New York Times, per esempio, a fine conferenza, ha riconosciuto che "*At the global treaty conference on telecommunications [in Dubai], the United States got most of what it wanted…*"[4]. e che quindi, non firmando il trattato, il messaggio che è lanciato dagli USA al mondo da questa conferenza è chiaramente confuso (murky!). Il quotidiano di New York, infatti, fa notare che, leggendo gli articoli del trattato si vede che la parola Internet non è mai presente, che l'art 1.1. chiaramente evidenzia che il trattato non fa riferimento ai *content related aspects of telecommunications*. Inoltre il preambolo fa un esplicito richiamo a un uso delle regulations "*in a manner that respects and upholds their human rights obligations*", rendendo chiaramente più difficile la giustificazione da parte di paesi come la Cina e l'Iran delle loro pratiche censorie su Internet. Inoltre, varie proposte contrarie ai voleri degli USA sono state rimosse. Quella per esempio concernente il controllo del sistema d'indirizzamento degli indirizzi Internet o la proposta presentata da vari stati di far pagare a società come Google e Facebook la connessione alle reti degli operatori telcos sulla base del traffico spedito ai clienti delle telcos.
Secondo il NYT, la posizione assunta dagli Stati Uniti non avrà ripercussioni sul modo in cui Internet opererà nei prossimi anni, ma certamente evidenzia il completo rifiuto da parte degli USA a riconoscere anche una simbolica *global oversight* della rete. Pur avendo ottenuto molto nel trattato, la presenza nella risoluzione 3 di temi legati a Internet è stata considerata inaccettabile ed ha portato alla non sottoscrizione del trat-

4 "Message, if Murky, from U.S. to the World", by Eric Pfanner, The New York Times, 14 Dicembre 2012

tato e al boicottaggio della cerimonia finale.
Ma il risultato della Conferenza di Dubai ha evidenziato anche la sostanziale assenza di una strategia e di una vera posizione autonoma da parte dell'Europa. La Commissione Europea e molti stati Europei si sono puramente allineati alle posizioni USA, rinunciando a svolgere un ruolo autonomo e potenzialmente foriero di equilibri più avanzati sul terreno della geopolitica di Internet, come invece in passato (per esempio WSIS 2005) l'Europa aveva tentato di svolgere. Va inoltre evidenziato che la Commissione Europea, non ha supportato in nessun modo l'industria europea, diversamente da quanto invece ha fatto l'amministrazione USA rispetto all'industria americana.

4 Implicazioni dei risultati della Conferenza di Dubai

Va innanzitutto ricordato che il trattato entrerà in vigore nel 2015 e che, come spesso accade in queste circostanze, molti stati hanno chiesto di consultare i propri governi nei paesi di provenienza prima di aderire. Per i paesi che hanno deciso di non aderire al nuovo trattato varranno le regole del 1988. Inoltre, le relazioni tra due paesi di cui uno ha accettato il nuovo trattato e l'altro no, saranno anch'esse regolate dal trattato del 1988.[5]
Per quanto riguarda le implicazioni di policy, una lettura attenta dei risultati della Conferenza di Dubai suggerisce due elementi di riflessione.

a) Il lavoro svolto per l'aggiornamento del trattato contiene delle novità importanti e complessivamente il nuovo testo è da considerarsi come il compromesso più avanzato oggi raggiungibile.
b) L'assenza di unanimità tra i pasi membri dell'ITU rivela una contrapposizione ideologica molto forte più che sui contenuti del trattato stesso su come la *governance* di Internet vada affrontata.

L'iniziativa da condurre nei prossimi mesi, deve tendere perciò da un lato a chiarire quanto il trattato e le connesse risoluzioni effettivamente contemplano e dall'altro a evidenziare che le visioni differenti sul tema della *governance* internazionale di Internet che la Conferenza di Dubai ha evidenziato, richiedono nuovi approcci e modelli di riferimento che, partendo dalle esperienze migliori oggi esistenti, pongano le basi per una ridefinizione dei meccanismi e delle regole della governance mondiale di Internet ■

solo dal punto di vista economico, ma anche da quello geopolitico. Per questa ragione, alcuni stati ritengono necessario riaffermare la loro giurisdizione diretta su Internet soprattutto sui temi della privacy, della sicurezza e della protezione dei diritti di proprietà. Come si chiarirà di seguito, questo processo da parte degli Stati, non è però senza contraddizioni perché sfida una cultura di Internet aperta e senza confini. Ma fino ad oggi, Internet come è stata governata e perché l'attuale modello di governo di Internet appare insufficiente?

2 Oggi, chi governa Internet?

L'apertura, la connettività globale, la natura decentralizzata che caratterizzano Internet, la rendono quanto mai resistente alle forme tradizionali di governo centrale. Internet appare, infatti, come una rete molto distribuita e apparentemente senza un controllo centrale. I pacchetti d'informazioni, basati sull'IP (*Internet Protocol*) sono in grado di trovare da soli la propria strada dalla partenza all'arrivo. Internet si caratterizza per essere una rete di reti, a loro volta possedute e gestite da entità private, come gli operatori di telecomunicazioni, gli Internet Service Providers e altre società. La natura distribuita di Internet quindi, potrebbe generare l'impressione che nessuno ne sia proprietario e che nessuno la controlli. Molto spesso, parlando di Internet si richiama anche l'analogia con i *Commons*, tradizionalmente definiti come risorse naturali come le foreste, l'atmosfera, i fiumi o i pascoli, condivise e utilizzate da tutti. Internet cioè è considerata come un bene pubblico. È importante in questo contesto fare due precisazioni:

1) Per gli economisti il bene pubblico ha delle caratteristiche ben precise. Infatti, non deve essere possibile limitarne l'accesso e il consumo di questo bene da parte di un individuo non deve limitarne quello di un altro. È chiaro che questo non è il caso di Internet perché è possibile limitarne l'accesso e l'uso della rete può generare fenomeni di congestione. Inoltre, l'offerta del servizio ha un costo di realizzazione e di gestione che dovrà sempre essere sostenuto o dai privati o dalla collettività.
2) Ci si dimentica di evidenziare che, come sostenuto dal demografo Garret Hardin, il primo a parlare nel 1968 di tragedia dei *Commons*, come distruzione delle risorse comuni e pubbliche, l'unico modo per scongiurare la fine dei com-

5 ITU (2012), "The treaty signing process explained" , ITU Web site

mons è quello di "*manage the commons*" cioè di creare regole che permettano di gestire le risorse comuni (Hardin 1998).

Quindi, se è vero che Internet è una grande risorsa a disposizione di tutti, anche Internet ha bisogno di un coordinamento tecnico centrale, per permetterne il suo funzionamento operativo.

Tre sono le funzioni fondamentali che regolano il funzionamento di Internet: a) l'assegnazione dei blocchi d'indirizzi IP (*Internet Protocol Addresses*); b) il funzionamento dei *root name servers*; c) la definizione e l'attuazione delle politiche per la definizione dei domini di primo livello (*Top Level Domains*) come .com, .org, ecc.[6]

Gli indirizzi IP sono senz'altro la risorsa più importante per garantire la gestione dei pacchetti d'informazioni sulla rete Internet. L'ICANN (*Internet Corporation for Assigned Names and Numbers*) si occupa di suddividere Internet in spazi d'indirizzamento da assegnare ad autorità locali (RIPE per l'Italia) che si occupano di assegnare ulteriormente blocchi d'indirizzi IP agli *Internet Service Provider*. La parte più critica della gestione degli indirizzi è la loro definizione e assegnazione. Gli indirizzi IP devono necessariamente essere unici per permettere l'identificazione univoca delle varie parti della rete. Questo processo perciò, richiede forme di coordinamento per concordare come gli indirizzi IP devono essere fatti, cioè standardizzati, e per poi assegnarli a ciascun terminale o cliente in maniera univoca (il processo di assegnazione è svolto dai Regional Internet Registries). Esistono poi problemi di gestione economica degli indirizzi perché essi non sono infiniti e quindi gli spazi vanno gestiti in modo efficiente, garantendo che ci sia equilibrio tra domanda e offerta d'indirizzi. In realtà, ICANN non si occupa solo di assegnare gli indirizzi, ma associa anche gli indirizzo IP ai nomi dei siti web che usualmente digitiamo nel nostro Internet browser. La traduzione del nome logico del sito web in indirizzo (IP) è svolto da Internet che gestisce questi aspetti attraverso il secondo elemento fondamentale della sua architettura: i protocolli di IP routing e il DNS (*Domain Name Server*). Infine ICANN gestisce le politiche per la definizione dei domini di primo livello come .com e, dopo una fase di scarsità artificiale, con la decisione del Giugno 2011 di aumentarne significativamente il numero, ha aperto nuove possibilità di sviluppo di questo mercato. Complessivamente, la gestione di queste funzioni, formalmente tecniche e che in teoria, in alcuni casi, potrebbero essere addirittura svolte da macchine (come avviene per la gestione dei nomi a dominio di secondo livello), ha invece assunto nell'ultimo decennio, una forte valenza economica e politica ed ha portato allo sviluppo di una grande dibattitto sulla governance di Internet.

3 Le organizzazioni per la governance di Internet

Sin dalla sua nascita Internet è stata gestita attraverso un processo *bottom up* chiamato, *multistakeholder* e caratterizzato, in teoria, da un coinvolgimento paritario da parte dei governi, del settore privato e della società civile. Storicamente però la società civile e il settore privato, hanno svolto i ruoli maggiori: la prima ha contribuito soprattutto con lo sviluppo del software e dei protocolli che costituiscono il sistema nervoso di Internet e il secondo ha offerto i *backbones*. I governi hanno senza dubbio svolto un ruolo più limitato. Molte delle entità che hanno contribuito a definire Internet fin dalla nascita, continuano oggi a caratterizzarne l'attività. Quella che oggi è una struttura di entità indipendenti, nacque come un insieme di piccoli comitati e advisory panel creati dal governo degli Stati Uniti per guidare la gestione di Internet.

Nel 1992, i membri di questi gruppi decisero di fondare ISOC (*Internet Society*) come organizzazione non–profit, con l'obiettivo di garantire una discussione permanente sulle implicazioni legali, politiche, economiche e sociali dello sviluppo di Internet. All'interno di ISOC, l' IAB (*Internet Architecture Board*) garantisce lo sviluppo tecnico e ingegneristico di Internet, guidando il lavoro dell'*Internet Engineering Task Force* e di altri gruppi di lavoro. Le varie entità che fanno capo a ISOC contribuiscono a gestire il funzionamento quotidiano di Internet.

Nel 1994, Tim Berners-Lee, l'inventore del *World Wide Web*, ha creato il World Wide Web Consortium (W3C), con il compito di definire gli standard per il web.

Nel 1998, per gestire le funzioni centrali di governance di Internet, la gestione degli Indirizzi IP e i nomi a dominio, fu creata l' ICANN (*Internet Corporation for Assigned Names and Numbers*). L'ICANN è stata registrata in California come una società non-profit e opera in conformità a un *Memorandum of Understanding* con il Dipartimento del Commercio degli USA . La figura, presenta la classica icona del processo di Internet Governance.

6 Vedi Viktor Mayer Schoenberger e Malte Ziewitz (2005)

WHO RUNS THE INTERNET?

NO ONE PERSON, COMPANY, ORGA

The Internet itself is a globally distributed computer ne
Similarly, its governance is conducted by a decentraliz
from civil society, the private sector, governments, the
cooperatively from their respective roles to create shar

WHO IS INVOLVED:

IAB A C P S R
INTERNET ARCHITECTURE BOARD
Oversees the technical and engineering development of the IEFT and IRTF.
www.iab.org

ICANN C O P V
INTERNET CORPORATION FOR ASSIGNED NAMES AND NUMBERS
Coordinates the Internet's systems of unique identifiers: IP addresses, Protocol-Parameter registries, top-level domain space (DNS root zone).
www.icann.org

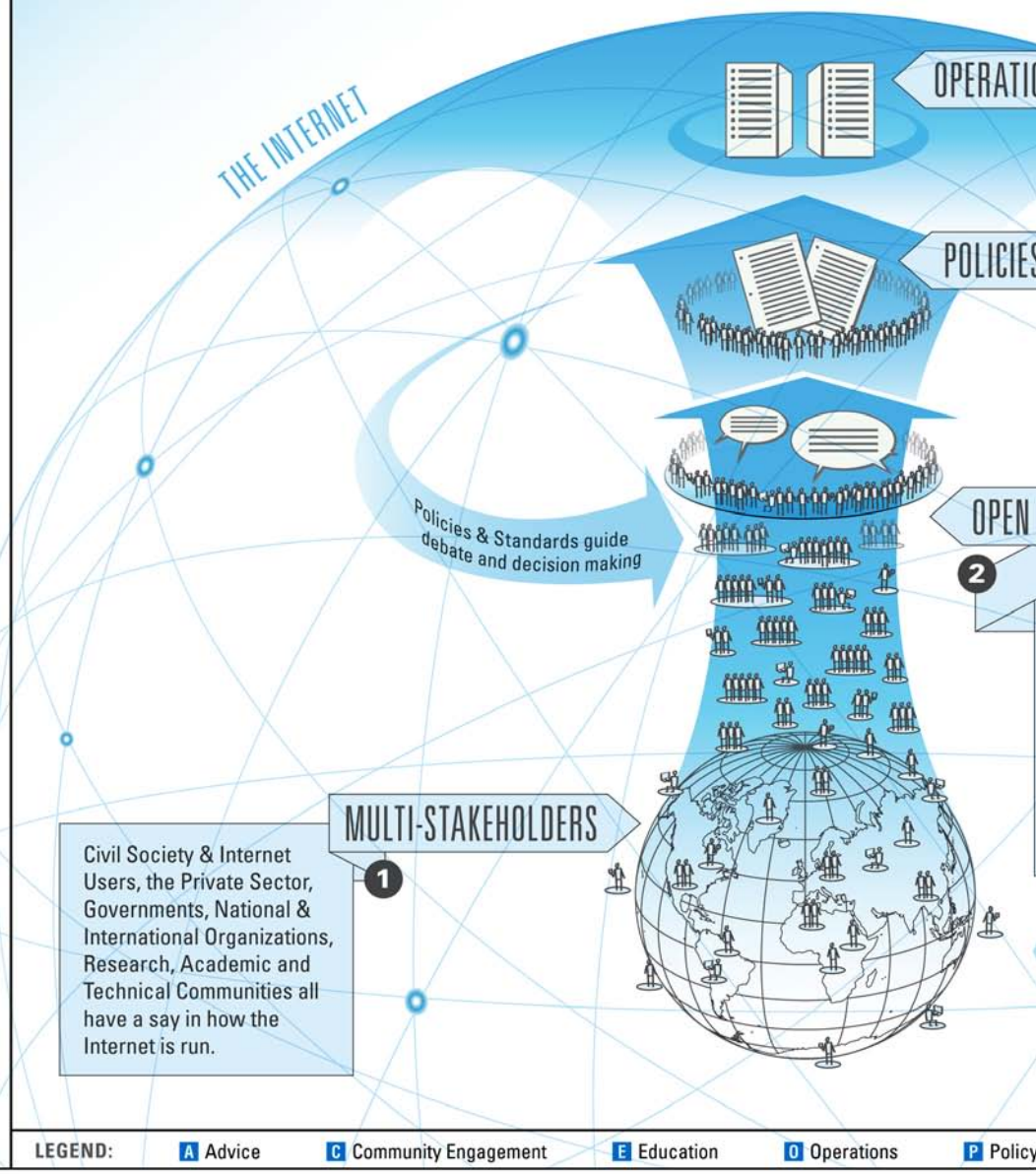
IETF C P S
INTERNET ENGINEERING TASK FORCE
Develops and promotes a wide range of Internet standards dealing in particular with standards of the Internet protocol suite. Their technical documents influence the way people design, use, and manage the Internet.
www.ietf.org

IGF A C P
INTERNET GOVERNANCE FORUM
A multi-stakeholder open forum for debate on issues related to internet governance.
www.intgovforum.org

IRTF R
INTERNET RESEARCH TASK FORCE
Promotes research of the evolution of the Internet by creating focused, long-term research groups working on topics related to Internet protocols, applications, architecture and technology.
www.irtf.org

GOVERNMENTS AND INTER-GOVERNMENTAL ORGANIZATIONS C P
Develop laws, regulations and policies applicable to the Internet within their jurisdictions; participants in multilateral and multi-stakeholder regional and international fora on Internet Governance.

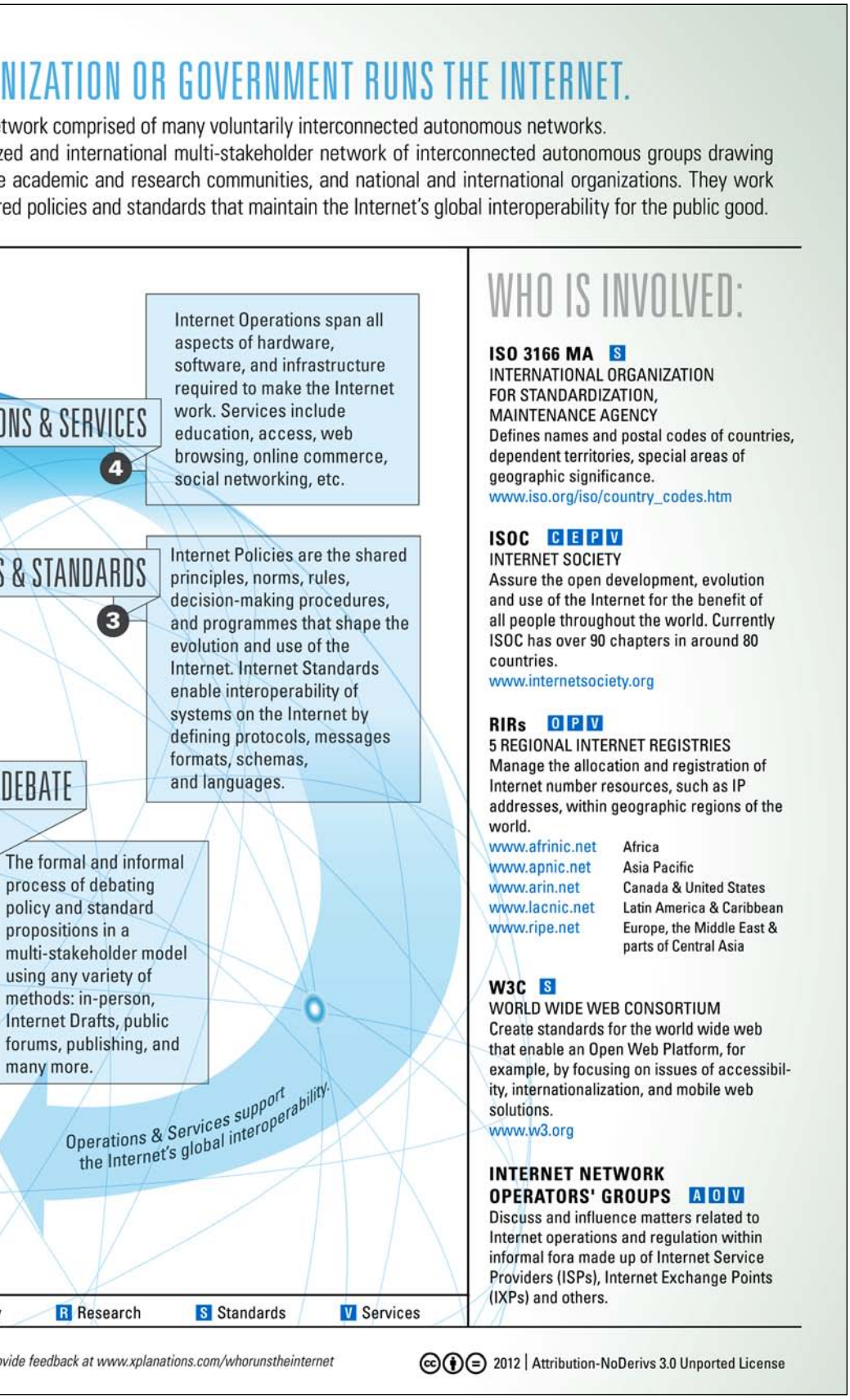
HERE IS HOW IT WORKS:



LEGEND: A Advice C Community Engagement E Education O Operations P Policy

XPLANATIONS™ by XPLANE.com

This graphic is a living document, designed to provide a high level view of how the internet is run. It is not intended to be a definitive guide. Please pro



3.1 La dinamica Stati - Rete

Lo sviluppo di Internet ha nei fatti messo in discussione il modo in cui si sono articolate le relazioni tra stati negli ultimi secoli.
La sfida ha riguardato la definizione stessa di Stato Nazione, nata dal Trattato di Westphalia nel 1648 e considerato dagli storici alla base delle sovranità nazionali degli stati moderni. L'architettura istituzionale definita da questo trattato prevedeva una società di stati nazione indipendenti e sovrani e una rete di organizzazioni intergovernative come la famiglia delle Nazioni Unite, la Banca Mondiale e il Fondo Monetario e varie organizzazioni regionali. Questo modello era basato sulla distinzione fondamentale tra le attività regolate dallo stato all'interno dei propri confini nazionali e dall'altro le interazioni transnazionali governate da accordi internazionali negoziati solo tra i governi[7].

È evidente che, la natura decentralizzata e transazionale della rete, combinata con la liberalizzazione del settore delle telecomunicazioni ha portato a una redistribuzione dell'autorità e del controllo e a nuove forme di partecipazione. Questo ha generato la nascita di nuove istituzioni legate alla comunità tecnica che definisce gli *standard* (come lo IETF) o gestisce gli indirizzi e i nomi a dominio (come l'ICANN), attraverso reti transazionali nate al di fuori degli stati nazionali e che si caratterizzano come veri e propri nuovi luoghi decisionali e che stanno portando alla creazione e allo sviluppo di nuove forme di partecipazione e collaborazione, e di nuove forme di governance della rete stessa.

7 Vedi Bertrand de La Chapelle (2011)

4 I cambiamenti di Internet e la tendenza verso una governance meno informale

Nella discussione sulla governance di Internet è anche necessario considerare accanto alla dinamica tra stati e rete, i profondi cambiamenti che hanno caratterizzando Internet rispetto a quando è nata, agli inizi degli anni '90. Si è tardato molto a riconoscere che l'ambiente tecnologico ed economico dell'Internet di oggi è cambiato profondamente da quello dell'Internet delle origini. Secondo la letteratura più recente[8] quattro fenomeni hanno contribuito a questo cambiamento:

a) l'aumento del numero e della diversità degli utenti finali: da un gruppo ristretto di accademici a una base di utilizzatori molto più ampia e molto meno sofisticata;
b) l'aumento nella diversità e complessità delle applicazioni: si è passati dall'uso prevalente delle applicazioni a bassa intensità di banda come posta elettronica e web browsing alla video conferenza, ai giochi on line che richiedono molta più banda e al P2P e al cloud computing, che generano pattern di traffico molto più sfidanti per le reti rispetto a quelli precedenti;
c) l'aumento delle tecnologie di accesso a internet (ADSL, fibra, cavo, soluzioni wireless) e del numero e dei tipi di terminali per connettersi a Internet (pc, tablet, smartphone, RFID tags, etc.) hanno generato una nuova complessità nella gestione della rete stessa;
d) La definizione di relazioni commerciali molte più complesse: la natura di rete di reti di Internet ha comportato la nascita di relazioni commerciali come il private peering o le Content Delivery Networks molto diverse da quelle degli anni precedenti.

Questi cambiamenti tecnologici ed economici degli ultimi anni stanno caratterizzando Internet come una realtà molto più eterogenea e dinamica rispetto al passato, producendo soprattutto un profondo mutamento nei pattern di uso di Internet che richiederà significativi cambiamenti negli schemi architetturali e nella sua gestione. Un'area che sta già risentendo di questi cambiamenti è proprio quella della *governance*, in cui si assiste a un inevitabile declino di modelli di *governance* informali. L'eterogeneità e il numero di utenti che oggi caratterizza Internet spingono, infatti, sempre di più verso una *governance* più formale della rete rispetto ai modelli cooperativi e alle sanzioni informali usate nel passato. La letteratura sulle norme sociali, che ha i suoi punti di riferimento nei lavori di Robert Ellickson (1991) e del premio nobel Elinor Strom (1990), chiarisce che i metodi informali di *governance* funzionano solo in comunità piccole e chiuse, con interessi omogenei, caratteristiche queste oggi non più riscontrabili nel mondo internet che invece si caratterizza sempre di più per collegare miliardi di persone con una grande varietà di esigenze. La necessità di una *governance* più formale sta già producendo la definizione di regole più precise per quanto riguarda per esempio, la lotta allo spam, la gestione del *Domain Name System* e quella delle reti.

5 Criticità dell'attuale modello di governance di Internet

Anche se l'idea originaria dei creatori di ICANN al Dipartimento del Commercio americano era quella di un ruolo puramente tecnico nella gestione del sistema dei nomi a dominio, in pratica, ICANN fu creata per risolvere i conflitti e le controversie legate ai nomi a dominio, soprattutto con riferimento alla creazione di nuovi nomi a dominio di primo livello (TLD). Proprio per questo, Secondo alcuni osservatori, il governo USA ha nei fatti utilizzato ICANN per "esternalizzare" la funzione di "*policy making*", verso un *industry self regulatory body*[9].

L'essere diventata nei fatti, un *global policy maker*, ha comportato anche la necessità di creare in ICANN una struttura rappresentativa dei vari *stakeholders* di questo processo, coinvolgendo, però senza diritto di voto, nel GAC (*Governmental Advisory Committee*) l' ITU (*International Telecommunication Union*), il WIPO, La Commissione Europea, l' OECD (*Organization for Economic Cooperation and Development*) e i Governi nazionali. In altri gruppi e committee, la società civile, la comunità tecnica come l'*Internet Engineering Task Force* e il *World Wide Web Consortium*. È evidente però, come nella crescente dinamica tra Stati Nazione e il protagonismo della comunità globale di Internet, l'aver affidato da parte dell'amministrazione americana funzioni vitali della Governance di Internet non a un trattato internazionale o a un'organizzazione intergovernativa, ma a un organismo non espressione diretta degli stati, fu interpretato come un atto molto unilaterale ed ha portato ad alimentare nel tempo una certa insofferenza per un'Internet troppo US Centric. Le preoccupazioni per un'Internet "troppo americana" e per il ruolo non solo tecnico, ma sempre più politico che ICANN svolgeva, hanno destato

8 Vedi Yoo(2012)
9 Vedi Mueller (2002)

nel tempo maggiori perplessità ed ha portato le altre aree geografiche del mondo a richiedere un peso maggiore nell'ICANN, puntando sul carattere globale di Internet. A questa insofferenza, va anche aggiunta la consapevolezza di molti paesi in via di sviluppo, inclusi quelli democratici, di vivere la contraddizione di dipendere sempre più da un'infrastruttura digitale come Internet, che però è disegnata e coordinata in grande parte dai paesi del Nord del mondo.
Con l'obiettivo di creare una visione e una conoscenza comune della società globale dell'informazione e di rendere più semplice il dibattito sulle differenze di opinione sulle politiche di governo di Internet, l'ITU nella Conferenza Plenipotenziaria di Minneapolis del 1988, approvò una risoluzione per proporre l'idea di un WSIS (*World Summit on the Information Society*) sotto gli auspici delle Nazioni Unite. Quest'attività ha portato a due conferenze mondiali, una a Ginevra nel 2003 e un'altra a Tunisi nel 2005. In quella di Tunisi, il 18 Novembre del 2005, a chiusura dei lavori, fu approvata l'agenda di Tunisi che conteneva la seguente definizione di Internet Governance:

"*Internet Governance is the elaboration and application, by governments, civil society, the private sector and international organizations, in their respective roles, of shared principles, norms, rules, decision making procedures and programs that shape the evolution and use of the Internet*"

Per la prima volta, un documento delle Nazioni Unite, riconoscendo la necessità del coinvolgimento di tutti gli attori nel processo di Internet *governance*, formalizzò il modello *multistakeholder*. Inoltre, in Tunisi, le Nazioni Unite risposero alla creazione di ICANN attraverso un'analoga innovazione: l' IGF (*Internet Governance Forum*), cioè un luogo di discussione sui temi dell'Internet Governance, aperto a tutti gli stakeholders, ma con funzioni puramente consultive. Il processo WSIS è stato anche una reazione alle preoccupazioni della comunità internazionale che il potere di governance su Internet fosse concentrato in poche mani. L'internazionalizzazione veniva perciò vista come la via naturale per garantire una *governance* più inclusiva.

6 Gli elementi per una nuova governance globale di Internet

La riflessione sullo stato dell'Internet Governance non può sottovalutare che mentre fino a pochi anni fa i conflitti sulla cultura e la governance di Internet erano in gran parte ipotetici, negli ultimi 10 anni le sfide ad un'Internet aperta e senza confini sono diventate realtà quotidiane. La Cina per esempio ha pubblicamente annunciato il blocco dei siti web come Facebook, Twitter e Skype. Ma anche governi democratici che di solito sostengono la libera circolazione d'idee su Internet, in alcuni casi hanno assunto atteggiamenti contrari a questi principi. Si pensi al caso del Primo Ministro inglese, che, durante le proteste di piazza a Londra nell'Agosto del 2011, accusò Twitter e Facebook di facilitare i disordini, minacciandone il blocco delle comunicazioni[10]. Anche negli USA, nell'area di San Francisco, nell'estate del 2011, l'Autorità dei Trasporti decise di interrompere le comunicazioni mobili e via Internet per contenere alcune dimostrazioni in corso. Anche le Aziende private non sono immuni da queste contraddizioni. Si pensi alle aziende manifatturiere del settore ICT che vendono le proprie tecnologie informatiche e di comunicazione IP per la sorveglianza e il controllo a governi e stati che chiaramente le useranno per scopi repressivi. Il caso più lampante è quello di aziende come Google che da un lato si fa paladina di un Internet libera e aperta (*do not evil*), ma che poi si trova costantemente coinvolta nel mancato rispetto delle leggi sulla privacy per un uso non corretto dei dati dei suoi clienti, come nel caso di Street View or Google+[11]. Questi comportamenti, pubblici e privati, sono destinati a moltiplicarsi se non si definiscono nuove istituzioni e regole per la governance globale di Internet.

6.1 Il ruolo di ICANN riformata

Il punto di partenza per un'arena istituzionale adeguata alla nuova governance globale di Internet può essere rappresentata, secondo molti osservatori, da un'ICANN riformata. La natura globale e l'esperienza tecnica acquisita fino ad oggi da ICANN, devono portare a riconoscere in ICANN il ruolo di agenzia globale per la *governance* di Internet. ICANN, per svolgere pienamente questo ruolo, deve essere profondamente riformata per diventare più responsabile (*accountable*) e trasparente nelle sue attività e la sua governance deve essere riorganizzata.
Il problema di ICANN, è quello di avere da un lato un forte potere sulle risorse critiche per la *govern-*

10 "*In wake of riots, British PM proposes social media ban*", http://articles.cnn.com/2011-08-11/tech/london.riots.social.media_1_social-media-facebook-and-twitter-blackberrys?_s=PM:TECH

11 Vedi Mackinnon R. (2012)

ance di Internet e dall'altro di non avere quelle forme di controllo sul suo operato che invece guidano di solito altre *corporation*. ICANN, non deve diventare un'organizzazione pubblica e deve mantenere la sua natura non profit. La riforma di ICANN deve riguardare essenzialmente due aspetti:

La *membership* di ICANN; il controllo dell'attività di ICANN. ICANN è una società privata. Se fosse for-profit, sarebbe controllata dal mercato. Non essendolo, non è vincolata dalla disciplina del mercato. Inoltre l'ICANN, a differenza per esempio dei RIRs (*Regional Internet Registries* che gestiscono operativamente gli Indirizzi IP a livello di aree regionali del mondo ed hanno come membri gli operatori telefonici, gli ISPs, ecc.), non ha *azionisti*, per statuto. Questo sembra essere il limite fondamentale nel modo in cui è costituita[12]. Ogni riforma di ICANN deve perciò prevedere la revisione del concetto di *membership*.

L'altro elemento critico è il consiglio di amministrazione, la cui attività non può essere impugnata. Il processo di controllo e di appello delle decisioni del *Consiglio di amministrazione* è molto debole. Possono essere, infatti, costituiti *review panel* ad hoc che hanno solo la possibilità di richiedere, in modo non vincolante, al *Consiglio* di riconsiderare le decisioni prese (riinserendo per esempio la questione nuovamente all'ordine del giorno). Ogni ipotesi di riforma deve prevedere perciò la creazione di un processo indipendente di revisione delle decisioni del *Consiglio di amministrazione* che preveda la possibilità esplicita di cambiarne le decisioni.

6.2 L'approccio multi-stakeholder: una strada da consolidare

È stato evidenziato in precedenza che, nella dinamica tra Stati nazione e le nuove opportunità di partecipazione e di trasparenza offerte da Internet, l'approccio *multi-stakeholder* si basi sugli attori esistenti come i governi, il settore privato, la società civile, le organizzazioni internazionali. È necessario però evidenziare che mentre il sistema degli stati nazione non rappresenta la forma più adeguata per governare Internet, va anche detto che il processo multi-stakeholder, sia per ICANN e sia per l'IGF, è ancora nelle sue fasi iniziali e che probabilmente funziona molto bene per la governance di singole entità, ma molto meno quando applicato al governo di processi complessi. Per quanto riguarda, per esempio, i meccanismi di partecipazione, va detto che il diritto alla partecipazione e il carattere aperto proprie del processo *multi-stakeholder* non garantiscono per sé l'effettiva partecipazione degli attori rilevanti per il processo. La partecipazione e la condivisione sembrano essere diventati fine a se stessi. Questo processo è definito da alcuni osservatori, un "*new partecipatory evangelism*" e sembra però offrire più opportunità di pura partecipazione che una concreta disponibilità a influenzare le decisioni. C'è infatti una significativa differenza tra *making your views known and making your views count* [13].

È questa un'area in cui il processo multi-stakeholder deve migliorare attraverso la definizione di meccanismi che rendano più effettiva la partecipazione alle decisioni.

Analoghe considerazioni possono essere fatte per quanto riguarda la trasparenza del processo. Uno dei limiti può essere l'information overload legato all'eccessiva trasparenza. Migliaia di pagine di documenti, studi, relazioni dei vari meeting sono disponibili sui siti dell'ICANN o dell'IGF. Uno sforzo va fatto per render più facilmente accessibile questo materiale.

Si possono creare inoltre problemi di cattura da parte di stakeholder particolarmente forti nella rappresentanza (paesi sviluppati nell'IGF e nel GAC, imprese USA nel settore privato, come gli Internet Evangelist, ecc.) e quindi è necessaria una corretta azione di mutua vigilanza[14].

7 L'ITU e l'Internet *Governance*

Le condivisibili preoccupazioni gestionali legate al fatto che l'ICANN non diventi un'organizzazione pubblica internazionale, non devono impedire di affrontare senza ideologia il ruolo che l'ITU può svolgere nel processo multistakeholder di governo di Internet.

La Conferenza di Dubai ha purtroppo evidenziato l'esistenza ingiustificata di una sorta di fobia verso l'ITU e il suo fantomatico ruolo di minaccia enorme e permanente alla governance d'internet[15]. Questa posizione è incarnata soprattutto da industry leader come Vint Cerf di Google. Quest'approccio non è giustificabile, perché l'ITU non ha alcun potere diretto sulla governance di Internet. Più in generale non ha potere di enforcement diretto, ma si basa solo sull'iniziativa degli stati membri. Inoltre, dal punto di vista della standardizzazione la sua centralità dagli anni

12 Vedi Milton Mueller (2010), pag 249
13 Vedi IGP (2009)
14 Vedi La Chapelle (2011)
15 Vedi Milton Mueller (2012)

'80 si è oggettivamente ridotta. Per quanto riguarda Internet, l'attività dell'ITU è essenzialmente definita dalle Risoluzioni 101 "*Internet Protocol (IP)-based Networks*" (Rev. Guadalajara, 2010), dalla Risoluzione 102: "*ITU's role with regard to international public policy issues pertaining to the Internet and the management of Internet resources, including domain names and addresses*" (rev Guadalajara, 2010), e Risoluzione 133: "*Roles of administrations of Member States in the management of International (multilingual) domain names*" (Rev. Guadalajara, 2010).
Complessivamente, nei vari ambiti di competenza da esse previste, queste risoluzioni invitano l'ITU a cooperare e a coordinare l'attività con le altre organizzazioni che caratterizzano oggi la governance di Internet quali l'ICANN, i RIRs, lo IETF, l'ISOC e il W3C. In questo contesto quindi la presenza dell'ITU nel processo di Internet Governance è pienamente legittimata. Per quanto riguarda poi la natura multistakeholder dell'ITU, è in corso un dibattito. Secondo l'ITU, a parte i governi e il settore privato che già aderisce come sector member, anche la società civile può seguire questo processo e nel caso d'istituzioni non-profit che abbiano un carattere internazionali esse possono anche richiedere l'esenzione dal pagamento della sector member fee[16]. Secondo alcuni la partecipazione di alcuni gruppi stakeholder, come la società civile, potrebbe essere migliorata[17]. Da questo punto di vista, è indubbio che l'ITU debba diventare più trasparente, rendendo disponibili gli atti e i materiali dei suoi gruppi di lavoro e soprattutto del Council Working Group on International Internet Related Public Policy Issues che dovrebbe essere anche aperto ai membri di settore e alla società civile. Questi miglioramenti dal lato della trasparenza aiuterebbero a eliminare incomprensioni e creerebbero un clima più favorevole al confronto e alla cooperazione tra tutti i soggetti che animano il processo multistakeholder.

8 Dalla governance Multi-stakeholder a quella multi-institutional

Secondo alcuni osservatori, la varietà dei temi e delle criticità legate a Internet rende impossibile avere un unico regime di *governance*. Infatti, una *governance* unificata richiederebbe una visione comune sul futuro di Internet e sui problemi che la *governance* dovrebbe risolvere. Questo consenso non esiste. Di conseguenza, l'attuale sistema di *governance* dovrà evolversi da un sistema *multi stakeholder* a uno *multi-institutional*. In altre parole si tratterebbe di associare a ogni esigenza di governance, l'istituzione più adatta ad affrontarla. Perciò, alcuni problemi come la *Cybersecurity*, richiederanno un coinvolgimento maggiore degli stati nazione, attraverso anche accordi internazionali e globali tra loro. Altri invece, come la definizione di standard tecnici e d'interoperabilità possono essere gestiti meglio attraverso meccanismi di *self-regulation* and *co-regulation* tra gli *stakeholder* principali. Temi riguardanti comunità ad hoc, come per esempio l'uso d'internet per persone diversamente abili, sarà gestito meglio attraverso un processo bottom-up che includa le comunità direttamente interessate[18].

9 Conclusioni

La natura sempre più globale e pervasiva di Internet pone con forza la necessità di nuove istituzioni globali. Il punto di partenza deve essere il riconoscimento di ICANN come agenzia globale per la governance di Internet. Bisogna lavorare però a migliorarne la trasparenza e la responsabilità (*accountability*) delle sue azioni. Il lavoro di definizione delle policy all'interno di questo quadro istituzionale va invece svolto dagli *stakeholder* dei vari settori: governi, settore privato e società civile che partecipano a ICANN. Nel complesso il processo multi stakeholder va migliorato e va fatto evolvere verso un sistema multiistituzionale, in cui ci sia un rapporto più stretto tra sfida da governare e istituzione più adatta al governo di ciascun processo. La governance globale di Internet non ha ancora raggiunto un equilibrio: il processo di cambiamento istituzionale continua! ■

Bibliografia

Bauer, J. (2011), Panarchy, Kiel Global Economic Symposium

Bernabè F. (2012), "*Libertà Vigilata: privacy, sicurezza e mercato nella rete*", Laterza

De La Chapelle B. (2011), Internet Policy Making, MIND

Ellickson R. (1991) "Order without Law: How Neighbors Settle Disputes, Harvard College

Hardin G. (1968), "The Tragedy of the Commons", Science 162, 1243-1248

Hardin G. (1998), "The extension of the Tragedy of the Commons", Science 280, 682-683

16 ITU (2013) http://www.itu.int/en/membership/Pages/default.aspx

17 WTPF report , Cisco and ISOC Contribution (2013)

18 Vedi :Johannes Bauer, (2011)

IGP (2009), "ICANN, Inc: Accountability and participation in the governance of critical Internet resources"

In wake of riots, British PM proposes social media ban", http://articles.cnn.com/2011-08- 11/tech/london.riots.social.media_1_social-media-facebook-and-twitter-blackberrys?_s=PM:TECH

ITU(2013): http://www.itu.int/en/membership/Pages/default.aspx.

ITU- WTPF report, 2013

Mueller M, (2012), "ITU Phobia:why WCIT was derailed ", IGP Blog

Milton Mueller (2010), Networks and States, MIT Press

Mueller M. (2002), "Names , Number and Global Governance" in "Cyber Policy and Economics in an Internet Age", a cura di William Lehr and Lorenzo Pupillo, Kluwer Academic Publisher

OECD(2011) http://www.oecd.org/document/19/0,3746en_2649_201185_47056659_1_1_1_1,00.html

Mackinnon R. (2012) "Consent of the Networked, The worldwide struggle for Internet freedom", Basic Books

Schoenberger v. e Malte Ziewitz (2005) " Jefferson Rebuffed: The United States and the Future of Internet Governance" working paper

Strom E. (1990), "Governing the Commons" Cambridge University Press.

Yoo, C. (2012), "The Dynamic Internet ", AEI press

lorenzo.pupillo@telecomitalia.it

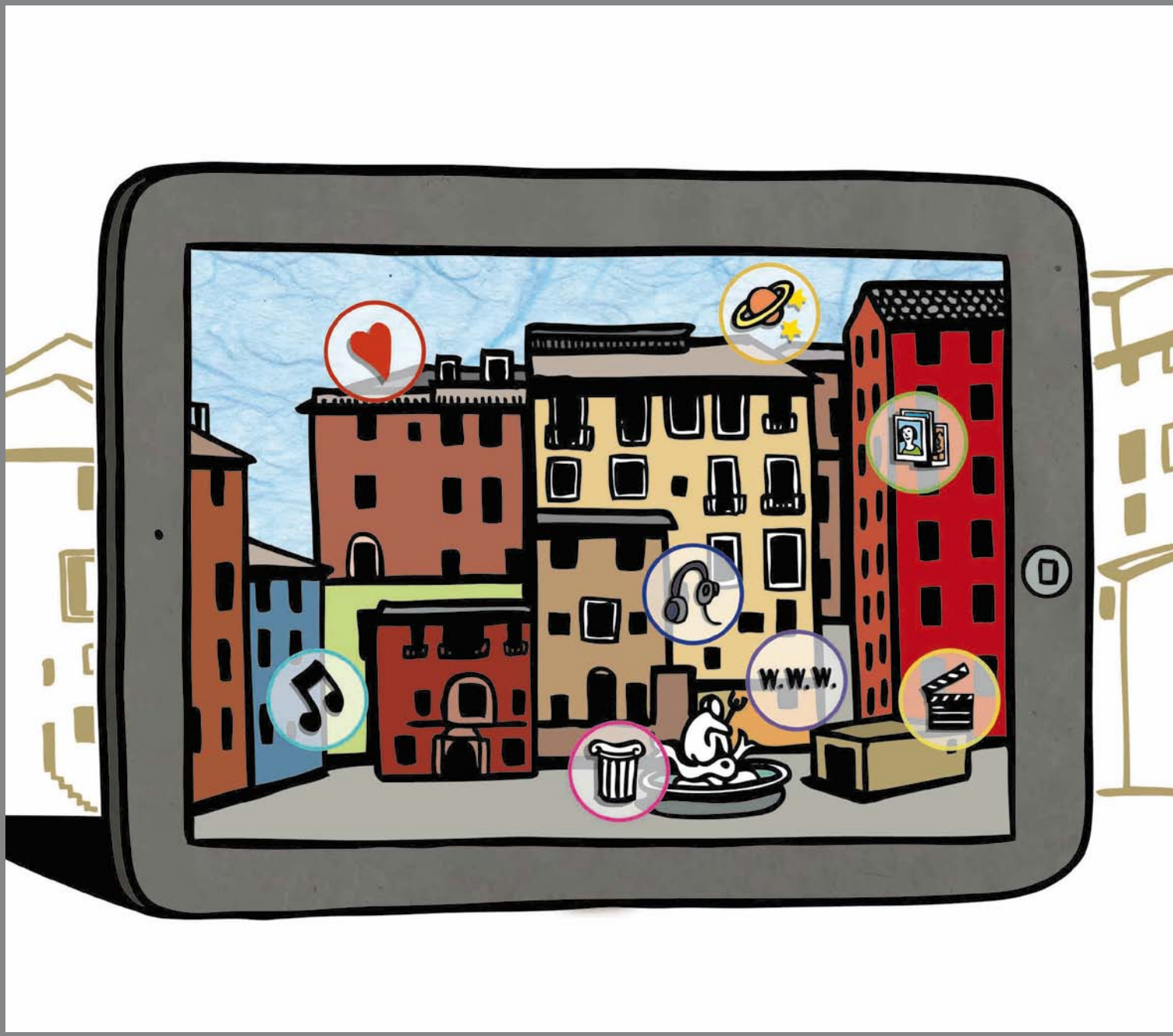
Lorenzo Maria Pupillo

Dottore in matematica, specializzato in Gestione dell'Economia e dell'Impresa all'Istituto Adriano Olivetti di Ancona e PhD all'University of Pennsylvania di Filadelfia con una tesi in Economia delle Telecomunicazioni, oggi opera nel settore Public and Regulatory Affairs di Telecom Italia e si occupa di Internet Governance, di Internet Policy and Economics , di Green ICT and Energy e di Reti di Nuova Generazione.
In precedenza, in Azienda ha ricoperto diversi ruoli e responsabilità; è stato anche Advisor del Global Information and Communication Technologies Department della Banca Mondiale in Washington. Prima di lavorare per Telecom Italia è stato Member of Technical Staff ai laboratori Bell dell'AT&T in New Jersey (USA), economista presso l'ISAE e consulente per aziende pubbliche e private e organizzazioni internazionali.
È Affiliated Researcher al Columbia Institute for Tele Information della Columbia University.
Ha pubblicato diversi libri e articoli in econometria applicata, economia industriale e telecommunications policy.
È membro dei comitati editoriali di numerose riviste economiche internazionali. È inoltre membro di vari advisory board di organizzazioni professionali ed istituti di ricerca internazionali.

Usa il tuo smartphone per visualizzare approfondimenti multimediali

SGUARDO AUMENTATO: SCENARI APPLICATIVI

Carmen Criminisi, Luca Lamorte, Elio Paschetta, Nicoletta Salis



Per Realtà Aumentata o realtà mediata dall'elaboratore si intende "l'arricchimento della percezione sensoriale umana mediante informazioni, in genere manipolate e convogliate elettronicamente, che non sarebbero percepibili con i cinque sensi"[1]. In questa definizione si nasconde il concetto di come sia cambiato il nostro modo di interagire con la realtà che ci circonda e gli oggetti che la compongono. In questo articolo si descrivono alcuni scenari applicativi di soluzioni in modalità aumentata.

1 Introduzione

La "Realtà Aumentata" permette di mescolare il mondo esterno con informazioni e contenuti digitali "invisibili" all'occhio umano, ma non all'occhio "attento" del telefonino (Figura 1): questa tecnologia permette di sovraimporre degli oggetti digitali interattivi sullo schermo, rendendo, quindi, la realtà "cliccabile e connessa".

Telecom Italia, già a partire dal 2010, ha approfondito questo nuovo paradigma di ricerca visiva e interattiva, declinandolo su diversi filoni applicativi: dal mondo della carta stampata, a

Figura 1- Il paradigma della Realtà Aumentata

quello del turismo, della casa e del negozio.

2 Il mercato di riferimento

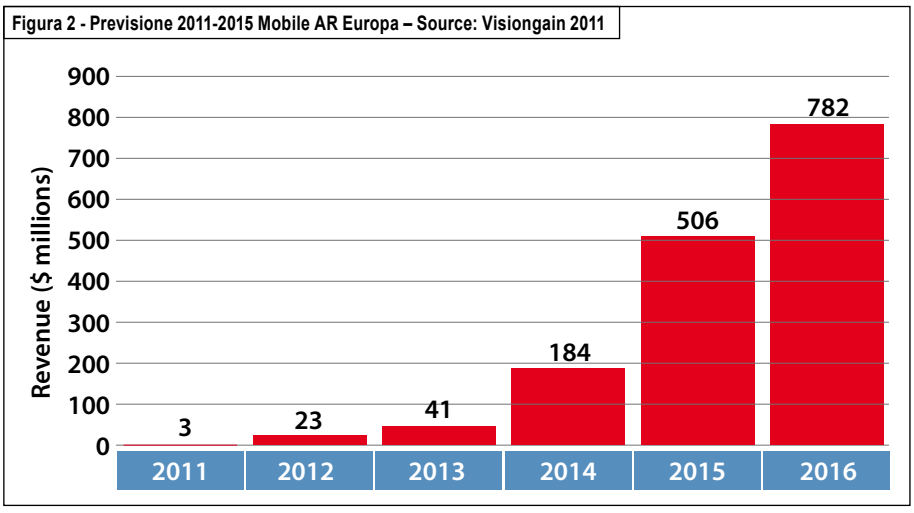
Per contestualizzare questa tecnologia rispetto al mercato, di seguito è riportato un diagramma che illustra la previsione di crescita del Mobile Augmented Reality (MAR) nel quinquennio 2011-2016 per il mercato europeo.
Come si nota, è attesa una crescita esponenziale nei prossimi 3 anni. La ricerca di Visiongain mostra che il mercato Europeo del MAR rappresenterà nel 2016 il 27% del mercato globale
Secondo la ricerca condotta da Visiongain [2], anche negli altri mercati stranieri è attesa una crescita tanto significativa da essere indicata come una delle più rilevanti e globali nel settore delle comunicazioni e della tecnologia per il quinquennio fino al 2016.
In questo contesto la maggior parte delle revenue dovrebbe arrivare dall'advertising, che resta il modello di business più promettente e l'evoluzione nonché l'affermazione del MAR sono smartphone technology driven. Nel tempo, il MAR cambierà la sua proposizione: da tecnologia stand alone, diventerà sempre più integrata in altre forme di comunicazione, gaming, social media e mass media.

3 La piattaforma ARTES di Telecom Italia

ARTES (*Augmented Reality Telco Enablers & Services*) è la piattaforma tecnologica di riferimento server-side, realizzata integralmente in Telecom Italia persupportare le applicazioni e i servizi che utilizzano il paradigma della Realtà Aumentata.
Questa piattaformaè stata concepita come una soluzione modulare per garantire la massima flessibilità di espansione e di aggiunta di funzionalità e gli scenari di servizio che verranno descritti nei prossimi paragrafi ne dimostrano la sua versatilità .
La piattaforma rende disponibili, a livello programmatico, delle API (Application Programming Interface) che permettono la facile implementazione, anche a possibili partner esterni, di feature di AR su servizi Telecom Italia anche già commerciali. Nei primi mesi del 2013 la piattaforma ARTES è stata messa in esercizio sulla Nuvola Italiana di Telecom Italia per rendere disponibili le varie componenti/funzionalità sia per le altre piattaforme commerciali di Telecom Italia sia ai clienti (business, in particolare, secondo il modello B2B2C o anche B2B2B2C) per l'offerta di nuove proposizioni basate sulle funzionalità più avanzate (advertising, AR social, AR Campaigns, ...). La Figura 3 mostra l'architettura modulare della piattaforma e la suddivisione in due fasi del progetto di messa in campo:

- La prima fase si incentra prevalentemente sull'AR Browsing, ossia sulla vista sulla fotocamera del telefono di elementi aumentati in sovraimpressione, sulla base dell'output di sensori come GPS e bussola, ma senza riconoscere (e quindi interagire) con il flusso live delle immagini della fotocamera; verranno quindi abilitate in Fase I funzionalità come:
  - *Mash-up*: Fusione delle informazioni e dei contenuti da più fonti (social e istituzionali);
  - *Cluster*: Presentazione dei punti di interesse in "grappoli" (cluster) per una migliore fruizione;
  - *AR Search per POI e Free Text*: Ricerca dello specifico POI di interesse o tutti i POI che sono correlati al testo immesso per la ricerca;
  - *Advertising Personalizzato*: advertising ad hoc per il cliente o possibilità di "guadagnare punti" giocando con la realtà che lo circonda;
  - *AR Social*: possibilità di vedere i messaggi FB e TW intorno a se' e interagirvi;
  - *Eventi-Itinerari*: scoprire eventi o itinerari suggeriti;

Figura 2 - Previsione 2011-2015 Mobile AR Europa – Source: Visiongain 2011



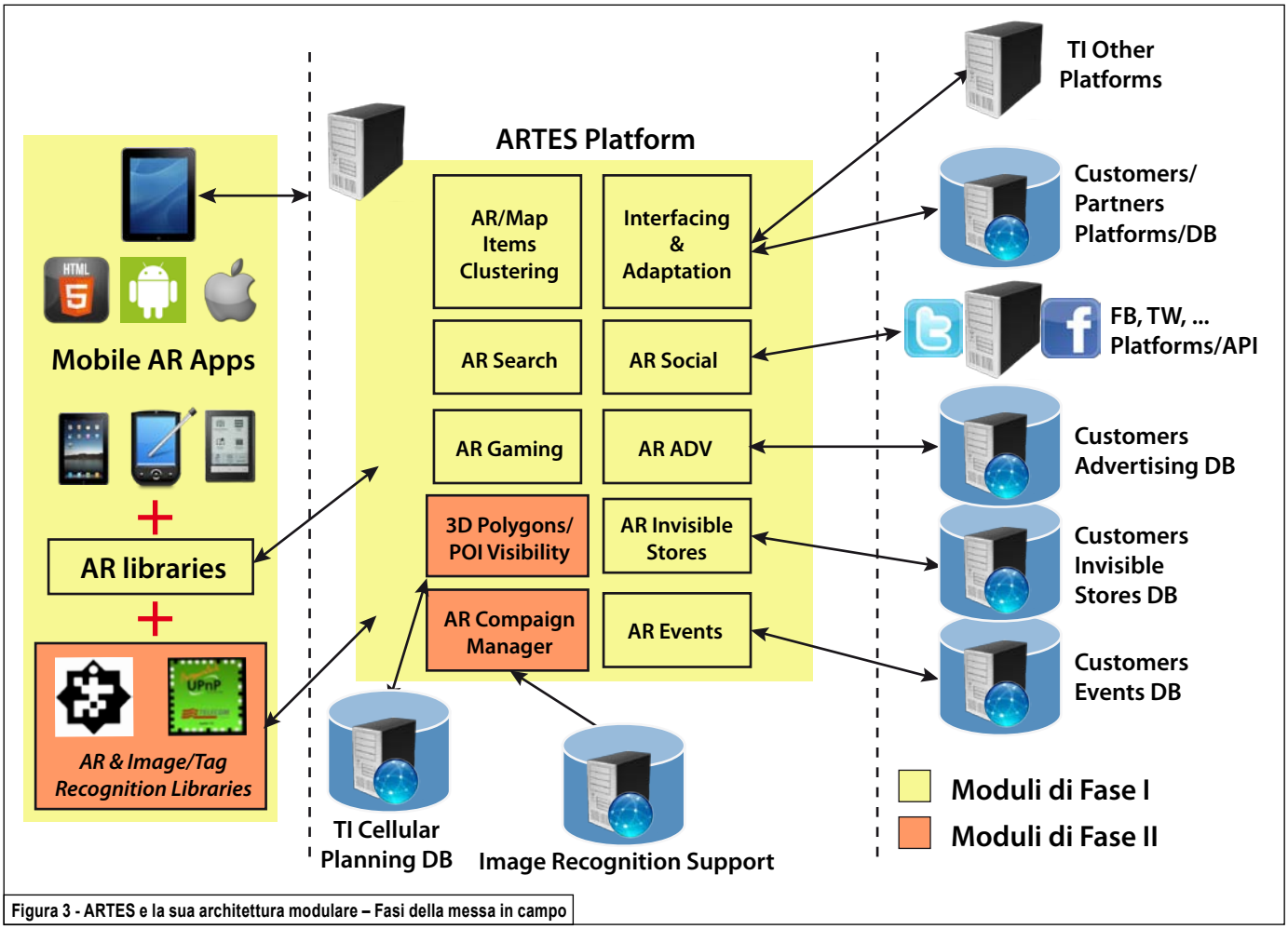


Figura 3 - ARTES e la sua architettura modulare – Fasi della messa in campo

- *Condivisione*: esprimere un giudizio o lasciare un commento;
- "*Invisible Store*": vetrina virtuale per prodotti e negozi.

• La seconda fase aggiunge alle caratteristiche tecniche di Fase I anche il riconoscimento visuale real-time del flusso live delle immagini della fotocamera, con sovrapposizione di icone 2D/3D alle immagini di riferimento scelte come target dal sistema per il riconoscimento; verranno quindi abilitate in Fase II funzionalità come:

- *Augmented Magazine*: inquadrando con lo smartphone una rivista, si scoprono nuovi contenuti multimediali di approfondimento (il caso del Notiziario Tecnico n. 1 del 2013);
- "*Vedo dentro*":
  - inquadrando un prodotto commerciale (ad esempio un modem ADSL, il nuovo telefono Sirio Classico di Telecom Italia, ...), il cliente può «scoprire» prima dell'acquisto tutti i dettagli sul prodotto ;
  - inquadrando un monumento, un ristorante, ... se ne può esplorare l'interno;
- *Augmented Products*: inquadrando un prodotto commerciale, il cliente vi può interagire con giochi/ads/packaging virtuale/personaggi 3D, ...;
- *Augmented Home*: interazione con gli oggetti di casa in tempo reale: inquadrando gli elettrodomestici di casa, si potranno visualizzare i consumi in tempo reale e agire con un click sugli elettrodomestici stessi.

3.1 Augmented Reality SDK

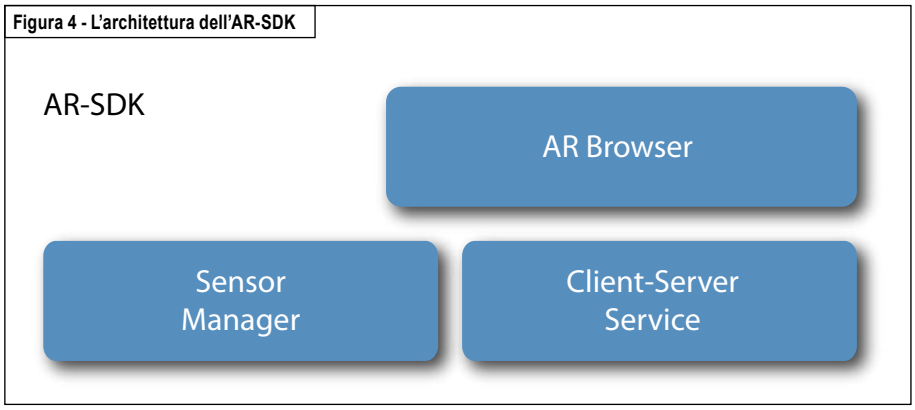
Nell'architettura generale di Figura 3 è mostrato anche il dominio mobile e applicativo della piattaforma (parte sinistra). In particolare è identificato un modulo chiamato "AR Libraries": infatti, l'esperienza maturata nello sviluppo di servi-

zi AR ha evidenziato la necessità di creare un SDK (*Software Development Kit*) o meglio un componente software che permettesse di velocizzare la realizzazione delle applicazioni e di sollevare lo sviluppatore dalla gestione di noti problemi/attività che un'applicazione di questo tipo richiede. Il primo fra tutti consiste nella gestione corretta delle funzionalità esposte dagli smartphone come per esempio i sensori di Localizzazione e di Orientamento. Soprattutto questi ultimi, se mal gestiti, inficiano notevolmente la stabilità ed l'usabilità dell'applicazione. L'utilizzo di filtri è essenziale per attenuare e rendere più armonici i movimenti degli oggetti digitali da visualizzare sulla scena live che lo smartphone sta inquadrando che risulterebbero altrimenti fluttuanti, rendendo l'esperienza sgradevole. Un secondo ed importante elemento è la connessione con il Server, attraverso cui lo smartphone mantiene aggiornati i contenuti da visualizzare sulla base del contesto (location, raggio d'azione, categorie, tipologia di vista, etc). In ultimo, è necessario interagire con la fotocamera dello smartphone per poter applicare sulla sua vista un "livello" aggiuntivo che presenti all'utente i contenuti arricchiti.
Mettendo a fattor comune le esperienze acquisite con i primi prototipi delle applicazioni AR e con la piattaforma ARTES, abbiamo sviluppato una libreria AR, chiamata AR-SDK, con la quale è possibile creare con semplicità un'applicazione di Realtà Aumentata, in quanto gestisce principalmente le tre problematiche evidenziate sopra e lo sviluppatore dovrà solo preoccuparsi del l'interfaccia grafica e dell'interazione con l'utente.
L'architettura dell'AR-SDK è quella presentata in Figura 4 ed è composta dai seguenti moduli:

- Client-Server Service per la gestione della connessione con la piattaforma Artes, attraverso un Servizio Android;
- Sensors Manager per la gestione del sensore di Posizione e Location con l'aggiunta di filtri per attenuare la risposta non sempre "stabilizzata" del sensore;
- AR Browser dal quale viene aperto lo stream della Fotocamera (come sfondo) ed è possibile applicare dei livelli che lo svilippatore puo estendere e personalizzare ed automaticamente vengono visualizzati in sovrapposizione della camera.

Oggi l'AR-SDK è in versione "beta", per cui molte altre funzionalità potrebbero essere aggiunte in seguito per rendere ancora più semplice creare la propria applicazione AR.

Figura 4 - L'architettura dell'AR-SDK



4 L'attività di standardizzazione del Mobile Augmented Enabler

Parallelamente alle attività di prototipazione interna della piattaforma ARTES e delle relative applicazioni, è stata guidata da Telecom Italia in OMA (*Open Mobile Alliance*) [10] anche l'attività di standardizzazione di un framework completo per abilitare servizi mobili basati sulla Realtà aumentata fortemente inspirato a ARTES. In particolare sono stati definiti, secondo un paradigma client-server, i componenti funzionali del framework di riferimento e le interazioni tra essi.
L'enabler MobAR assicura scambio e accesso universale agli AR Content, fornendo meccanismi per il trasporto, il filtering e la personalizzazione degli AR Content. OMA MobAR, come detto è costruito secondo un modello client-server, con il MobAR Client che ottiene dal MobAR Server informazioni e contenuti che arricchiscono/aumentano la scena che l'utente sta esplorando attraverso il suo cellulare.
In particolare, con l'introduzione nell'architettura dell'AR-SDK descritto sopra, la piattaforma ARTES è sempre più compliant alle specifiche tecniche OMA MobAR. Alcuni dei prototipi mobili su ARTES e compliant con lo standard OMA MobAR sono stati mostrati al MWC 2013 [8] durante un evento, che aveva lo scopo di dare rilevanza alla specifiche tecniche definite in OMA, mostrando alcune implementazioni di esse.

5 Scenari applicativi

Qui di seguito sono riportati i principali scenari applicativi che,

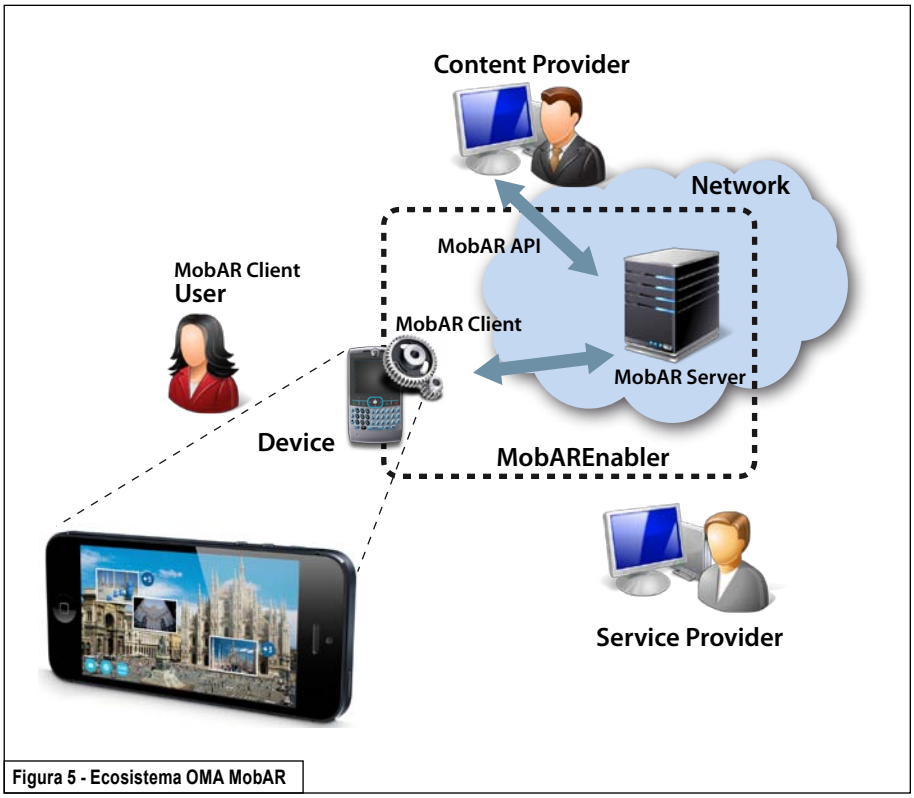


Figura 5 - Ecosistema OMA MobAR

Figura 6 - Icona che identifica la presenza di un contenuto aumentato nel Notiziario Tecnico

accanto all'Augmented Magazine applicato a questa stessa rivista, rappresentano filoni di applicazione diretta della Realtà Aumentata.

5.1 Augmented Magazine

Lo scenario applicativo che può "sperimentare" chi sta leggendo in questo momento questo primo numero del Notiziario Tecnico 2013 di Telecom Italia è quello identificato con il termine di Augmented Magazine, con il quale in generale ci si riferisce ad un arricchimento con contenuti extra di una rivista, un libro o in generale della carta stampata.
L'Augmented Magazine èuno strumento molto potente, in quanto aiuta ad espandere potenzialmente all'infinito lo spazio per sua natura "limitato" della carta stampata, abilitando inoltre anche un'interazione immediata con contenuti multimediali e interattivi.
Grande risonanza mediatica ha avuto per esempio la scelta di Ikea per il suo catalogo 2013, a cui ha affiancato contenuti multimediali e 3D in AR [3]: sfogliando il catalogo cartaceo, e "guardando" le pagine stampate tramite lo schermo del proprio smartphone ricostruzioni tridimensionali dei mobili si avvicendano a gallerie fotografiche di uno stesso ambiente di casaQuesta idea è stata mutuata e personalizzata per applicarla in Telecom Italia proprio al nostro Notiziario Tecnico con la nuova app L'Editoria+ che si può installare sia dall'Apple Store che da Google Play.
Sfogliando questa rivista, trovate in alcune pagine l'icona riportata in Figura 6. Questa indica la presenza di contenuti AR che arricchiscono l'esperienza del lettore. Puntando il proprio smartphone

Figura 7 - Icone 3D per accedere ai contenuti aggiuntivi

verso la pagina, l'app L'Editoria+ sarà in grado di riconoscerla e sovraimporrà sullo schermo un'icona digitale indicativa del contenuto multimediale che aumenta e completa ciò che è stato stampato. Quindi in base al contenuto che arricchisce la pagina, sullo schermo del proprio dispositivo si animeranno icone 3D, attraverso le quali si accede ad un livello superiore di esperienza di lettura: si andrà quindi oltre le "sole parole" stampate per scoprire dettagli, approfondimenti che resterebbero difficilmente accessibili.

Figura 8 - Il prototipo SeeAR

5.2 Augmented Tourism

Uno dei campi applicativi più immediati per la Realtà Aumentata è il turismo, ossia la declinazione di questa tecnologia con l'obiettivo di supportare il cittadino/turista nella fruizione intelligente e innovativa della città e/o di un'esposizione-mostra.

5.2.1 SeeAR: la Realtà Aumentata attorno a me

SeeARè stato, nel 2011, il primo prototipo di applicazione mobile sviluppato a scopo prevalentemente turistico/informativo in Telecom Italia [4].
L'utente, guardandosi attorno alla ricerca, ad esempio, di un ristorante di cucina tipica, contestualmente trovava anche un insieme di informazioni utili al fine di individuare il locale a lui più congeniale. Cliccando su uno dei "fumetti" mostrati in sovraimpressione sulla camera del cellulare (si veda Figura 8) l'utente poteva accedere ad una scheda ricca di informazioni: l'indirizzo e il numero di telefono, i contenuti istituzionali relativi a quel punto di interesse (come il sito web), le recensioni e i commenti degli utenti, possibilità di fare "check-in" o di vedere chi dei propri amici l'aveva già fatto, il menù e le promozioni del ristorante stesso. Con SeeAR si poteva anche "dialogare", chiedendo, ad esempio, di farsi accompagnare, "guidare verso" il punto di interesse selezionato. E dopo la visita si poteva lasciare il proprio "segno", commentando e votandoil locale, in modo da condividere la propria esperienza con gli amici.
Un altro modo per agevolare l'accesso ai contenuti consiste nella funzionalità del "Freeze" ovvero "fotografare la realtà aumentata", che permette di "bloccare" la scena della vista con tutte le informazioni aggiuntive sovraimpresse, che possono poi essere "cliccate" in un secondo momento.

5.2.2 La Smart City App per Expo 2015

Nel campo Augmented Tourism, c'è anche la Smart City App per Expo 2015. In seguito all'aggiudicazione del Bando di Gara emesso dalla società Expo 2015 S.p.A. "per l'affidamento del servizio di ideazione e sviluppo di un prototipo relativo alla piattaforma tecnologica "Smart City Mobile Platform" per la fruizione intelligente della città, utilizzabile in movimento nell'ambiente urbano su devices mobili", Telecom Italia, in quanto mandataria del RTI (Raggruppamento Temporaneo di Impresa) con le società specializzate Telecom Design e Click'n'Tap, ha guidato la progettazione e l'implementazione end-to-end del prototipo[7], che è stato presentato in anteprima. al Mobile World Congress di Barcellona [8].
La Smart City App vuole essere lo strumento di riferimento per fornire informazioni, servizi e intrattenimento su Expo 2015, sui Paesi partecipanti, sul territorio cittadino e nazionale, sui partner e tutti gli attori coinvolti. Lo scopo è assicurare una relazione costante con il visitatore, anche attraverso le reti di connettività mobile di nuova generazione LTE e i dispositivi più evoluti, che garantiranno esperienze sempre più coinvolgenti e complete.

Figura 9 - La Social Camera - una delle funzionalità di Realtà Aumentata della Smart City App

In particolare, il primo prototipo della Smart City App integra alcune tecnologie innovative come la Realtà Aumentata e il Visual Search, grazie alle quali è possibile vedere Milano oggi ed Expo 2015 domani in modo sorprendente, unendo la visione reale ad animazioni e contenuti multimediali che arricchiscono l'esperienza del cittadino e del turista. Inoltre, questa applicazione consente di sperimentare una maggiore interattività social, con modelli di comunicazione visuali (urban painting) e la creazione di percorsi condivisi con i propri amici, con chi ha già vissuto le stesse esperienze o intenderà farle (personal assistant).
L'applicazioneè strutturata in diverse sezioni:

- *Personal Assistant*: funzionalità, informazioni e strumenti che consentiranno all'utente di organizzare al meglio la propria visita dell'Expo e della città, condividendo la propria esperienza con gli amici e sui Social Network;
- *City Map & AR Vision*: mappe (2D, 3D e AR) interattive e arricchite di informazioni aumentate, che permettono l'accesso ai POI social/augmented nelle vicinanze e la ricerca di punti di interesse sulla base di categorie (e.g. ristoranti, monumenti, ...);
- *AudioTour*: Audio guide interattive della città, che accompagnano l'utente nel suo percorso di visita;
- *You Paint*: contenuti augmented creati da Expo e dagli utenti associati a specifiche posizioni nella città
- *Social Camera*: visualizzazione, e.g., delle immagini di un luogo condivise sui principali SN, di POI, ..., in overlay alla vista live della fotocamera, con la possibilità di "catturarle" e di fare "social sharing" (Figura 9).

In parallelo Telecom Italia sta lavorando per rendere possibile la fruizione di alcune delle funzionalità della Smart App progettata su smartphone Android, opportunamente adattate e riprogettate, anche su Tablet e, nei prossimi mesi, anche sui cosiddetti Smart Glasses, al fine di raggiungere un adattamento e una massimizzazione della user experience nell'interazione con l'App anche tramite questi nuovi device che si stanno affacciando sul mercato.

5.3 Augmented Home

Un ulteriore campo di applicazione della Realtà Aumentata approfondito da Telecom Italia riguarda il filone dell'Home Automation. L'obiettivo della ricerca è quello di sfruttare la piacevolezza della user experience dell'AR per visualizzare informazioni utili per l'utente, al fine di monitorare lo stato dei propri elettrodomestici, il loro consumo ed eventuali malfunzionamenti in essere.
Attraverso un approccio Technology Driven il team di lavoro, attraverso sessioni di brainstorming e l'utilizzo della propria creatività e delle specifiche competenze tecniche, ha ideato un mock up animato di una applicazione di Augmented Home realizzato con un tool di rapid prototyping. Di seguito vengono descritte le principali funzionalità del servizio.

- *Login e Configurazione della casa*: al primo accesso all'utente viene richiesto di configurare la propria casa in una modalità intuitiva al fine di poter meglio collocare la posizione dei propri elettrodomestici all'interno dell'abitazione ed agevolare cosi la fase successiva di riconoscimento dell'ambiente;
- *Provisioning*: l'app chiede all'utente di fare un provisioning di foto degli ambienti domestici. Quando nessuna foto è presente l'utente verrà invitato a scattare delle foto della propria casa;
- *Riconoscimento*: l'app è pronta. Ad ogni nuovo accesso i l'app

Configurazione della casa

Presentazione informazioni in AR

Funzione Fault in modalità AR

partirà con la schermata del riconoscimento, per poi accedere alle principali funzionalità dell'app.: la sezione "Info", la sezione "Lente" e la sezione "Fault";

- *Info*: riconoscendo l'elettrodomestico si possono avere informazioni sullo stesso (stato di funzionamento, tempo al termine, consumi, ecc...) con dei messaggi di pop-up;
- *Lente*: si esplora l'interno di un elettrodomestico, accedendo anche al manuale senza dover ricorrere alle istruzioni cartacee.
- *Fault*: segnala la presenza di malfunzionamenti all'interno degli elettrodomestici della casa. L'app permette così di scoprire anche quale sia il guasto.

L'app SmartHome consente quindi di riconoscere dispositivi "Smart", ossia quei dispositivi capaci di comunicare con la rete domestica per fornire informazioni aggiuntive, ad esempio sul loro stato e il loro consumo.

5.4 Augmented Products

Un altro ambito di applicazione della Realtà Aumentata di Telecom Italia è quello dei prodotti aumentati o Augmented Products. L'idea di fondo è quella di utilizzare la Realtà Aumentata come ulteriore strumento di comunicazione che potenzia l'efficacia dei media tradizionali (flyer, video, web sites, ...). L'efficacia dell'offerta risulta così massimizzata e l'utente finale può essere supportato nelle sue azioni quotidiane di acquisto e di utilizzo dei prodotti Telecom Italia (in particolare del-

la casa digitale, delle nuove offerte Fibra e mondo ultra-Internet, ...). Tra i possibili scenari:

- *Nel negozio*: "conosco cosa compro": in questo scenario il cliente, avvicinandosi ad esempio, al nuovo Sirio Classico di Telecom Italia (Figura 11) o alla scatola del modem ADSL, lo riconoscerà col proprio smartphone e in AR visualizzerà una serie di informazioni che lo aiuteranno a meglio conoscere il prodotto: pubblicità, sconti, specifiche tecniche, contenuto della scatola;
- *A casa*: "aiuto al montaggio": in questo secondo scenario il cliente, comprato il prodotto, verrà supportato nel montaggio e nella configurazione del dispositivo passo dopo passo (Figura 12).

Figura 11 - Come può essere aumentato il nuovo Sirio Classico di Telecom Italia

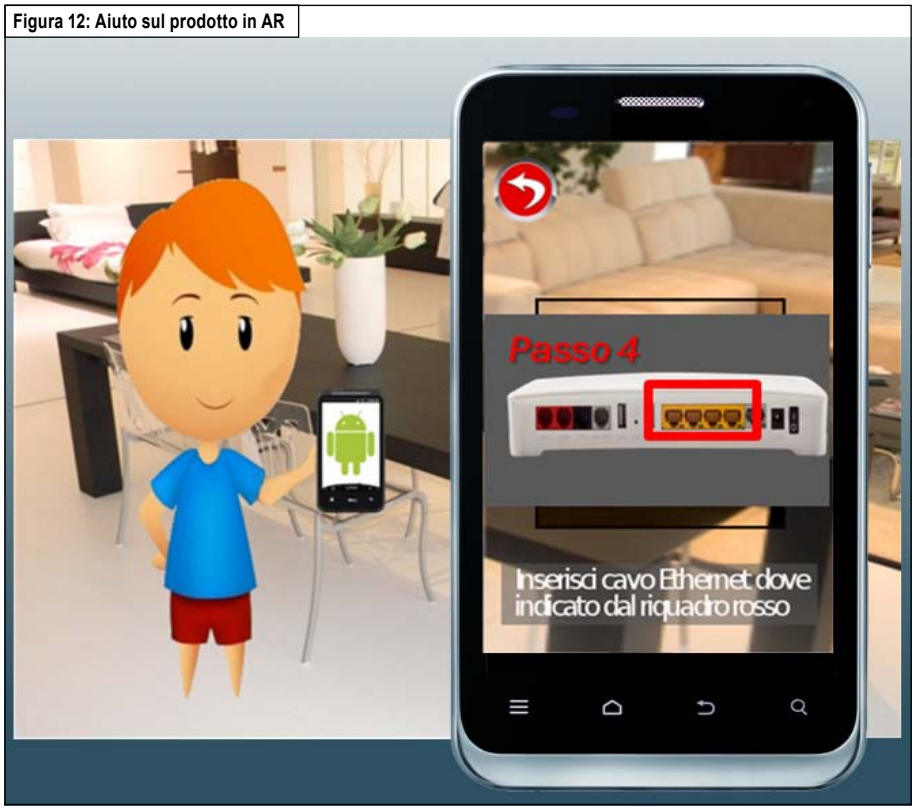
Conclusioni

Telecom Italia nei suoi laboratori di ricerca e innovazione sta continuando a lavorare per migliorare sempre più gli scenari applicativi e gli altri servizi prototipali basati su questa tecnologia, investendo sulle nuove funzionalità di:

- "riconoscimento e interazione", ossia sul riconoscimento automatico delle immagini e degli oggetti in esse contenuti unito alla tecnologia della realtà aumentata, in modo da perfezionare la user experience dell'utente sia nell'ottica della Internet of Things sia per aumentare l'immediatezza e la semplicità dell'interazione;
- "guardare attraverso" per poter avere informazioni anche "oltre" il visibile;
- "gioco con la realtà", un nuovo paradigma di gioco basato sulla realtà aumentata.

Per proseguire con i suddetti obiettivi e per supportare gli scenari applicativi descritti in questo articolo e quelli futuri, Telecom Italia sta portando ARTES in esercizio sulla sua Nuvola Italiana per renderne disponibili componenti/funzionalità sia al proprio interno,sia per le altre piattaforme commerciali aziendali sia direttamente ai clienti, per l'offerta di nuove proposizioni basate sulle funzionalità più avanzate di Realtà Aumentata ■

Figura 12: Aiuto sul prodotto in AR



Acronimi

AR	Augmented Reality o Realta' Aumentata
POI	Point of Interest
ARTES	Augmented Reality Telco Enablers & Services
API	Application Programming Interface
TI	Telecom Italia
B2B2C	Business to Business to Consumer
B2B2B2C	Business to Business to Business to Consumer
MAR	Mobile Augmented Reality
OMA	Open Mobile Alliance
MobAR	Mobile Augmented Reality
SDK	Software Development Kit

Bibliografia

[1] *"2015 weekend nel futuro: viaggio nelle tecnologie che stanno per cambiare la nostra vita"*, Vito Di Bari, Paolo Magrassi, Il Sole 24 Ore, 2005

[2] *"Mobile Augmented Reality 2011-2016"*, Visiongain, 2011.

Urlografia

[3] *http://www.youtube.com/watch?feature=player_embedded&v=QQ8HNXtl7jQ*

[4] *http://www.telecomitalia.com/tit/it/innovation/hot-topics/services/realta_aumentata.html*

[5] *http://se-rm3-7.se.tp-ilabiis.alice.cdn.interbusiness.it/publicmedia/SeeAR.mp4*

[6] *http://www.iot-butler.eu/*

[7] *http://www.expo2015.org/area-stampa/comunicati-stampa/telecom-italia-ed-expo-2015-al-mobile-world-congress-barcellona-presen*

[8] *http://www.mobileworldcongress.com/*

[9] *http://www.metaio.com/*

[10] *http://openmobilealliance.org/*

carmen.criminisi@telecomitalia.it
luca.lamorte@telecomitalia.it
elio.paschetta@telecomitalia.it
nicoletta.salis@telecomitalia.it

Usa il tuo smartphone per visualizzare approfondimenti multimediali

Carmen Criminisi
ingegnere delle Telecomunicazioni è entrata in Azienda nel 2007. Sin dall'inizio ha fatto parte dell'attuale progetto Mobile Social Enablers & Applications, occupandosi inizialmente della definizione di una piattaforma prototipale di Mobile Adversing Context-Aware, per poi passare ad occuparsi della definizione degli enabler di servizio in ambito Social e Realtà Aumentata. Le attività di definizione hanno riguardato principalmente la partecipazione all'attività di normativa nel gruppo di standardizzazione Open Mobile Alliance, in cui ha guidato il gruppo MobAR (Mobile Augmented Reality). Sta contribuendo a diversi progetti di ricerca europei: FI-CONTENT e BUTLER ed è co-autrice di articoli pubblicati in conferenze e riviste.

Luca Lamorte
ingegnere Informatico è in Azienda dal 2003. Si è occupato nel passato di servizi di video-conferenza e applicazioni basati su protocolli SIP e XMPP. Negli ultimi anni si è specializzato nel mondo mobile per passare poi a sviluppare ricerca su Android e sulle tecnologie HTML5. Ha seguito e sviluppato soluzioni innovative nel campo della Realtà Aumentata (SeeAR), dell'Advertising Contestualizzato e ha lavorato su aspetti Social legati alla produzione di contenuti User-Generated. Ha partecipato a diversi progetti europei quali OPUCE, C-CAST ed ora SOCIETIES, allo standard W3C nel gruppo POI-WG. Inoltre con il Politecnico di Torino segue tesi e stage per sviluppi su piattaforme Android.

Elio Paschetta
laureato in Informatica è in Azienda dal 1986. Ha lavorato inizialmente sulle tematiche di Intelligenza Artificiale, applicando le tecniche dei Sistemi Esperti alla diagnosi degli apparati della rete telefonica. In tale ambito ha anche progettato e sviluppato il linguaggio per Sistemi Esperti C-Rule. Ha poi operato nell'ambito dell'Ingegneria del Software sia nel progetto europeo EURESCOM che per la Stima dei Costi di sviluppo software. Ha conseguito anche la certificazione di Function Point Specialist. Ha poi operato nell'ambito della metodologia MCDA (Multiple Criteria Decision Aid) per la valutazione e la scelta di fornitori e prodotti e applicazione al Work Force Management. Negli ultimi anni ha operato, sia come ricerca che come sviluppo lato server e mobile client (.NET e Android) per Context Awareness e in particolare per sistemi di Reasoning e algoritmi e servizi di Recommendation e di Augmented Reality (principalmente Notiziario Tecnico aumentato e Expo 2015).

Nicoletta Salis
ingegnere Elettronico con Master in Telecomunicazioni e certificazione di Project Management Professional del Project Management Institute nel 2011, dal 2000, lavora in Telecom Italia. Si è sempre impegnata, da una parte in diverse attività internazionali (progetti di ricerca IST, collaborazioni bilaterali con le principali aziende del settore ICT, ...), dall'altra nel coordinamento tecnico di gruppi di lavoro che affrontano tematiche innovative sui servizi mobili di telecomunicazione, in primis l'applicazione ad essi della Realtà Aumentata.. Da ottobre 2012 è Project Manager del progetto di realizzazione di Smart City App, il prototipo per i visitatori di Expo 2015 e coordina gli sviluppi e il passaggio all'esercizio della piattaforma ARTES di realtà aumentata di Telecom Italia.

Notiziario Tecnico di Telecom Italia
Anno 22 - Numero 1, Aprile 2013
www.telecomitalia.com/notiziario-tecnico
ISSN 2038-1921

Proprietario ed editore
Gruppo Telecom Italia

Direttore responsabile
Michela Billotti

Direttore tecnico
Oscar Cicchetti

Comitato di direzione
Alessandro Bastoni,
Francesco Cardamone,
Gianfranco Ciccarella,
Sandro Dionisi,
Daniele Franceschini,
Stefano Nocentini,
Roberto Opilio,
Cesare Sironi

Segreteria di redazione
Carla Dulach

Contatti
Corso d'Italia, 41 – 00148 Roma
Tel. 0636882550
notiziariotecnico.redazione@telecomitalia.it

Progetto editoriale
Peliti Associati

Art Director
Mario Peliti

Grafica e impaginazione
Marco Nebiolo

Illustrazioni
Giulia D'Anna

Fotografie
Patrizia Valfrè

A questo numero hanno collaborato
Luigi Artusio
Michele Bellavite
Stefano Brusotti
Gianfranco Ciccarella
Carmen Criminisi
Luciana Costa
Rosalia D'Alessandro
Roberta D'Amico
Paolo De Lutiis
Gabriele Elia
Fulvio Felice Faraci
Marcello Fausti
Luigi Gambardella
Elena Anna Maria Guercio
Luca Lamorte
Carlo Alberto Licciardi
Lucia Longo
Antonio Manzalini
Roberto Minerva
Corrado Moiso
Francesco Nonno
Elio Paschetta
Lorenzo Maria Pupillo
Fabio Renzulli
Daniele Roffinella
Nicoletta Salis
Roberto Saracco
Karen Sollins
Stefano Tagliabue
Mario Ullio
Vinicio Vercellone
Gianluca Zaffiro

Stampa
Tipografia Quintily
Viale Enrico Ortolani, 149/155
00125 Roma

Registrazione
Periodico iscritto al n. 00322/92 del Registro della Stampa
Presso il Tribunale di Roma in data 20 maggio 1992

Chiuso in tipografia
15 aprile 2013

Spedizione in A.P. -45% - art.2 20B Legge 662/96 - Filiale di Roma
ISSN 2038-1921