limes
RIVISTA ITALIANA DI GEOPOLITICA

A CHE SERVONO I SERVIZI

Parte I

il SENSO *dell'*AMERICA *(e dell'*ANGLOSFERA*) per i* DATI

L'ORO NERO DEI DATI

di *Francesco* VITALI

Alleanze e scontri tra le intelligence per la conquista dei big data. *Dallo spionaggio dei leader alla profilatura di massa come metodo predittivo. Il ruolo delle società di telecomunicazioni. Senza un controllo democratico, si avvera la profezia di Orwell.*

1. OGNI CONFLITTO HA SEMPRE COME CAUSA scatenante un bene prezioso per il quale lottare. Ottenere uno strumento per il benessere economico, per lo sviluppo sociale, per il potere e per il suo esercizio nei confronti degli amici e dei nemici. Oggi lo scontro tra le potenze verte su un bene particolare: i dati. Tutte le nazioni avanzate hanno attivato tecnologie e infrastrutture spesso parallele a quelle ufficiali per l'acquisizione, la raffinazione e lo sfruttamento di questo preziosissimo bene primario.

Il nuovo oro nero contemporaneo ha caratteristiche simili e diverse rispetto al petrolio, allo *shale gas*, ai minerali radioattivi, alle terre rare, all'acqua. Per poter trasformare i dati in potere reale sono comunque necessari grandi investimenti e una visione strategica su come utilizzarli al meglio. Il valore intrinseco di questo nuovo bene è così alto da aver scatenato una sorta di caccia sotterranea, in cui i principali eserciti non operano fronteggiandosi all'aperto, ma celati nei principali servizi di intelligence del mondo. I documenti lasciati trapelare da Edward Snowden, pur non svelando particolari eclatanti, offrono comunque elementi e conferme utili per una rilettura di come vengono perseguiti gli interessi nazionali (e quelli particolari) dei pochi gruppi che riescono ad accedere al «vero» potere.

I dati sono una materia prima molto peculiare. Sono ovunque, nelle nazioni ricche e in quelle povere. Sono prodotti da ogni tecnologia moderna e in qualunque tipo di interazione: quando inviamo un'email, premiamo il tasto di un cellulare, apriamo lo sportello di un frigorifero, accendiamo il televisore, acquistiamo un prodotto. Non si esauriscono e sono perfettamente duplicabili e riutilizzabili.

Diversamente dagli altri beni sono al tempo stesso materia prima, semilavorato e prodotto finito. Non sono biodegradabili, ma come un buon vino, invec-

chiando possono acquisire nuove proprietà. E più si incrociano, più acquistano valore. Come nelle formule chimiche, però, non tutti gli aggregati producono la stessa ricchezza: alcune somme di dati possono generare grande conoscenza, altre producono grandi quantità di scarti, o «rumore». Per poter usare i dati, come per il petrolio, è necessario dotarsi di pozzi da cui attingere, condutture e navi per trasportarli, centri per stoccarli e lavorarli, una rete di distribuzione per grossisti e «utilizzatori finali» di quella preziosa conoscenza che, utilizzata in chiave tattica o strategica, genera potere, un immenso potere.

Solo partendo da questo presupposto si può cominciare a comprendere la bulimia digitale che ha colto i servizi di intelligence mondiali e di cui la National Security Agency non è stato altro che il precursore. Le informazioni svelate sino ad ora nell'ambito del Datagate [1] non sono altro che la punta dell'iceberg di quello che già oggi accade intorno a noi.

Sarebbe ingenuo e poco opportuno chiedere alle agenzie di intelligence di non fare il proprio mestiere, ovvero spiare a tutela della sicurezza nazionale. Ha fatto molto discutere in questi mesi il fatto che venissero spiate le comunicazioni della cancelliera tedesca Angela Merkel, dei cardinali papabili, della *presidenta* brasiliana Dilma Rousseff e dell'argentina Cristina Fernández de Kirchner, delle strutture ministeriali che si occupano di gestione delle risorse petrolifere ed energetiche. Difficile immaginare un paese che, indipendentemente dalle convenzioni internazionali, non abbia tra i suoi interessi strategici quello di capire come intendono procedere i leader mondiali su fondamentali questioni politiche ed economiche. Dai documenti di Snowden, però, emerge una realtà ben diversa: i grandi leader possono essere considerati quasi delle vittime collaterali nell'immenso aspirapolvere attivato dai servizi segreti. L'obiettivo è ben più vasto: la popolazione mondiale.

Ovviamente un tipo di raccolta del genere può apparire senza senso se non si chiariscono gli obiettivi dell'intelligence. Occorre dunque tornare agli elementi base: ai dati, ai *big data*, che vengono raccolti e al valore aggiunto, in termini di conoscenza e potere, che rappresentano.

2. Le carte di Snowden raccontano che la National Security Agency (Nsa) statunitense, anche grazie alle infrastrutture messe in piedi dal gruppo Five Eyes (Australia, Canada, Regno Unito, Nuova Zelanda e Stati Uniti) e la collaborazione [2] diretta o forzosa di altre agenzie e società private, raccoglie i metadati [3] delle telefonate su rete fissa e mobile della maggior parte dei paesi del mondo.

1. Vedi ad esempio: G. Greenwald, *No Place to Hide*, London 2014, Hamish Hamilton.
2. Dalle ultime rivelazioni emerge il ruolo inaspettato della Germania, che si caratterizza come la principale base delle operazioni di ascolto dell'Nsa in Europa, con un minimo di 12 centri di raccolta e analisi delle comunicazioni sul proprio territorio. Cfr. «Mein Nachbar NSA», *Der Spiegel*, 16/6/2014 e documenti originali su sito www.spiegel.de
3. Tutte le informazione che descrivono la telefonata, come il numero chiamato e quello chiamante, il luogo, l'orario eccetera. In questo caso i metadati sono raccolti per ragioni tecniche e per la corretta fatturazione del servizio.

L'analisi dei metadati, in particolare di quelli delle reti mobili, consente una sorta di pedinamento dell'utente, spesso molto più efficiente di quello che può essere realizzato da una persona fisica. Tali dati dicono infatti dove ci troviamo, da dove veniamo e dove stiamo andando, con chi stiamo parlando e molto altro. I metadati di un singolo utente diventano molto più interessanti se si incrociano con quelli di altri soggetti e si seguono nella loro evoluzione cronologica. Gli elementi così incrociati consentono di passare da una semplice analisi puntuale del soggetto e delle sue relazioni a una profilazione predittiva [4] dei suoi comportamenti, riuscendo a inferire, anche senza necessariamente ascoltare le sue telefonate, dove sta andando, con chi si incontrerà e per fare cosa: una riunione riservata, una gita in famiglia, una fuga extraconiugale, un crimine. Ovviamente, maggiori sono le informazioni incrociate sul soggetto e sulle persone da cui è circondato, più preciso è il quadro.

Queste informazioni vengono raccolte su tutta la popolazione, tanto che solo il programma Shell'Trumpet nel 2012 elaborava già 2 miliardi di *call events* [5] (presumibilmente il Call detail record che include i dati sia delle telefonate effettuate sia di quelle tentate) al giorno. Quindi, se consideriamo tale numero come riferibile alle telefonate realmente effettuate, possiamo stimare che questo sottogruppo dell'attività dell'Nsa già da solo poteva coprire circa il 60-70% delle chiamate mondiali.

L'Nsa, il Gchq britannico e gli altri servizi, analizzano non solo i tabulati telefonici, ma lo stesso contenuto delle conversazioni. In base alla disponibilità di infrastrutture sul posto o di duplicazione e trasporto di questi dati, le telefonate vengono scandagliate in tempo reale per parole chiave e poi conservate per compiere analisi molto più approfondite. Da una delle brevi presentazioni fatte trapelare da Snowden tramite Glenn Greenwald e integrata da WikiLeaks emerge, ad esempio, che il programma Somalget, attivo dal 2009, prevedeva sin dall'inizio la registrazione e la conservazione per un mese del 100% delle telefonate su rete mobile effettuate in Afghanistan e Bahamas e che la tecnologia e le modalità usate in quel programma si sarebbero potute tranquillamente replicare in altre nazioni.

Non è dato sapere se questi due paesi siano solo una frazione delle decine di Stati in cui già avveniva questo tipo di registrazione in massa – magari sotto altri nomi – o se siano stati usati dall'Nsa solo come test, in attesa di incremen-

4. F. Vitali, «La geopolitica economica dei dati e il futuro del dominio», *Nomos&Khaos*, Rapporto Nomisma 2011-12 sulle prospettive economico-strategiche – Osservatorio scenari strategici e di sicurezza, 2012, pp. 207-231.

5. Non è facile stimare con precisione la capacità dei singoli programmi dell'Nsa dai pochi documenti sinora pubblicati, soprattutto perché la terminologia utilizzata, essendo tecnicamente ambigua (le traduzioni in italiano tra l'altro sono quasi tutte sbagliate), si può prestare a molteplici interpretazioni. A volte, non è chiaro se un «evento» si riferisca a una singola chiamata o anche alle chiamate tentate, e se i metadati di una telefonata (di solito il Call detail record, Cdr) vadano conteggiati come un singolo evento oppure considerati separatamente in base alle specifiche informazioni trasmesse, come l'orario della telefonata, l'Imsi (International mobile subscriber identifier) o il Vlr (Visitor location register).

tare le capacità di conservazione ed elaborazione. Capacità tecnologiche poi acquisite dagli americani con il completamento del nuovo megacentro informatico di Bluffdale, nel deserto dello Utah, che dispone di infrastrutture grandi almeno sette volte quelle del Pentagono e capacità computazionali assolutamente insondabili, vista anche l'introduzione dei nuovi computer quantici (anche se è ancora in corso una disputa tra scienziati sul fatto che le macchine oggi a disposizione, almeno quelle di tipo commerciale, possano essere veramente classificate come tali).

Molti altri programmi dell'Nsa di cui si conosceva l'esistenza, ma spesso non il nome, sono dedicati al ben più interessante monitoraggio del traffico Ip che gli utenti di Internet effettuano con computer tradizionali o apparati mobili (smartphone, tablet e orologi intelligenti), come XKeyscore. Dai documenti sul programma Rampart-A emerge che 33 Stati [6], tra cui l'Italia e altri 16 membri dell'Unione Europea, concedono all'Nsa accesso diretto alle infrastrutture di comunicazione in fibra ottica presenti sul proprio territorio. Anche nei paesi in via di sviluppo gran parte della vita reale si è infatti duplicata o trasferita *online*: dai contatti tra amici e professionisti alle passioni politiche o sessuali, dalle condizioni di salute allo stato psicologico di ogni utente. Fino a pochi anni fa, per conoscere le condizioni di salute di un importante personaggio politico era necessario corrompere informatori e medici, oppure prelevare campioni biologici del soggetto. Sono famosi i water chimici trasportati dai capi di Stato durante la guerra fredda per non rischiare di lasciare informazioni preziose al nemico. Ora, per ottenere impronte digitali e fotografie di un leader, appuntamenti e documenti riservati, informazioni sulla sua salute o sulle sue abitudini e sulle sue perversioni, sul suo umore e sui suoi amori, sulle sue letture e su ogni altro aspetto della sua vita, la via più semplice, economica ed efficiente è quella di accedere al suo smartphone, tablet o computer.

3. I documenti fuoriusciti dall'Nsa evidenziano con grande efficacia il ruolo determinante giocato dalle principali società di telecomunicazioni e dai fornitori americani di servizi *online* e non solo, in un mercato in cui l'unica mano invisibile non è quella immaginata da Adam Smith, ma quella dell'Agenzia per eccellenza. Acquisire i contenuti delle telefonate mondiali, infatti, non è un compito alla portata di tutti e richiede quasi sempre la collaborazione volontaria (ben remunerata) o imposta (in genere dalla normativa sulla sicurezza nazionale) delle società del settore. Per controllare le comunicazioni internazionali è sufficiente accedere ai cavi in fibra ottica dei principali *carriers* internazionali (sono poco più delle dita di una mano, con una forte crescita del gruppo indiano Tata e un calo del gruppo americano Verizon) per coprire la quasi totalità delle chiamate. Anche l'Italia, essendo attraversata da cavi di interesse stra-

6. R. GALLAGHER, «How Secret Partners Expand NSA's Surveillance Dragnet», *The Intercept*, 18/6/2014.

tegico, è al centro di questa disputa. Ne è un esempio la notizia (forse una polpetta avvelenata fatta pubblicare a titolo di avvertimento da 007 concorrenti) sulle «nuove sonde» [7] installate a Palermo per spiare tutto il traffico voce e dati che passa sulla dorsale internazionale Sea-Me-We 4.

Per il traffico nazionale la situazione è più complessa e dipende da come è impostata l'infrastruttura di ogni paese. Se non è centralizzata, occorre accedere alle principali centrali di transito che gestiscono il traffico telefonico e poi trasmettere all'esterno il traffico duplicato. Molto più semplice è registrare il traffico mobile in aree di maggiore interesse, come è stato fatto su Roma e Milano. Tra l'altro, i dati di raccolta delle telefonate sono ben diversi da quelli ufficiali, legati prevalentemente ad attività della magistratura, che sono forniti ad esempio da Vodafone nel suo *Law Enforcement Disclosure Report* pubblicato nel giugno 2014. La società telefonica ha però confermato che alcuni governi accedono direttamente alla sua rete per ascoltare e duplicare le telefonate di interesse.

La raccolta dei metadati delle telefonate non richiede infrastrutture particolari. I tabulati e le altre informazioni sono quasi tutti centralizzati nei sistemi di fatturazione delle compagnie telefoniche e il loro peso è assai più basso rispetto alla parte voce di una comunicazione. Anche il traffico dati su Internet – dalla navigazione alle email, alle telefonate Voip (il 20% delle comunicazioni mondiali passa in questa forma) – è molto semplice da intercettare per il gruppo dei Five Eyes. Il sistema di indirizzamento delle comunicazioni, infatti, è costruito in maniera tale da far transitare la maggior parte dei pacchetti di traffico negli Stati Uniti, anche se si spedisce un'email da Roma a Bologna. L'apposito programma di intercettazione globale XKeyscore funziona perfettamente a modo di superaspirapolvere. Non tutte le comunicazioni sono però coperte da questi sistemi, così si interviene a coprire i vuoti di traffico direttamente dai dispositivi degli utenti, magari sfruttando bachi (falle) [8] hardware e software (spesso fatti installare appositamente) di server, router o pc. Ne è un esempio Cisco, leader mondiale del settore, che nonostante i ricchi interessi convergenti con i servizi di intelligence, di fronte alle rivelazioni ha comunque protestato per l'invadenza dei servizi americani.

Hanno pianto lacrime di coccodrillo anche tutte le maggiori società che offrono servizi tramite Internet, come Google e Facebook, Apple e Microsoft, Amazon e Twitter, i produttori di sistemi operativi e di applicazioni. Queste società, tra l'altro, dispongono di dati particolarmente interessanti per le attività di intelligence: dato che gran parte del loro business si basa proprio sulla profilazione dei loro utenti, dispongono di moltissime informazioni già elaborate e

7. Secondo l'articolo, la strumentazione di spionaggio sarebbe stata installata presso lo *hub* gestito da Telecom Italia Sparkle su richiesta di un'importante società americana. Vedi «Esclusivo. Nuove sonde siciliane "spiano" Europa e M.O.», *SiciliaInformazioni*, 7/11/2013; cfr. anche P. CHATTERJEE, «Glimmerglass Taps Undersea Cables for Spy Agencies», *Ipsnews*, 22/8/2013.

8. Vedi il caso di *Heartbleed*, tenuto celato per anni dai servizi segreti, per aggirare senza sforzi le protezioni di OpenSSL.

«pronte all'uso». Vengono così enormemente ridotti gli sforzi che i servizi devono fare *ex post* per estrarre conoscenza puntuale e strategica da quei dati, magari per ricattare un personaggio scomodo o per capire lo sviluppo politico di un'intera nazione.

In questo gioco di specchi per il controllo e la gestione delle tecnologie che utilizziamo ogni giorno, consapevolmente o inconsapevolmente, non stupisce la campagna che il governo americano ha intrapreso da alcuni anni contro l'adozione di servizi e prodotti offerti dai colossi cinesi delle telecomunicazioni Huawei e Zte – tra i primi cinque fornitori al mondo, Europa inclusa, in quasi tutti i settori delle telecomunicazioni e dei dispositivi elettronici – con l'accusa di essere un potenziale strumento di spionaggio. È infatti spiacevole far sostituire il proprio cavallo di Troia, tra l'altro ben pagato dagli acquirenti, con quello di un paese antagonista.

La competizione per la conquista dei dati si gioca anche a livello normativo e commerciale, magari attraverso i trattati di libero scambio, come il Ttip (Transatlantic Trade and Investment Partnership), in fase di gestazione. Proprio per questo, l'approvazione della nuova normativa europea in materia di protezione dati (in particolare il regolamento oggetto di recepimento automatico nella legislazione nazionale di tutti i paesi Ue), che avrebbe creato qualche problema – per lo meno formale – alla raccolta dei dati europei, è stata bloccata da Washington e da alcuni governi dell'Unione attraverso una formidabile azione di lobbying. La strategia *divide et impera* messa in atto dalle società e dal governo statunitense ha avuto successo. Il regolamento e la direttiva, per motivi differenti, avrebbero scontentato anche altri governi europei, non ultimo quello tedesco, che continua a negoziare senza successo con gli Stati Uniti un accordo bilaterale in materia di intelligence.

4. Se questa raccolta di dati fosse tutta indirizzata alla lotta al terrorismo e al crimine in generale, ci si aspetterebbe di non trovare più alcun cattivo in libertà. Se non già da ora (considerati gli sviluppi tecnologici), entro un paio d'anni non dovrebbero esserci quasi più né riciclaggio, né corruzione. Dovrebbe scomparire qualunque traffico illecito internazionale, dalle armi alla droga, e le attività terroristiche dovrebbero essere limitate a territori dove esistono aree abbastanza grandi per nascondersi in caverne isolate dal mondo. Se, al contrario, entro un paio d'anni non dovesse succedere nulla di tutto ciò, allora dovremmo cominciare a preoccuparci, perché a perdere non sarebbe il crimine, ma la libertà di noi tutti.

Questa dissonanza tra capacità spionistiche e obiettivi raggiunti contro il malaffare non dipende da un problema tecnologico, ma dal fattore umano. Il primo aspetto da considerare è di tipo tecnico: ci può essere tutta la scienza e la tecnologia che si vuole, ma alla fine – almeno per il momento – le decisioni finali restano appannaggio di esseri umani, i rapporti sono letti da esseri umani, le correlazioni evidenziate sono analizzate da esseri umani. Si crea quindi un collo di bottiglia, anche nel settore dell'intelligence e a livello governativo, che riduce

molto l'utilità dei dati raccolti. Non dimentichiamo che, da un punto di vista cognitivo, ogni essere umano è in grado di valutare correttamente non più di 7-9 opzioni contemporaneamente [9].

Il secondo aspetto, ancor più interessante, riguarda il non allineamento tra obiettivi strategici dichiarati e reali. Una raccolta massiccia di informazioni, infatti, è poco utile (o utilizzata) per catturare i cattivi della terra; viceversa, è utilissima ai fini della manipolazione strategica di tipo politico, economico e sociale, a un livello molto superiore rispetto alle *infowars* [10] che abbiamo conosciuto sinora. L'aspirapolvere orwelliano si rivela quindi fondamentale per programmi puntuali di Sigdev (Signals development) avanzati, come Squeaky Dolphin [11] sviluppato dal Gchq britannico, oppure per una delle tante iniziative della Darpa (Defense Advanced Research Projects Agency) americana, come il Social Media in Strategic Communication Programme, avviato nel 2011 in contemporanea alle primavere arabe per finanziare progetti «rivoluzionari» nel campo della comunicazione strategica sui social network con l'obiettivo di «creare e prevenire eventi inattesi in campo strategico».

A un enorme potere, come quello dell'Nsa e di tutte le agenzie sorelle, deve corrispondere un analogo controllo democratico; a tal fine, deve esserci un pari livello di trasparenza, almeno sugli obiettivi tattici e strategici e sulle modalità operative adottate. Questo banale principio vale anche per tutti quei centri che, per la legittima e necessaria attività di difesa dello Stato, fanno del segreto la loro principale modalità d'azione. Se vogliamo che la punta dell'iceberg svelata da Snowden non esca dai confini di una lieve paranoia per trasformarsi in una vera piovra mondiale, totalmente autonoma e senza più alcun indispensabile bilanciamento con gli altri diritti fondamentali, è necessario attuare subito alcune riforme in questo senso.

Qui i buoni propositi di Obama sono ancora rimasti sulla carta. E l'accondiscendente comitato di controllo senatoriale sull'intelligence (Fisa, Foreign Intelligence Surveillance Court), che da fedele passacarte non ha mai bloccato una richiesta di raccolta dati, ha dovuto subire anche l'umiliazione di veder violare i propri computer dalla Cia, intervenuta di nascosto per cancellare report scomodi sul proprio operato.

Anche l'Italia ha le sue ombre: nessuno ad esempio ha ancora spiegato a chi sono serviti i 300 mila accessi alle banche dati strategiche nazionali, anche private, effettuati (apparentemente per combattere il crimine informatico) nei primi sei mesi del 2013. Nessuno ha approfondito il dato incredibile (ma per il motivo opposto) fornito al Copasir dal procuratore generale della Corte d'appello di Roma, che nel corso del 2013 avrebbe ricevuto per competenza e autorizzato ai servizi soltanto 12 intercettazioni preventive. Forse questa cifra non

9. S. Bagnara, *L'attenzione*, Bologna 1984, il Mulino.
10. F. Vitali, «Infowar, la conquista dell'anima», *Limes*, «Progetto Jihad», 1-2004, pp. 105-115.
11. G. Greenwald, «How Covert Agents Infiltrate the Internet to Manipulate, Deceive, and Destroy Reputations», *The Intercept*, 24/2/2014.

è stata comunicata con esattezza al pubblico, ma è ovvio che con una quantità di intercettazioni così limitata non si stana neppure il ras di un mercato rionale di frutta e verdura di una grande città.

Si esce così dalla geopolitica per entrare nella farsa. O le leggi attuali sono «troppo strette» per le necessità degli 007 mondiali, o sono gli 007 «troppo abbondanti» per le attuali leggi nazionali. Questo aspetto, con gli altri, merita un'approfondita riflessione.

APPENDICE

Come si fa un'intercettazione

di *Danilo Benedetti*

Durante il 2013 sono stati scambiati, nel mondo, circa 520 miliardi di minuti di conversazioni telefoniche: il 20% su Voip (Voice over IP, cioè via Internet), il resto con tecnologia «tradizionale» Tdm (*grafico 1*).

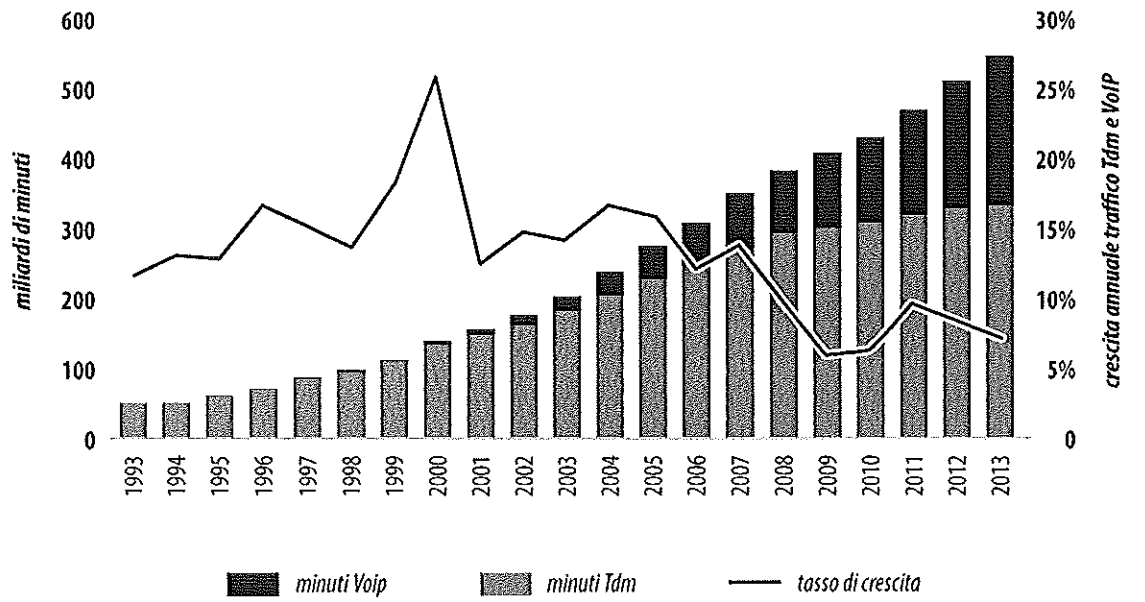
Le mappe che descrivono i flussi di traffico fra i paesi misurano abbastanza fedelmente questi fenomeni, con un'avvertenza: la quantità di banda consumata dai differenti servizi varia enormemente, ma non è un buon indicatore del valore economico del traffico scambiato. Si pensi ad esempio a una telefonata internazionale tra l'Italia e gli Stati Uniti, che occupa pochi Kb/s (kilobit per secondo), ma che ha un costo di decine di centesimi al minuto, rispetto allo *streaming* gratuito di un video su YouTube in alta qualità, che può impegnare centinaia di Kb/s senza però necessitare di un pagamento «diretto».

Le principali direttrici internazionali del traffico telefonico coinvolgono gli scambi fra Asia, Stati Uniti ed Europa, mentre America Latina e Africa sono direttrici meno ricche, anche se questo dato è destinato a evolvere rapidamente.

I principali cavi sottomarini

Oltre il 99% del traffico dati e voce scambiato nel mondo viaggia su cavi in fibra, mentre l'1% rimanente è affidato ai satelliti. La *carta 1* mostra il percorso dei principali cavi di telecomunicazione attivi nel mondo. È evidente come i loro tracciati ricalchino le principali direttrici di traffico: le direttrici meglio servite sono quelle che legano Stati Uniti, Europa e Asia – in particolare Cina e Giappone. Negli ultimi anni, però, sono entrati in servizio anche numerosi cavi che raggiungono i territori africani affacciati sull'Atlantico. Questo trend è in decisa crescita, come mostra la *carta 2*, che evidenzia i soli cavi attualmente in fase di realizzazione.

Grafico 1 - CRESCITA DEL TRAFFICO TELEFONICO INTERNAZIONALE



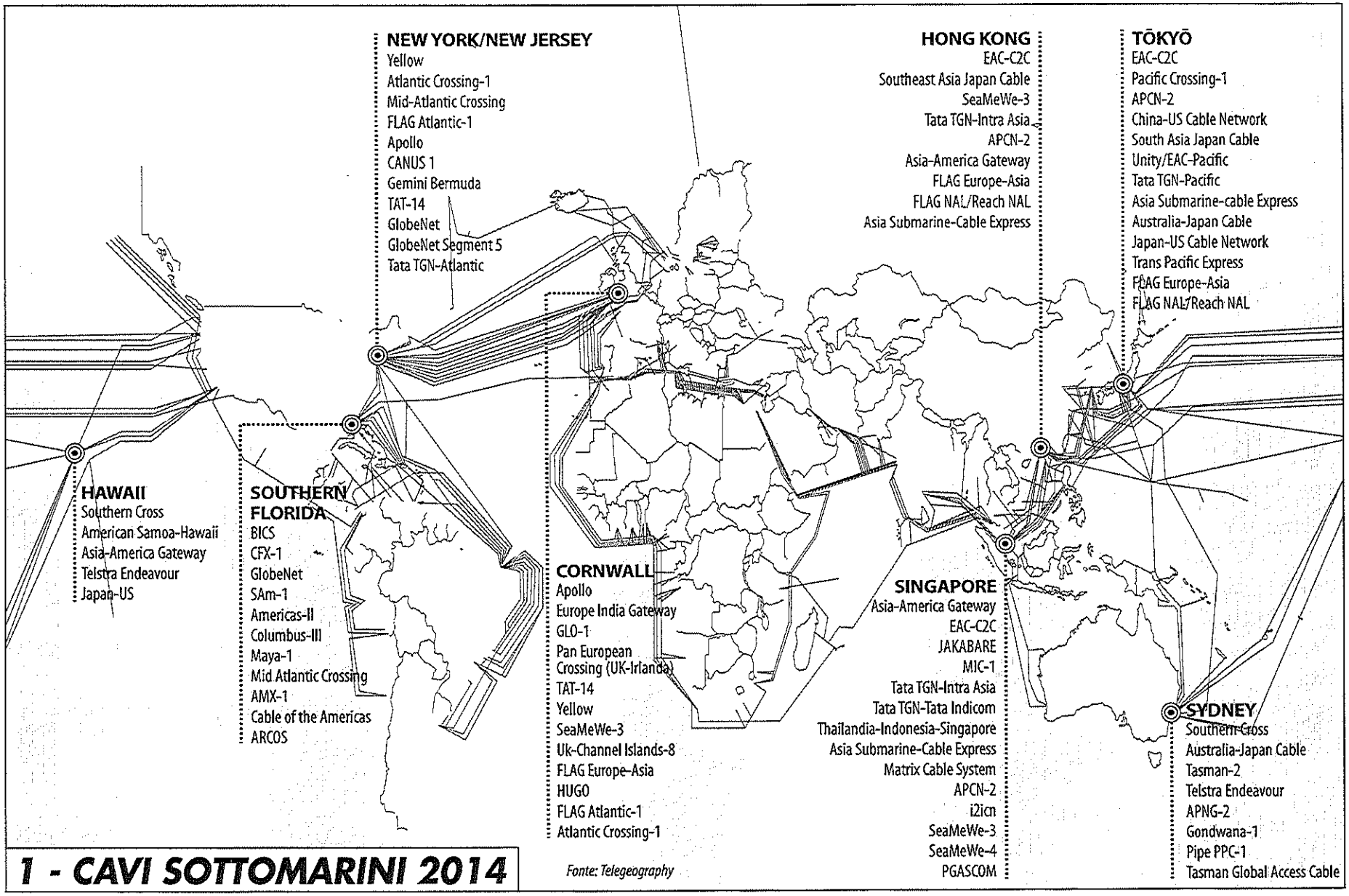
Fonte: Telegeography

La posa di cavi sottomarini è effettuata principalmente da consorzi di operatori telefonici, i quali poi divengono proprietari di una parte della capacità di trasmissione del cavo stesso, per usarla in modo diretto o per rivenderla ad altri operatori. In tali consorzi cominciano ad apparire i nomi di Facebook (Asia-Pacific Gateway – Apg) e Google (Southeast Asia-Japan Cable – Sjc), i quali hanno un interesse evidente nel «rompere» il monopolio dei *carriers* sul traffico dati, specialmente nei collegamenti diretti verso i più promettenti mercati del Sud-Est asiatico. Qui infatti si registra negli ultimi anni una crescita esplosiva del traffico Internet, in special modo cinese, come evidenziato dal *grafico 2.*

È difficile parlare di «cavi principali» per due motivi: le direzioni maggiormente servite sono sempre coperte da più di un cavo e, per ragioni di ridondanza, il traffico telefonico di ciascun *carrier* è di solito affidato a più cavi diversi. Per quanto riguarda i cavi che interessano l'Italia, i principali sono:

• SE-ME-WE 3, da 960 Gbps (gigabit al secondo), uno dei più lunghi cavi in uso, collega Mazara del Vallo con innumerevoli paesi del Nord Europa, del Medio Oriente e del Sud-Est asiatico. Il suo completamento, nel 2000, è stato reso possibile da un accordo fra 92 diversi operatori (*carta 3*).

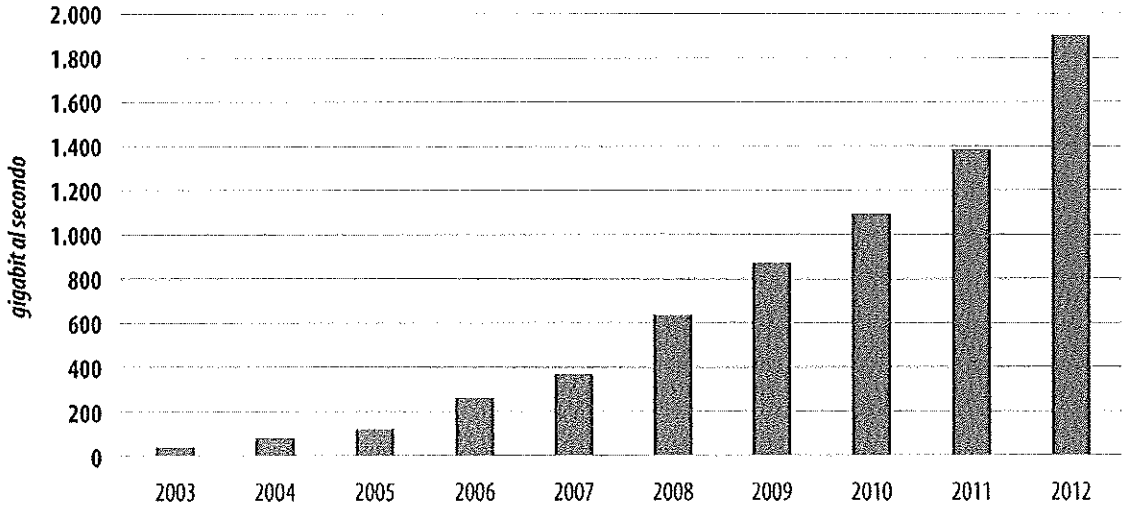
• MedNautilus, da 3,8 Tbps (terabit al secondo), in servizio dal 2001, collega Catania con Grecia, Turchia, Israele e Cipro. Di proprietà di Telecom Italia, sino al 2012 garantiva un sostanziale monopolio delle telecomunicazioni da e per Israele. Questo cavo ha espanso la capacità del precedente LEV, da 20 Gbps, in servizio dal 1999.



1 - CAVI SOTTOMARINI 2014

Fonte: Telegeography

Grafico 2 - LA CRESCITA DI INTERNET IN CINA



Fonte: Terabit Consulting

• SE-ME-WE-4, da 1,28 Tbps, che collega Palermo con numerosi paesi del Mediterraneo, del Medio Oriente e del Sud-Est asiatico. Il cavo è stato realizzato ed è tutt'ora gestito da 16 operatori, tra i quali figura Telecom Italia Sparkle (*carta 4*).

• I-ME-WE, da 3,8 Tbps, che collega Catania con Marsiglia, Egitto, Emirati Arabi Uniti, Libano, Pakistan e India. È stato completato nel 2011 da un consorzio di 9 aziende: BhartiAirtel (India), Etisalat (Eau), France Telecom (Francia), Ogero (Libano), Ptcl (Pakistan), Stc (Arabia Saudita), Telecom Egypt (Egitto), Telecom Italia Sparkle (Italia), Tata Communications (India) (*carta 5*).

La tecnologia e la competenza per il progetto e la realizzazione di cavi sottomarini di lunga distanza costituiscono una formidabile barriera all'ingresso per nuovi attori economici, favorendo la struttura di oligopolio che caratterizza questo mercato. Come mostra il *grafico 3*, quasi metà del mercato è coperto dalla franco-americana Alcatel-Lucent, seguita dalla statunitense TE SubCom e dalla giapponese Nec. Normalmente, il cavo posato è gestito finanziariamente dal consorzio che lo ha costituito, attraverso un'apposita struttura. Gli interventi fisici sul cavo, siano essi dovuti a rotture o a necessità di *upgrade* della capacità, sono normalmente demandati alle aziende che li hanno posati. La forte percentuale di investimenti non-telco (22% nel periodo 1987-2012) nasce dalla bolla di Internet di fine anni Novanta. Se si limita la fotografia agli ultimi cinque anni (2008-12), la percentuale di cavi finanziati da operatori di telecomunicazioni o loro consorzi sale all'80%.

2 - CAVI SOTTOMARINI IN FASE DI REALIZZAZIONE

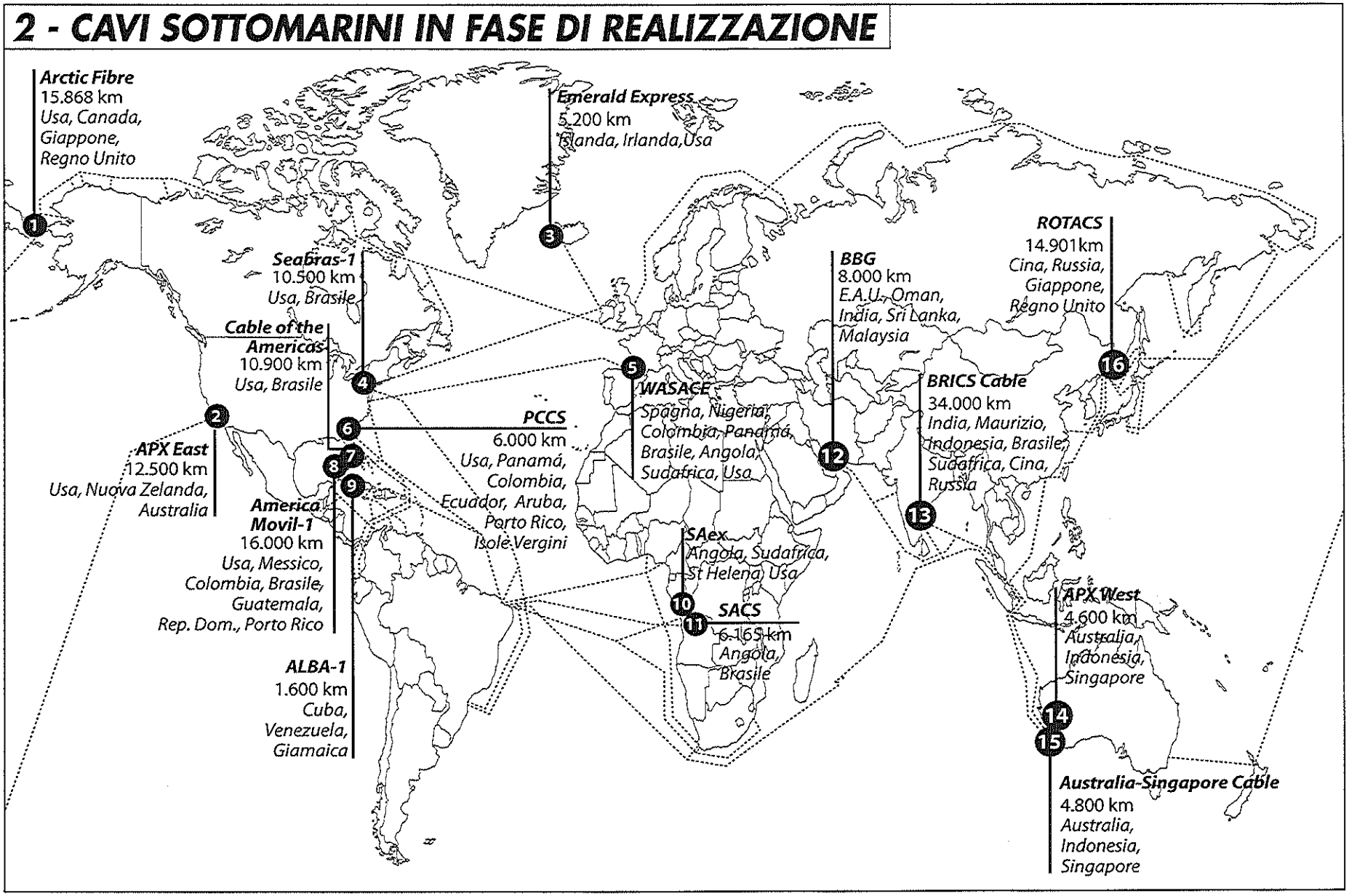
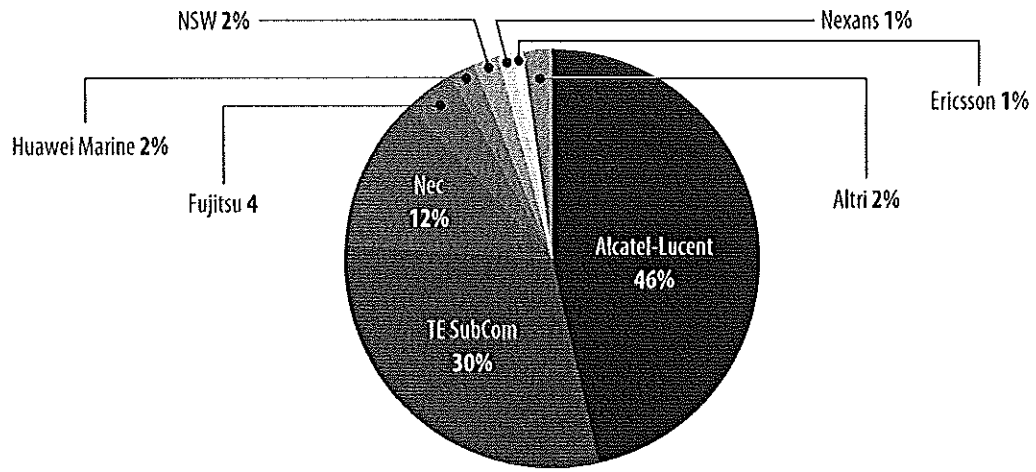


Grafico 3 - MARKET SHARE DELLA REALIZZAZIONE E GESTIONE CAVI



Fonte: Terabit Consulting

I carriers *principali e il funzionamento delle reti*

Gli ultimi anni hanno visto l'enorme crescita di Tata Telecom, che raccoglie e distribuisce il traffico internazionale generato primariamente da Sud-Est asiatico e Medio Oriente. A fronte di ciò, gli operatori europei (Bics/Belgacom, Kpn, France Telecom, Deutsche Telecom e Telecom Italia) occupano una posizione ancora forte *(grafico 4)*. Oltre a essere normalmente presenti nei consorzi che guidano la progettazione, la realizzazione e la gestione dei cavi sottomarini, le società internazionali di telecomunicazioni gestiscono anche gli apparati presenti nei *landing-points* dei cavi. Nel caso di programmi di intercettazione massiccia (quale, ad esempio, il programma inglese Tempora), la *Süddeutsche Zeitung* ha riportato i nomi delle società di tlc coinvolte: Bt, Global Crossing, Interoute, Level 3, Viatel, Verizon Business e Vodafone Cable.

Ma come funziona una rete di telecomunicazioni e che implicazioni ha per l'intercettazione? Le reti sono costruite ad albero, dove le foglie sono gli utenti (o meglio, i singoli telefoni connessi alla rete) e a ogni biforcazione dei rami siede un apparato di *switching*, in grado di indirizzare la chiamata.

Questo schema è applicabile sia alle reti fisse che a quelle mobili, anche se talora i livelli gerarchici possono essere superiori a due. Per il principio di economicità, si cerca ove possibile di non far «salire» il traffico verso le centrali di livello gerarchico superiore, per non impegnare risorse costose (i cavi fra centrale e centrale, le risorse computazionali di ciascuna centrale attraversata). In pratica, ogni chiamata sale fino al livello gerarchico che ha entrambi i telefoni (chiamato, chiamante) fra le sue foglie. Nelle infrastrutture nazionali non esiste di solito un «supernodo» gerarchico; piuttosto, le centrali di livello gerarchico più alto sono

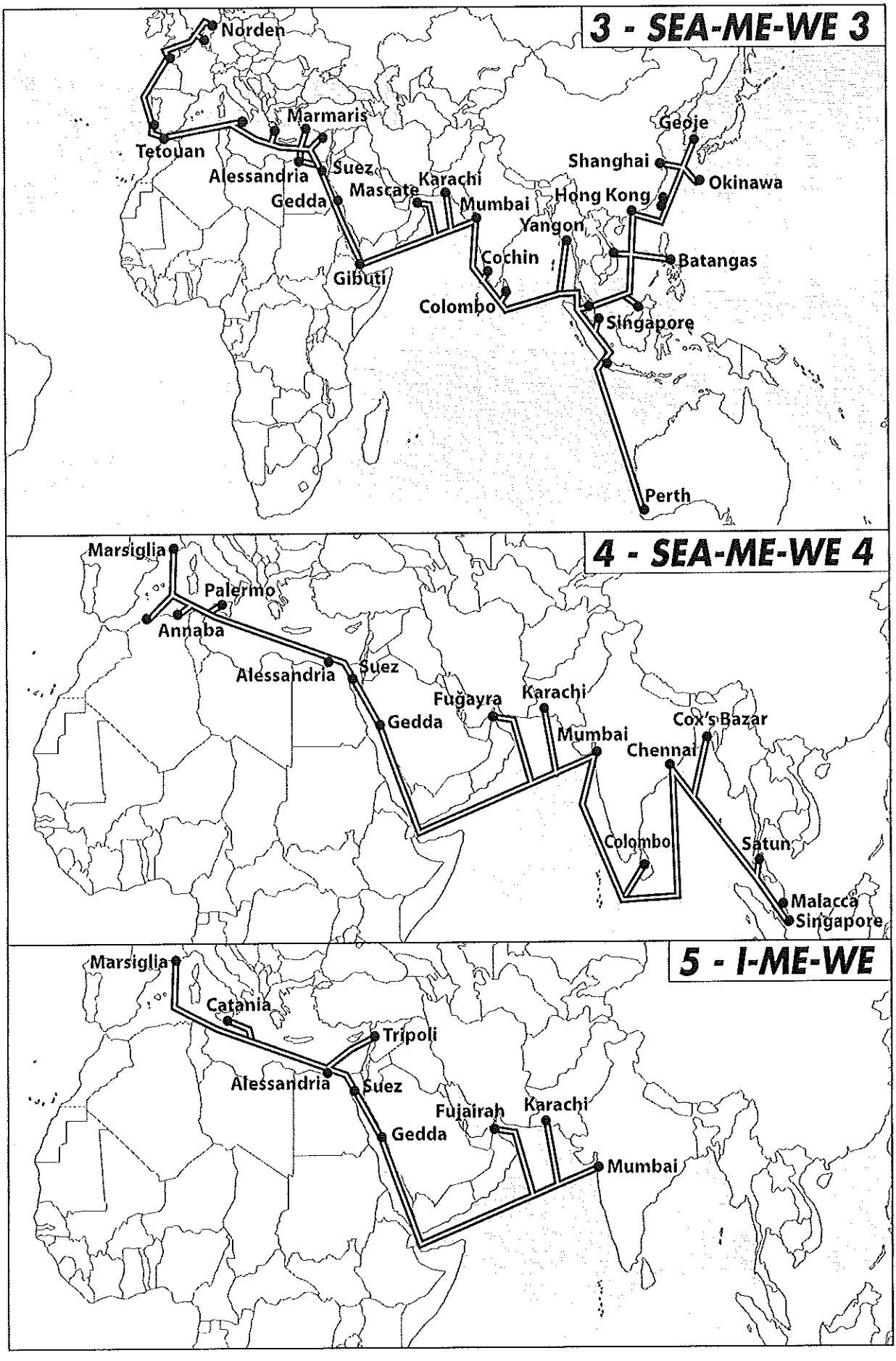
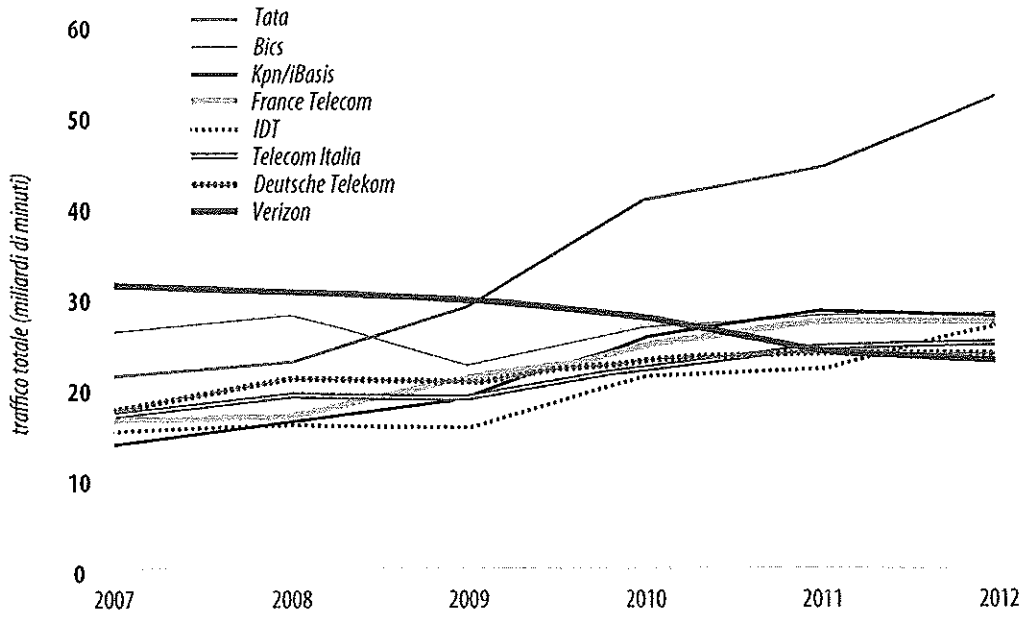

3 - SEA-ME-WE 3
Norden
Marmaris
Tetouan
Alessandria
Suez
Gedda
Mascate
Karachi
Mumbai
Yangon
Cochin
Colombo
Gibuti
Geoje
Shanghai
Okinawa
Hong Kong
Batangas
Singapore
Perth
4 - SEA-ME-WE 4
Marsiglia
Palermo
Annaba
Alessandria
Suez
Gedda
Fuğayra
Karachi
Mumbai
Chennai
Cox's Bazar
Colombo
Satun
Malacca
Singapore
5 - I-ME-WE
Marsiglia
Catania
Tripoli
Alessandria
Suez
Gedda
Fujairah
Karachi
Mumbai

Grafico 4 - TRAFFICO INTERNAZIONALE GESTITO DAI PRINCIPALI CARRIER



Fonte: Telegeography

direttamente connesse tra loro. Tale architettura è replicata da ciascuno dei principali operatori telefonici (fissi e mobili) di un paese.

I tipi di intercettazione

Quando si parla di intercettare le comunicazioni, nel campo del traffico voce ci si riferisce a due diverse possibilità: l'intercettazione, ascolto e memorizzazione delle conversazioni telefoniche; oppure la raccolta dei cosiddetti metadati telefonici, in gergo tecnico noti come Cdr (Call detail record). Il Cdr è normalmente utilizzato dalle compagnie telefoniche per effettuare la tariffazione, in quanto contiene i numeri telefonici del chiamato e del chiamante, l'ora della chiamata e la sua durata. L'accesso ai soli Cdr permette di sapere chi chiama chi e quando, ma non contiene alcuna informazione utile a risalire al contenuto della conversazione.

Il primo tipo di intercettazione è di norma eseguito su richiesta della magistratura e su determinate utenze telefoniche. Un'attività di intercettazione massiccia richiede l'accesso alle centrali telefoniche di tutti gli operatori per deviare il traffico verso il sistema intercettante. Tale attività necessita inoltre di enormi quantità di memoria di massa, per immagazzinare le conversazioni registrate. L'attività è semplificata in quei paesi in cui il traffico telefonico attraversa una singola centrale telefonica nazionale.

L'intercettazione dei Cdr è tecnicamente più semplice, perché i metadati sono di solito raccolti in un punto centrale direttamente dall'operatore telefonico. Inoltre, il volume di dati trattato è considerevolmente minore rispetto al caso della raccolta di intere conversazioni. Ovviamente, in un paese con più operatori è necessario raccogliere i Cdr di tutte le compagnie telefoniche.

L'intercettazione massiccia come quella attribuita ai programmi Tempora del Gchq britannico o Xkeyscore della statunitense Nsa – di norma illegale nei paesi in cui viene effettuata – richiede l'installazione di sonde, o comunque l'esecuzione di una copia del traffico (come la soluzione *CyberSweep* offerta dall'americana CyberGlass). I punti più indicati per questo tipo di attività sono quelli di concentrazione del traffico, in particolare i *landingpoints* dei cavi sottomarini. Si tratta di un insieme relativamente limitato di punti nevralgici, da cui transita la maggior parte delle comunicazioni internazionali, sia dati sia voce (tradizionale e Voip).