Autore: Raoul Chiesa - *Settembre 1999*

Le Reti di Controllo Globale: un'analisi approfondita dei casi Echelon ed Enfopol in una visione a 360°

"Nel 1997, prima del rapporto STOA, una ricerca del termine Echelon su Internet riportava meno di una decina di risultati. Oggi, nel settembre del 1999, quella stessa ricerca riporta 60.740 pagine Web. La gente vuole capire come Echelon viene usata e cosa dice quel rapporto."
(Raoul Chiesa)

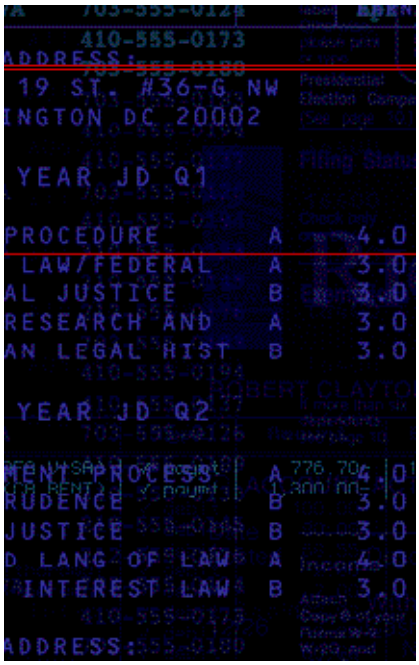
Abstract:
Sette brevi percorsi di lettura uniti da un argomento comune, per capire le nuove problematiche di sorveglianza globale: ogni settimana un approfondimento sui singoli argomenti, sui singoli punti chiave che compongono un mosaico chiamato "Controllo Globale". Una visione "diversa e nuova" da parte di un hacker che oggi protegge le reti, ma anche una visione da parte di un cittadino della ***Comunità Europea*** che vorrebbe dire "no" a tante cose.

Autore: Raoul Chiesa - *Settembre 1999*

Le Reti di Controllo Globale: un'analisi approfondita dei casi Echelon ed Enfopol in una visione a 360° - Premessa

1. Premessa

Un ringraziamento particolare per aver contribuito - con informazioni, racconti, aneddoti e spiegazioni in una forma personale ed amichevole - alla stesura di questo articolo va a Steve Wright e a Simon Davies:
il primo è direttore della ***Omega Foundation*** di Manchester ed autore del rapporto STOA (1)1998 per il Parlamento Europeo intitolato "An Appraisal of the Technologies of Political Control (Una valutazione sulle tecnologie di controllo politico), dopo il quale si è iniziato a parlare anche tra "la gente comune" del caso Echelon;
il Dr. Simon Davies lavora al Computer Security Research Center della London School of Economics a Londra ed è fondatore del gruppo di osservazione ***Privacy International***. Senza le spiegazioni, le opinioni e le testimonianze di queste due persone questa storia non si sarebbe potuta raccontare.



(1) STOA: Scientific and Technologies Options Panel of the European Parliament

Autore: Raoul Chiesa - *Settembre 1999*

Le Reti di Controllo Globale: un'analisi approfondita dei casi Echelon ed Enfopol in una visione a 360° - Introduzione: Sorveglianza Globale

2. Introduzione
Sorveglianza globale

.... intercettazioni telefoniche, microspie, telecamere, sniffing, hacking, per arrivare sino ad agenti segreti e controspionaggio, sono termini ai quali siamo oramai abituati o ci stiamo abituando; esiste però un altro termine, un po' inquietante, del quale talune persone sono a conoscenza, altre hanno sentito parlare capendone poco, ed altre ancora - la maggior parte - non sanno assolutamente nulla.

La stampa cartacea, quella "ufficiale", ha iniziato a parlarne in Italia il 20 marzo 1998 quando il settimanale "il Mondo" dedicò un primo "speciale" dal titolo eclatante: "Licenza di spiare, i segreti di Echelon: così USA e Gran Bretagna ci spiano". Si riferiva al caso Echelon, alla scoperta ufficiale della sua esistenza.
Seguì una seconda uscita nel numero successivo (2), poi una terza(3) .....poi le prime timide interrogazioni parlamentari da parte di alcuni degli eurodeputati italiani di stanza a Bruxelles. Romano Carratelli, deputato del Partito Popolare (lo stesso del Ministro della Difesa, Beniamino Andreatta) il primo aprile 1998 ha presentato a Prodi un'interrogazione parlamentare in cui chiede di sapere "se il governo italiano è a conoscenza del sistema Echelon e se l'Italia è coinvolta in questa vicenda e quali iniziative sono state intraprese o si intende intraprendere per garantire la sicurezza del Paese e dei suoi cittadini". Prodi il 24 aprile dello stesso anno, quando era Presidente del Consiglio, durante una seduta parlamentare, dichiara di non sapere nulla riguardo ad Echelon, aggiungendo che un sistema di controllo sistematico delle telecomunicazioni risultava essere, secondo lui, poco credibile e non realizzabile.
In altri paesi europei accadeva più o meno lo stesso: The Guardian Online, il Tribune e il Sunday Times in Inghilterra, Liberation in Francia con uno speciale di 4 pagine, De Groen in Olanda, il New York Times nella sua rubrica Cybertimes, persino il Giappone, con due articoli il 19 settembre 1998 ed il 10 gennaio 1999 su Mainichi Shimbun, tutti insomma pubblicano interrogativi sul caso.
Ed è forse un caso il fatto che tutti questi articoli siano stati pubblicati dopo l'uscita di un film quale "Nemico Pubblico" (4)? Era proprio necessario un ***film*** per esporre il problema a tutti e suscitare finalmente l'interesse dei mass-media ?

Analizzando il rapporto STOA, risultava spontaneo porsi delle domande sul ruolo dell'accoppiata NSA(5) /CIA (6) americana e del GCHQ(7)inglese. Ma nessuno lo fece...e chi tentò di farlo (esemplare la battaglia condotta da "Il Mondo"), arrivando al punto di riuscire a far sì che la commissaria europea Emma Bonino e la Commissione Europea si rivolgessero alla Gran Bretagna per chiedere una conferma o una smentita, chi ci ha provato è rimasto solo con il gelido silenzio del governo inglese. Tutte denuncie passate inosservate.

La seconda tornata dei mass-media gridò successivamente ad una "rivincita", "Enfopol: la risposta europea ad Echelon.". Tra parentesi sbagliandosi - e di molto, come vedremo in seguito - sul significato della cosa.

Poi, gradualmente, il silenzio.

Il rapporto STOA(8) (122 pagine di analisi su armi, tecnologie, reti e servizi segreti) è stato pubblicato il 18 dicembre 1997. Il 27 gennaio 1998 è stato presentato al "European Parliament Committee on Civil Liberties and Internal Affairs". Oggi siamo nel settembre del 1999, e ancora pochi sanno cosa dice, cosa scopre e cosa spiega, di cosa ci avverte questo rapporto.

In questa serie di articoli sui punti chiave delle reti di controllo globale, cercherò di spiegare cosa e quali sono, di dare il mio punto di vista ed approfondire a livello tecnico i casi Echelon ed Enfopol, aggiungendo però alla visione d'insieme che andrò a descrivervi alcuni fattori all'apparenza estranei tra loro; il risultato finale è il termine inquietante sopra accennato: la ***Sorveglianza Globale.***


AN APPRAISAL OF TECHNOLOGIES
OF POLITICAL CONTROL

Working document
(Consultation version)

Luxembourg, 6 January 1998

PE 166 499

Directorate General for Research

Cataloguing data

Title An appraisal of technologies for political control

Publisher European Parliament
Directorate General for Research

"La copertina del Rapporto STOA per il Parlamento Europeo"

(2) Il Mondo, 3 aprile 1998: "dossier intercettazioni, un ex-agente racconta i segreti del sistema UkUsa Echelon"
(3) Il Mondo, 17 aprile 1998: "dossier esclusivo, caso Echelon, parla Luigi Ramponi. Anche i politici sapevano"
(4) Enemy of the State, 1998, Touchstone Pictures, Gene Hackman e Will Smith. http://movies.go.com/eos/site/index.html
(5) N.S.A. National Security Agency, agenzia governativa statunitense per la sicurezza nazionale
(6) Central Intelligence Agency
(7) G.C.H.Q. Government Communications Head Quarter
(8) http://cryptome.org/stoa-atpc.htm. N.d.R.: Ritengo sia dovere di ogni cittadino europeo scaricarlo e prenderne visione

Autore: Raoul Chiesa - *Settembre 1999*

Le Reti di Controllo Globale: un'analisi approfondita dei casi Echelon ed Enfopol in una visione a 360° - L'inizio Menwith Hill

3. L'inizio
Menwith Hill

Verso la fine degli anni '70, quando si era da poco laureato alla Lancaster University del Regno Unito, Steve Wright si imbattè per la prima volta in ***Echelon***: fotografò per interesse accademico e di studio sull'argomento delle torri-ripetitori, vicino al suo campus universitario, le quali ufficialmente svolgevano il ruolo di ponti telefonici per le chiamate a lunga distanza e transoceaniche ed erano collocate sul tetto dell'ufficio postale della sua città. Osservando giorni dopo le fotografie, notò che i dischi delle parabole non erano puntati verso il nord ed il sud del paese, bensì verso il nord dell'Irlanda ad ovest e verso un posto chiamato Menwith Hill ad est.
Tre settimane dopo fu prelevato a casa da due macchine dei servizi segreti e portato alla sua Università, la quale fu dunque la prima Università inglese a subire una perquisizione dell'Intelligence britannica.
Più o meno nello stesso periodo due ricercatori universitari norvegesi, Nils Peter Gledisch e Owen Wilkes - i quali stavano effettuando ricerche simili a quelle svolte da Wright ed un suo collega, ebbero seri problemi ...
Oggi possiamo dire che quei ricercatori ***stavano iniziando a scoprire le viscere dell'infrastruttura di ascolto globale della NSA.***

La base di Menwith Hill fotografata da un elicottero

Nel 1947, più di cinquant'anni fa, venne alla luce un "patto", un'alleanza strategica tra cinque paesi. Il patto fu chiamato Ukusa ed i paesi costituenti sono Stati Uniti, Gran Bretagna, Canada, Australia e Nuova Zelanda. L'obiettivo è chiaro e di ampia portata: intercettare, spiare, analizzare le informazioni che viaggiano nell'etere. Dagli anni 50 ad oggi la tecnologia ha fatto passi da gigante. La telefonia fissa, i telefax, quella cellulare, i satellititi, Internet: il mondo ha cambiato il modo di comunicare. Il patto Ukusa non è rimasto fermo.

Una cosa da chiarire prima di proseguire nella spiegazione del patto Ukusa ed arrivare poi a parlare di Echelon, è il fatto che questa alleanza sia stata sì stipulata tra i governi dei diversi paesi membri, ma di fatto sia gestita dalle singole Intelligence dei vari paesi **(9)**

Oggi, 1999, dalle basi di Sugar Grove e Yakima negli USA, Walhopai in Nuova Zelanda, Geraldton in Australia, Morwenstow nel Regno Unito e da quella di Hong Kong (ricordiamoci, oggi divenuta cinese) partono le richieste di parole chiavi, frasi, nominativi: i dati vengono inoltrati al paese richiedente.
Questi dati vengono comparati a quanto intercettato dalla rete di controllo, analizzati e trasmessi attraverso satelliti dedicati dai due gateway di Fort Meade nel Maryland e Menwith Hill nella zona di North York Moors nel Regno Unito.
Menwith Hill è il centro nevralgico europeo di questo network, e Menwith Hill ha "creato" Echelon.

(9) ***N.S.A. e C.I.A. per gli USA, G.C.H.Q. ed MI6 per il Regno Unito, C.S.E. (Canadian Security Establishment) per il Canada, G.S.C.B. (Government Communications Security Bureau), per la Nuova Zelanda, DSD (Defense Signal Directorate) per l'Australia.***

Autore: Raoul Chiesa - *Settembre 1999*

Le Reti di Controllo Globale: un'analisi approfondita dei casi Echelon ed Enfopol in una visione a 360° - La Struttura di Ukusa ed il Ruolo di Echelon

4. Oggi
La Struttura di Ukusa e il ruolo di Echelon

Nicky Hager ha scritto e pubblicato, nel 1996, "Secret Power: New Zealand's Role in the International Spy Network (10) Il settimanale Il Mondo lo ha intervistato in occasione del primo articolo italiano su Echelon. Hager è stato di estrema importanza ed utilità per capire come funziona fisicamente la rete dello Ukusa Agreement. Nicky spiega a Il Mondo che "La particolarità del sistema Echelon è che la sua rete di satelliti, basi terrestri e supercomputer non è disegnata soltanto per permettere l'intercettazione di alcune particolari linee di trasmissione, bensì per ***intercettare indiscriminatamente*** quantitativi inimmaginabili di comunicazioni ***attraverso qualsiasi mezzo o linea di trasmissione***".

I - Le basi

Ogni compagnia telefonica nel mondo (Telecom Italia, Omnitel, Infostrada, France Telecom, KDD, etc..) utilizza per le comunicazioni internazionali uno dei 25 satelliti geostazionari Intelsat, i quali ruotano intorno alla Terra, stazionando sopra l'equatore. Nelle cinque basi di ascolto Ukusa vengono intercettate le comunicazioni gestite da questi satelliti.
Ogni Paese aderente al patto Ukusa ha in affidamento la copertura di un'area specifica del mondo: in Inghilterra ad esempio si trova la base che controlla il traffico europeo, sulle scogliere del Cornwall, mentre il traffico nord-sud del continente americano è gestito dalla base di Sugar Grove, a 250 chilometri circa dalla capitale americana. Le telecomunicazioni sul Pacifico sono invece divise tra la base americana di Yakima (250 chilometri a sud-ovest di Seattle), la base neozelandese di Waihopai - aperta nel 1989 (11) - e quella australiana, sita a Geraldton, la quale cura anche l'area dell'Oceano indiano.

II - Satelliti Spia

Dai primi anni '70 in avanti la N.S.A. ha messo in orbita una costellazione di satelliti spia, chiamata in codice "Vortex".
"L'ultima generazione di satelliti - spia è costituita da tre nuovi "bird" geosincronici messi in orbita negli ultimi quattro anni, che da soli coprono praticamente tutto il mondo", dice il massimo esperto del settore Jeff Richelson." Quello che copre l'Europa staziona in orbita a 22.300 miglia di altitudine sopra il Corno d'Africa ed e' controllato dalla base terrestre inglese di Menwith Hill, nel nord dello Yorkshire, che con i suoi 22 terminali satellitari è di gran lunga la più grande e potente della rete Ukusa" (12) Menwith Hill è quindi la stazione europea NSA di "scrematura ed inoltro" (matching & forwarding) più importante ed è distribuita su 4.9 acri di terreno: nel 1991 vince il "premio NSA" come stazione dell'anno, grazie alla sua ***estrema utilità durante la guerra del Golfo***.

III - Echelon, dictionary manager & Memex

La rivoluzione delle comunicazioni e tecnologie digitali ha facilitato di molto l'industrializzazione della sorveglianza, spiega Wright. Una volta, prima della caduta del Muro di Berlino, la polizia segreta della Germania dell'Est (13) disponeva di 500.000 informatori segreti, 10.000 dei quali erano necessari semplicemente per trascrivere le telefonate dei cittadini(14): oggi lo stesso lavoro è svolto o può essere svolto dalla tecnologia.
E' vero anche che la mentalità stessa, la psicologia nell'analisi dei dati, il mercato così come il modo di fare commercio sono enormemente cambiati in questi ultimi 30 anni: basti pensare al marketing: ieri si indagava su quante persone avessero un telefono, oggi su quante persone lo usano in una casa, per chiamare chi, dove e a che ora.

Steve mi illustra come questa nuova era tecnologica sia caratterizzata da sistemi che, "collegati in ***tempo reale***, custodiscono dati personali ***e*** sistemi di monitoring: questo significa che, per la prima volta, ci si trova davanti alla necessità di ***immagazzinare*** e contemporaneamente ***analizzare*** queste informazioni."
Si arriva allora al ***data-veillance***, termine che nasce dalla fusione delle parole ***surveillance*** (sorveglianza) ed elementi di ***artificial intelligence*** (intelligenza articificiale). Questa data-veillance è basata sull'approccio militare al così chiamato "C3I", vale a dire "Communications, Command, Control and Intelligence", una modalità gerarchica di usare le informazioni per coordinare l'Intelligence militare e le truppe.

Risulta allora ovvio che l'enorme mole di dati ed informazioni raccolta dai satelliti spia deve essere paragonata con le richieste pervenute dalle basi, al fine di scremare e catalogare le informazioni e realizzare il data-veillance:

il terzo e ultimo componente del sistema Ukusa è costituito da una matrice di network-supercomputer, i quali hanno la capacità di “assorbire, esaminare e filtrare in tempo reale enormi quantita' di messaggi digitali e analogici, estrapolare quelli contenenti ognuna delle parole - chiave preprogrammate, decodificarli e inviarli automaticamente al quartier generale del servizio di Intelligence dei cinque Paesi interessato ai messaggi che includono la parola predeterminata.
Questi supercomputer sono stati battezzati "dizionari", e ogni pochi giorni i "dictionary manager" dei cinque Paesi cambiano la lista delle parole chiave, inserendone delle nuove e togliendo delle vecchie a seconda dei temi politici, diplomatici ed economici di interesse per gli Usa e i suoi alleati", spiega Hager. "E una volta inserite le nuove parole e' solo questione di minuti prima che i dizionari comincino a sputar fuori messaggi che le contengono".
Per svolgere tutte queste funzioni è stato realizzato un sistema di intelligenza artificiale, battezzato Memex.
E’ interessante notare come ogni stazione di analisi abbia un proprio nome in codice: quando vengono inoltrati messaggi inerenti particolari keyword, il messaggio è sempre preceduto dal nome in codice della stazione che l’ha analizzato: la stazione di Yakima, ad esempio, situata in una zona desertica tra le Saddle Mountains e le Rattlesnake Hills, ha in uso il COWBOY dictionary, mentre la stazione neozelandese di Waihopai ha nome in codice FLINTLOCK. Questi codici di identificazione sono dunque registrati all’inizio di ogni comunicazione intercettata, affinchè gli analisti riceventi sappiano sempre ***quale stazione ha intercettato, scremato ed inoltrato il messaggio.***
Vi sono poi altri centri di smistamento oltre Menwith Hill: queste stazioni hanno - oltre ai compiti sopra esposti - la funzione di ascolto per i satelliti geostazionari ***non appartenenti*** alla rete Intelsat. In aggiunta alle stazioni di ascolto puntate verso questi satelliti, infatti, ed oltre la stazione di Menwith Hill, abbiamo altre quattro stazioni base: Shoal Bay, vicino alla città di Darwin nell’Australia del nord (targetting verso i satelliti indonesiani), Leitrim, appena a sud di Ottawa, Canada (satelliti latino americani), Bad Aibling in Germania, e Misawa nel nord del Giappone.

Una visuale completa della base di Menwith Hill

IV - Percorsi ed output

Il “percorso” di questa mole di informazioni è dunque molto particolare: sulle colline della Cornovaglia le antenne di Morwenstow raccolgono i segnali dei satelliti Intelsat - i quali ***non viaggiano in criptato*** - e li inviano alla "operation room" dove sono stati dati in pasto prima a un potente amplificatore e poi a una batteria di radioricevitori sintonizzati sulle differenti frequenze da microonde su cui trasmettono gli Intelsat. Ogni frequenza ha un certo numero di bande di segnali, ognuna delle quali contiene a sua volta centinaia di messaggi telefonici, fax, telex ed e-mail elettronicamente compattati tra loro (è il cosiddetto multiplexing).
Grazie a speciali apparecchi americani chiamati ***statmux*** questo insieme di messaggi è stato separato nei singoli messaggi individuali che lo componevano, e i messaggi inviati nelle bande di frequenza di maggior interesse, cioè quelle che Echelon sa essere usate nelle comunicazioni importanti, sono stati inviati nel "dictionary", il supercomputer anima del sistema. A questo punto il computer ha prima convertito i vari tipi di messaggi - telefonate, fax, e-mail - in un linguaggio digitale standard, e poi ha attivato la ricerca delle parole richieste (keyword) inserite dai "dictionary manager" dei cinque Paesi. Tutti i messaggi contenenti le keyword sottoscritte sono poi stati immediatamente e automaticamente passati a un altro computer che li ha messi in codice e spediti via satellite al quartier generale della NSA, a Fort Meade nel Maryland, dove sono stati decodificati e analizzati dai tecnici americani.**(15)**

I prodotti finali del sistema Echelon si dividono in tre categorie distinte: i rapporti, i "gist" (gist in inglese significa nocciolo della sostanza) e i sommari. I rapporti sono traduzioni dirette di messaggi intercettati, i "gist" sono compendi telegrafici in cui si offre il succo del discorso e i sommari sono compilazioni che contengono informazioni di diversi rapporti e "gist" e vengono poi conservate nelle banche dati di ciascun servizio di "Signal Intelligence" dei cinque Paesi membri di Ukusa.**(15)**

"Ogni servizio ha la possibilità e il diritto di chiedere agli altri di fornire sommari da essi prodotti su particolari soggetti, specificando però a chi è destinata l'informazione", spiega Hager. Vista la frequenza di questi scambi, i Paesi dell'Ukusa hanno creato un sistema di distribuzione elettronica e in codice che muove continuamente rapporti tra un Paese e l'altro. Nel caso di informazioni particolarmente delicate, c'è inoltre a disposizione una rete di corrieri appartenenti allo staff del Defense Courier Service, di base al quartier generale della NSA a Fort Meade.**(15)**

I ricevitori satellitari di Menwith Hill

(10) Nelson, NZ, Craig Potton, 1996
(11)La base di Waihopai fu aperta su forti pressioni della NSA: negli anni immediatamente successivi fu largamente utilizzata per intercettazioni verso il Giappone e le comunicazione diplomatiche dalle varie ambasciate. Nicky Hager, Exposing the global surveillance system
(12)"Il Mondo", 20 marzo 1998, Claudio Gatti
(13) Stasi, Servizi Segreti della Germania dell'Est
(14)John O. Koeble. Stasi: The Untold Story of the East German Secret Police", Westview Press, Boulder, 1999
(15)"Il Mondo", 20 marzo 1998, op. cit.

Autore: Raoul Chiesa - *Settembre 1999*

Le Reti di Controllo Globale: un'analisi approfondita dei casi Echelon ed Enfopol in una visione a 360° - Sistema di controllo Globale: gli utilizzi

5. Oggi
Sistema di controllo Globale: gli utilizzi

Vent'anni dopo quella lontana visita da parte dell'Intelligence britannica, Steve Wright si prende dunque la sua rivincita: il rapporto Stoa(16) presentato al Parlamento europeo spiega che la rete-spia della NSA/GCHQ mina le basi del Trattato Europeo di Maastricht, il quale aveva il compito di garantire la parità in tutti gli scambi tra gli stati membri.
Nel 1998 ai membri del Parlamento Europeo vengono dunque fornite le evidenze dei fatti per cui la US NSA ed il Governo Britannico con i propri servizi segreti hanno **creato i mezzi per intercettare ogni comunicazione fax, e-mail e telefonica** (cellulare, fissa, radio) **all'interno dell'Unione Europea.** Voci non confermate e tantomeno autorizzate mormoravano da decenni di attività di spionaggio da parte della NSA in Europa, ma prima del rapporto STOA nel 1998 non c'era mai stata alcuna conferma ufficiale: ora il mondo sa che la NSA ha creato una capacità di sorveglianza sull'intero network di comunicazioni europeo.

Quello che però emerge dal rapporto STOA è ancora più inquietante: Echelon è il nome di una rete di supercomputer capace di esaminare vaste aree di spettri di comunicazione e individuare parole chiave precedentemente inserite o ricevute dagli altri nodi; la potenza di elaborazione (o "scanning and screening") di Echelon dichiarata dalla NSA era, nel **1992**, di **2.000.000 di comunicazioni all'ora**(17) Facendo un esempio concreto, se io impostassi come parola chiave ("keyword") la parola FIAT, gli elaboratori Echelon scandaglierebbero tutte le comunicazioni europee e paneuropee (telefonate, fax, comunicazioni via e-mail) per il termine FIAT e analizzerebbero in pochissimo tempo una mole impressionante di comunicazioni.

Ora, quello a mio parere ***ci deve fare pensare*** - e molto, ed in fretta - è che il rapporto STOA di Steve Wright abbia dimostrato come la NSA abbia sviluppato le proprie attività di spionaggio commerciale: nel 1990 furono impostate alcune keyword particolari, in quanto il colosso americano della telefonia, la At&t, concorreva ad una gara d'appalto contro la giapponese Nec, per la fornitura di strutture di telecomunicazioni all'Indonesia. Gli USA spiarono le trattative e l'appalto fu vinto dalla At&t: oggi le centraline telefoniche nazionali ed internazionali a Jakarta sono americane.

Esiste il forte sospetto, riportato anche da giornali britannici come il Sunday Times(18), che la rete di intercettazioni Echelon venga utilizzata da britannici e americani anche per ottenere informazioni economiche riservate relative alle politiche di grandi gruppi industriali o finanziari.
Allo stesso modo si è sospettato che all'indomani dalla tragedia della funivia di Cavalese, avuta conoscenza della forte reazione italiana e nel timore di un'escalation della crisi, la NSA abbia molto probabilmente inserito nel sistema le parole "Cavalese" e "Cermis". Hager spiega come "L'Italia e gli altri Paesi europei sono bersaglio costante di Echelon e la richiesta americana di inserire nuove parole - chiave relative a questioni italiane a Morwenstow sarebbe stata accolta dai tecnici inglesi senza alcuna sorpresa. Sarebbe stata un'operazione di routine, gestita a livello amministrativo", sostiene Hager. Da quel momento, ogni telefonata, fax, messaggio elettronico proveniente da o diretto a ministeri, uffici governativi, ambasciate e probabilmente anche residenze e quartier generali di leader politici e militari italiani contenente le parole Cavalese e Cermis può essere diventato bersaglio del sistema Echelon.(19)
Naturalmente nessuna di queste accuse è stata mai confermata dai diretti interessati.... Il Parlamento Europeo, in risposta, dopo tutto il clamore suscitato con il rapporto STOA, ha commissionato un nuovo rapporto dal titolo "Surveillance technology and risk of abuse of economic information"(20).

I cambiamenti nell'***informazione globale*** raccolgono tecnologie e tecniche per fornire mezzi sia al fine di acquisire informazioni economiche su concorrenti commerciali, sia per sviluppare controlli su gruppi radicali ed i loro contatti associati attraverso "friendship networks". Vedremo cosa accadrà....ma cerchiamo di non subire passivamente.

Scansionatura satelittare computerizzata per tracking visivo

(16) Rapporto STOA 1998: pubblicato dallo STOA, riferimenti: Project N.° IV/STOA/RSCH/LP/politicon.1
(17) Duncan Campbell, Tip for Tap, The Guardian, 10 settembre 1998
(18) Edizione dell' 11 maggio 1998
(19) Il Mondo del 20 marzo 1998, "Licenza di spiare. i segreti di Echelon"
(20)"Le tecnologie di sorveglianza ed i rischi di abusi sulle informazioni economiche"

Autore: Raoul Chiesa - *Settembre 1999*

Le Reti di Controllo Globale: un'analisi approfondita dei casi Echelon ed Enfopol in una visione a 360° - La "risposta europea": Enfopol

6. La "risposta europea": Enfopol

Una gioia mal riposta

Come accennato nell'introduzione, i giornali annunciarono con gioia ed "orgoglio" la scoperta di Enfopol, la rete di intercettazione Europea nata come risposta ad Echelon. In realtà le cose sono ben diverse...o sarebbe meglio dire che non sono cambiate poi di molto. Enfopol è sì infatti un sistema di controllo e spionaggio pianificato per collegare i diversi circuiti di polizia internazionale responsabili di polizia locale, dogana, immigrazione e sicurezza interna del Paese: peccato però che questa rete faccia capo all'F.B.I. americana.

Vero è che tra FBI e CIA/NSA non corre buon sangue (si vocifera che le prime "rivelazioni scomode" su Echelon siano opera dell'FBI stessa, la quale non ha mai gradito la "libertà" che la NSA e la CIA spesso si autoassegnano nelle operazioni di controllo e spionaggio elettronico), ma ciò non toglie il fatto che Enfopol non sia altro che il secondo grande orecchio degli Stati Uniti d'America sull'Europa.

Un'Europa che corre verso l'unificazione totale, la moneta unica, l'unione delle Intelligence dei vari Paesi membri, ma che ancora non ha un sistema ***proprio*** e che dipende in tutto e per tutto dagli USA. Un'Europa alla quale scotta il fatto che il Regno Unito abbia tenuto nascosto per decenni l'esistenza di Echelon e del patto Ukusa, un'Europa che si scopre di colpo arretrata tecnologicamente: a tutt'oggi i grandi backbone mondiali per le comunicazioni Internet si trovano negli Stati Uniti, e molto spesso quando chiamiamo un sito o inviamo un'e-mail, il dato rimbalza sino a New York prima di rientrare in Europa verso il paese chiamato.

Il consorzio EU-FBI

Da almeno quattro anni un consorzio internazionale fondato dall'FBI ha discusso e promosso progetti per intercettare i sistemi di comunicazione che fungono da collegamento tra i telefoni mobili ed i satelliti. L'interesse dell'FBI nella stesura di una simile rete di intercettazione è abbastanza chiara: dai primi anni 90 in poi l'Europa delle telecomunicazioni ha iniziato la privatizzazione, e incominciava a non essere più possibile una forma di intercettazione standard ***comune a tutti***. La tecnologia delle TLC (21) ha iniziato a correre velocemente prima ed esponenzialmente poi, rendendo obsoleto un consistente standard di intercettazioni. Quindi, siccome i sistemi sono diventati ***globali***, era dunque necessaria una completa collaborazione a livello internazionale, per permettere che il "phone tapping" continuasse ad essere realizzabile. Ricordiamoci poi che il sistema GSM è stato introdotto in Inghilterra poco dopo la seconda metà degli anni 80, mentre nel resto dell'Europa ha fatto la sua comparsa agli inizi degli anni 90, e che l'Inghilterra è membro del patto Ukusa dalla fine degli anni 40.

Questo consorzio ha spesso richiamato l'attenzione sulla "cooperazione globale tra le forze di Polizia europee, inclusa una nuova coscrizione dei fornitori dei nuovi sistemi di comunicazione, al fine di portare avanti le intercettazioni nel caso in cui ve ne fosse la necessità, seguendo specifiche istruzioni".

Il 3 dicembre del 1995 a Madrid, durante il summit "EU-US", è stato firmato il trattato "Transatlantic Agenda", parte del quale era il "Joint EU-US Action Plan", il quale analizzava questi sforzi come "un tentativo costante di ridefinire l'Alleanza Atlantica nell'era post Guerra Fredda". Pare che queste direzioni non indichino altro se non l'intenzione delle Internal Security Agency dei singoli Paesi membri dell'Unione Europea di acquisire un nuovo tipo di controllo globale a livello europeo.

La parte politica, così come nel caso Echelon, ha subito passivamente: sembra che nulla sia mai stato chiesto a riguardo della costruzione di una rete di intercettazioni con simili capacità a nessun governo europeo, che non ci sia mai stata alcuna richiesta di votazione o scrutinio, e che nemmeno il Comitato per le Libertà civili del Parlamento Europeo ne sia mai stato informato.

Leggi e standardizzazione europee

"La votazione fu semplicemente decisa in segreto, tramite uno scambio di telex tra i governi degli allora 15 paesi membri della EU", racconta StateWatch, organizzazione editoriale per i diritti civili. Sempre StateWatch informa che, ad oggi, ***"il piano per il sistema di Sorveglianza Globale EU-FBI è in sviluppo":*** in altri termini ciò significa che - come illustrato nel rapporto STOA - il progetto ha, come paesi interessati e complici, l'Europa dei 15 con, in più,

USA, Canada, Norvegia e Nuova Zelanda. Un gruppo “stranamente associato”, che non credo verrebbe accettato dai Ministeri degli Affari Interni dei singoli Paesi membri o dai parlamenti nazionali, e tantomeno dal Parlamento Europeo.

Naturalmente Enfopol si muove veloce, per cercare di raggiungere il “cugino” Ukusa: nel ***“rapporto Enfopol 19”***, StateWatch ha scoperto che “i numeri di carte di credito personali sono ora richiesti come un identificativo personale universale”. Nell’edizione precedente, ***“Enfopol 98 Rev2”***, non vi era alcun riferimento ai numeri di carte di credito.
Abbiamo poi dei cambiamenti meno vistosi tra la versione precedente e quella successiva, modifiche molto più “di classe” e quasi invisibili. Quello che segue è un estratto comparativo di una riga del rapporto ***Enfopol 98 Rev2*** ed ***Enfopol 19:*** arriviamo ad un rapporto di “minima variazione/altissima implicazione”.

“IP CONNECTIONS ARE NOT INCLUDED” (Enfopol 98 Rev2)

“ IP CONNECTIONS ARE NOT EXCLUDED” (Enfopol 19)

L’Italia ed il ruolo di Iridium

Risulta ovvio dopo qualche riflessione che queste proposte di cambiamento e standardizzazione avranno ripercussioni su molti Paesi membri della Comunità Europea, spesso con implicazioni ***costituzionali.*** In Italia, ad esempio, si trova la base terrestre di Iridium, la rete di satelliti di per le comunicazioni via telefono mobile satellitare. Iridium è un consorzio, dove i gateway sono di proprietà di uno o più investitori: ***“Iridium Italia e Iridium Communication Germany gestiscono il gateway Europea che è stata installata presso il centro spaziale "Piero Fanti" della Telespazio, in provincia de L'Aquila, a circa 130 km da Roma”***, ci informa gentilmente il sito web della Iridium Italia(22).

Il gateway italiano di Iridium presso il Fucino

Il sito ci spiega inoltre che “...la stazione del Fucino - la più grande infrastruttura civile per le telecomunicazioni al mondo - ***è stata scelta per la sua posizione geografica***, ottima per servire il continente europeo e le regioni limitrofe. Il Fucino ospita anche un centro GBS (Gateway Business System), un centro informativo per l'elaborazione e l'amministrazione dei dati del servizio (contratti, consumi, bollette)”.....credo che ora capiate l’importanza strategica della base Iridium.

La stessa Iridium Italia gestisce dunque la fornitura dei servizi IRIDIUM in Belgio, Bosnia Erzegovina, Croazia, Danimarca, Isole Faroe, Francia, Grecia, Jugoslavia, Italia, Liechtenstein, Lussemburgo, Ex Repubblica Jugoslava di Macedonia, Malta, Monaco, Paesi Bassi, San Marino, Slovenia, Svizzera, Città del Vaticano.....riflettiamo.

Gli accordi Enfopol vogliono dire allora che l’Italia, in quanto Paese membro e Paese ospitante la base terrestre satellitare europea, avrebbe delle responsabilità o implicazioni nel caso in cui intercettazioni remote venissero richieste sulla base dell’Aquila ? Come mi spiega Steve Wright, le opzioni possibili sono due:

1. l’attuale “opzione centralizzata”, la quale prevede che ogni singola intercettazione venga autorizzata attraverso “lettere internazionali di richiesta”;

2. un “approccio remoto”, il che significa che un singolo e generico ordine è dato dall’Italia alla sua stazione di terra, per impostare gli algoritmi di scrematura richiesti al fine di permettere l’attivazione autonoma di intercettazione tramite i fornitori di servizio nazionale, e la trasmissione automatica del materiale intercettato.

In tutto questa bagarre di problematiche politiche, legislative ed economiche non dobbiamo dimenticarci della criptazione, l’unica forma di difesa del privato cittadino per la privacy reale delle proprie comunicazioni digitali: in molti paesi del mondo è una tecnica proibita dalla legge, e paesi come la Francia hanno recentemente fatto delle vere e proprie inversioni ad U in termini legislativi rispetto ad altri paesi europei, liberalizzando l’uso della criptazione delle comunicazioni.
Ovviamente gli Stati Uniti spingono l’Unione Europea ad un uso più controllato di questa tecnologia.

Una stazione terrestre di Iridium

(21) ***N.S.A. e C.I.A. per gli USA, G.C.H.Q. ed MI6 per il Regno Unito, C.S.E. (Canadian Security Establishment) per il Canada, G.S.C.B. (Government Communications Security Bureau), per la Nuova Zelanda, DSD (Defense Signal Directorate) per l'Australia.***
(22)"Il Mondo", 20 marzo 1998, Claudio Gatti

Autore: Raoul Chiesa - *Settembre 1999*

Le Reti di Controllo Globale: un'analisi approfondita dei casi Echelon ed Enfopol in una visione a 360° - L'occhio si aggiunge all'orecchio: I sistemi di controllo a circuito chiuso urbani

7. L'occhio si aggiunge all'orecchio: I sistemi di controllo a circuito chiuso urbani

Le origini dei CCTV

La tendenza ai sistemi di sorveglianza a circuito chiuso (CCTV (23)) ha origine nel Regno Unito nel 1985: infatti, dopo un anno particolarmente brutto per il calcio inglese e complice l'influsso e l'immagine negativa apportata dai famigerati ***hooligans***, il Football Trust (associazione fondata dalle squadre di calcio inglese) autorizzò l'installazione di sistemi di controllo a circuito chiuso in 92 club. Il passo successivo fu fatto dalla Polizia britannica, la quale installò sistemi di CCTV mobile lungo tutta l'Inghilterra.
Nella totale assenza di regolamentazioni o linee guida, la polizia trovò molteplici utilizzi per questo sistema. La voce si sparse in fretta e il boom dei sistemi CCTV era fatto: ottimo appoggio quando si trattava di presentare l'evidenza delle prove ai processi, il sistema era perfetto anche come "tecnica di controllo sociale".
Telecamere iniziarono a spuntare nel centro di Londra così come nelle piazze principali di varie città, e i cittadini inglesi accolsero con piacere questi strumenti, meritevoli di dare una maggior sicurezza alle donne che tornavano dal lavoro alla sera, o ai bambini nei giardini.
Scuole, ospedali, biblioteche, piazze, vie, negozi.... Ovunque una telecamera ad osservare la folla, le strade, le automobili e le relative targhe degli automezzi.
Sebbene i sistemi CCTV siano utilizzati in altri paesi, nessuno di questi ha avuto un'evoluzione come il Regno Unito: l'evoluzione tecnologica è stata tale che si è arrivati ad un punto per il quale in molti centri urbani questa rete può essere considerata onnipresente. Si è arrivati a considerarli parte integrante del controllo e della lotta alla criminalità: non dimentichiamoci che, quando il mondo intero rimase shockato per le immagini dell'assassinio di un bambino da parte di due suoi amici di 10 anni, l'ultima immagine di James Bulger portato via dal centro città verso i binari abbandonati dove fu poi ritrovato proveniva dai sistemi CCTV del centro di sorveglianza dello shopping center di Liverpool. Le immagini stesse furono usate come prova durante il processo.

Le reti CCTV oggi

Oggi l'industria della sorveglianza visiva britannica spende tra i 150 ed i 300 milioni di sterline all'anno (24), con un parco di telecamere tra i 200.000 ed i 400.000 pezzi. L'Home Office britannico stima che circa il 95% delle città e dei paesi inglesi si stiano dirigendo verso i sistemi di controllo CCTV per la sorveglianza di aree pubbliche, parcheggi e zone residenziali. La crescita di questo mercato è quantificata dal 15 al 20% all'anno.
Le telecamere stesse sono cambiate - e di molto - dal 1985 ad oggi. Anche in questo caso, come per le reti del patto Ukusa, la tecnologia è progredita, permettendo telecamere antivandalismo, di ridottissime misure, con capacità di "motion detection" e con potenti zoom e dispositivi ad infrarossi, consentendo così anche la visione notturna.
La progettazione degli stessi sistemi è cambiata ed ha sposato tecniche militari di protezione: le nuove installazioni vengono effettuate in modo tale che ogni telecamera controlli sempre la postazione adiacente, fornendo così un controllo incrociato antivandalico ed evitando problemi di sabotaggio, i quali sono sempre esistiti ma raramente sono denunciati, specialmente in Irlanda del Nord. Il governo conservatore di John Major promosse tenacemente l'introduzione di questi sistemi, ed il governo Blair ha continuato per la stessa strada.

Qual è il risultato, oggi ? La più grande rete centralizzata di controllo sulla folla, sui luoghi di comune interesse, sugli avvenimenti di maggior rilievo; un piano su scala nazionale, per il quale entro 5 anni l'Inghilterra completerà la costruzione del più grande sistema di sorveglianza e controllo del traffico stradale il quale, quando sarà terminato, identificherà e seguirà le tracce ed i movimenti di praticamente tutti i veicoli della nazione.
Socialmente, questa tecnologia ha influenzato - e non di poco - le abitudini degli inglesi: nella città di Brighton, ad esempio, la polizia concede la licenza per i superalcoolici o per un locale pubblico solamente se lo stesso è dotato di sistema CCTV interfacciato con la polizia locale.

Abbiamo quindi una tecnologia che fornisce la soluzioni a problemi quali vandalismo, uso di droghe, alcolismo, molestie sessuali o razziali, creazione di disordine pubblico...I sistemi sono stati anche utilizzati per monitorare dimostranti durante manifestazioni (25).
I problemi nascono però, come nel caso di Echelon, dall'interfacciamento di questi dati con i database...
Quello che il governo inglese non dice è che tutte le telecamere inglesi sono state interfacciate a due strumenti

estremamente potenti: il Plate Tracking System e il Facial Recognition System.

Le nuove tecnologie

Il Plate Tracking System (P.T.S.) permette alle telecamere, mediante l'interfacciamento con data base esterni, di riconoscere le targhe delle autovetture, e ricercare quindi gli automezzi indicati dal sistema centrale.
Nel Regno Unito per esempio il sistema multifunzionale di gestione del traffico (Traffic Master) utilizza il riconoscimento delle targhe per mappare e gestire gli ingorghi autostradali. Tecnologie P.T.S. sono state installate anche in Svizzera, lungo la A1 Autobahn tra Zurigo e Berna.

Il ***Facial Recognition System*** (F.R.S.) permette invece di individuare e riconoscere tra la folla dei visi, delle facce le cui immagini sono immagazzinate negli archivi centrali di più Intelligence o corpi di polizia, nazionali ed internazionali. La tecnologia più utilizzata è il Mandrake System, il quale in teoria può riconoscere le caratteristiche facciali di un viso nel momento stesso in cui appaiono sullo schermo **(26)**.

Il F.R.S. applicato a Will Smith nel film "Nemico Pubblico

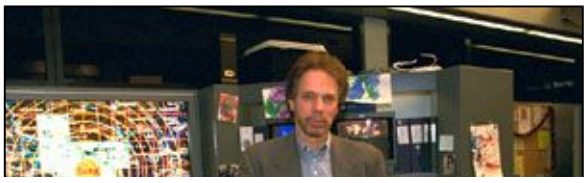
Il pericolo nasce quindi dall'interfacciamento di queste reti e questi sistemi con gli archivi esterni. La ***Video Surveillance*** sta diventando una infrastruttura nazionale e, forse, il governo USA utilizza già queste strutture per scopi di propria sicurezza nazionale.
Pensiamo però se - come nel caso di Echelon - queste tecnologie venissero utilizzate per scopi commerciali: immaginiamo le targhe delle automobili dei dirigenti di importanti compagnie e multinazionali, continuamente seguite e rilevate; immaginiamo personaggi politici o di rilievo nazionale ed internazionale, costantemente monitorizzati nei loro spostamenti.

Spero che molti dei lettori abbiano visto la scorsa stagione cinematografica il film "Nemico Pubblico", con Gene Hackman e Will Smith: nella storia la NSA era in grado di monitorare attraverso i satelliti, con scarti di pochi metri e una definizione di immagine molto vicina alla perfezione, gli spostamenti di persone e cose. Questo mediante una serie di filtri e controlli incrociati su telefonate, onde radio, dati sensibili (movimenti bancari, archivio telefonate, chiamate a pager, celle di provenienza chiamata, etc..) immagini via satellite e tracking via P.T.S. e F.R.S. ***Allo stato attuale e nel momento in cui scrivo, la tecnologia in possesso della NSA*** e del patto Ukusa, unita agli "archivi" on-line del patto EU-FBI, fanno di questo magnifico film - del quale consiglio caldamente la visione - ***un insieme di informazioni e tecnologie arretrate e "not updated"***....nonostante il film sembri fantascienza pura !

Nell'agosto di quest'anno gli Usa hanno lanciato "Ikonos-1", il più potente "image-satellite" commerciale mai realizzato. Le sue lenti paraboliche sono capaci di riconoscere oggetti di piccolissime dimensioni ovunque sulla faccia della Terra. Il satellite, di proprietà della Space Imaging di Denver, Colorado, è il primo di una nuova generazione di satelliti spia ad alta risoluzione di immagine, i quali utilizzano tecnologia ufficialmente riservata alle agenzie di sicurezza governativa. Altre dieci compagnie hanno ottenuto le licenze per effettuare lanci di satelliti simili, e quattro di esse hanno pianificato di effettuare i lanci entro la fine del 1999 **(27)**.

Mercoledì 12 agosto, invece, un missile Titan 4 dell'aeronautica militare statunitense è esploso mentre si innalzava in cielo dalle rampe della base di Cape Canaveral, in Florida. La base del missile era destinata a mettere in orbita un satellite Vortex, commissionato alla Lockeed dal National Reconnaissance Office, un'agenzia governativa di Intelligence. E i Vortex, come illustrato nella sezione Echelon di questo articolo, costituiscono la vera e propria ossatura satellitare del sistema di intercettazioni Echelon. Il satellite era destinato a coprire aree di importanza strategica per il governo Usa, quali Pakistan e India, Cina e Medio Oriente; il costo del satellite si aggira sul ***miliardo di dollari...***

L'impatto che i sistemi CCTV e le tecnologie correlate hanno creato nei confronti dei diritti, delle libertà, della privacy e della vita pubblica del singolo individuo è dunque molto, molto profondo. La distanza, la differenza tra la salvaguardia del cittadino e il calpestare i diritti privati di un essere umano è molto piccola. Hanno esagerato con Echelon, chi ci dice che non faranno lo stesso errore con le reti a CCTV ?



Una sala di controllo della NSA nel film "Nemico Pubblico

(23) CCTV: Closed Circuit Tele Vision; televisione a circuito chiuso
(24) tra i 225 ed i 450 milioni di dollari
(25) A seguito dei cortei "June 18" nel centro di Londra durante il 1999, l'High Court inglese ha capovolto la richiesta della polizia di ottenere le fotografie scattate dai giornalisti durante le dimostrazioni, considerando le immagini dei sistemi CCTV pubblici e privati adeguate per le esigenze della polizia e quindi utilizzabili legalmente e pienamente
(26) In questo caso però la percentuale d'errore può raggiungere il 20%
(27) Simon Davies, "Hi-res spy satellite set for launch", Daily Telegraph "connected", 8 luglio 1999

Autore: Raoul Chiesa - *Settembre 1999*

Le Reti di Controllo Globale: un'analisi approfondita dei casi Echelon ed Enfopol in una visione a 360° - Conclusioni: 50 anni per scoprirne l'esistenza: quanti per cambiare le cose?

8. Conclusioni
50 anni per scoprirne l'esistenza: quanti per cambiare le cose ?

L'evoluzione di Internet - sia dal punto di vista commerciale che tecnico, oltre che naturalmente di diffusione - ha apportato molte possibilità per la libertà ***reale*** di informazione e pensiero. Durante la recente guerra in Serbia, le sole radio funzionanti per un certo periodo, ed indipendenti dal regime, erano quelle via Internet: trasmissioni con mezzi di fortuna, connessioni a 9.600 o 14.400 baud (9.6K e 14.4K), ma spiegavano a persone di altri paesi come stavano realmente i fatti. Allo stesso modo, grazie al costante incremento delle reti di telecomunicazioni e delle ampiezze di banda trasmissiva, oggi troviamo le analisi dei bombardamenti NATO sulla Serbia entro poche ore dai lanci su svariati siti web.

La maggiore difficoltà imposta da questa rapida evoluzione è l'aumento massiccio di una varietà enorme di telecomunicazioni digitali, che oggi le Intelligence Agency devono monitorare, tracciare, tradurre ed interpretare.

Il termine WWW (World Wide Web, la Grande Ragnatela Mondiale) suggerisce una superstrada dell'informazione la quale è universalmente accessibile, ma naturalmente non è così. Ovviamente Internet raggiunge solamente una piccolissima parte della popolazione mondiale, all'incirca 65 milioni di persone, meno comunque dello 0.1% della popolazione mondiale. Inoltre ha una distribuzione ed un utilizzo principalmente nell'Europa dell'ovest e nel nord America; una percentuale ben più alta di questo 0.1%, però, è influenzata dalle multinazionali, dagli istituti di credito e finanziari, dalle strutture pubbliche, da ogni altro tipo di istituzioni o aziende che, comunque, custodiscono informazioni personali e che ***usano le infrastrutture delle telecomunicazioni per comunicare e scambiarsi dati***. **"Chi" può "cosa" ?**

Credo risulti logico che i primi target dei sistemi illustrati in questa serie di articoli, da Echelon ad Enfopol passando per i sistemi CCTV britannici e i loro interfacciamenti, fossero in primo luogo il terrorismo, lo spionaggio e la sicurezza dello Stato e dei cittadini. Forse, con il passare degli anni, questi obiettivi si sono persi. Forse il ***potere dell'informazione*** è un qualcosa che fa perdere la testa, o allontanare gli scopi originari. Spaventa un pò pensare al potere presente nelle mani di chi detiene simili quantità di informazioni, classificabili e inviabili attraverso terra, mare e cielo in tutto il pianeta.
Chi decide **quando** non è necessario richiedere autorizzazioni e seguire la prassi burocratica, chi decide quando la privacy di un privato cittadino o azienda può essere violata ? E' anche vero però che iniziano a scoprirsi delle "falle" nelle strutture delle varie Intelligence coinvolte. Per alcuni uomini il peso di un segreto simile può divenire eccessivo, le responsabilità che si sentono nei confronti degli "altri" troppo onerose.....

Defezioni

Le rivelazioni di un ex agente canadese della C.S.E, Michael Frost, colgono impreparati i diversi governi. Frost ha raccontato al settimanale Il Mondo di aver spiato, dall'interno di diverse ambasciate canadesi, le comunicazioni di altre sedi diplomatiche. Il nome in codice dell'operazione era Pilgrim. Un importante e sconvolgente particolare, per il nostro parlamento, è sicuramente il fatto che, dall'aprile del 1983 in poi, Frost ha operato nella capitale italiana. L'ambasciata canadese a Roma, dunque, come un vero e proprio centro di spionaggio (28).

A Frost si è aggiunto Richard Tomlison, ex agente dell'MI6, il servizio segreto britannico. Tomlison, che oggi si trova in “esilio” in Svizzera, ha rivelato in una lettera inviata alla Commissione per i Servizi Segreti della House of Commons, che i suoi ex-colleghi britannici sono stati costantemente impegnati in attività di spionaggio economico finanziario ai danni di altri Paesi europei. Prima fra tutti la Germania, ma anche la Francia, l’Italia, la Spagna. Voci non smentite mormorano dell’esistenza di un informatore dell’MI6 addirittura ai vertici della Bundesbank, la banca centrale tedesca. **System X e telefoni cellulari**

A questo punto quello che può venire da pensare ad un attento lettore è che singoli network di sorveglianza e controllo come quelli sopra elencati (CCTV, Echelon, Enfopol) vengano interconnessi, linkati, uno all’altro, per poter così fornire una rete completa di data-veillance, divenendo addirittura una sorveglianza in tempo reale dove tutti i componenti di una particolare organizzazione, società o partiti politici sono seguiti.
Il rapporto STOA spiega ad esempio come Polizia ed Intelligence Agency possano utilizzare sistemi di monitoraggio e localizzazione geografica, uniti a servizi di tracking per sorvegliare telefoni cellulari: il chip della carta GSM diventa quindi una nostra “impronta digitale”, o forse una “microspia permanente”.
Se questo termine può sembrarvi eccessivo e paranoico, Wright mi spiega che il “Sistema Digitale X” inglese ha come caratteristica di base l’essere in grado di poter mettere i telefoni cellulari “off hook”, ed ascoltare così le conversazioni che avvengono vicino all’apparecchio, divenendo in tal modo a tutti gli effetti un microfono remoto.
Questa caratteristica fornisce un mezzo di ***intercettazione su scala nazionale*** abbastanza economico per un governo, ed il System X è già stato esportato in Russia ed in Cina **(29)**

Le celle delle reti cellulari divengono così dei mini-dispositivi di tracking e possono localizzare i proprietari (o meglio, il loro segnale) in qualunque momento su un display ad informazione geografica, con scarti di poche centinaia di metri: tutto questo naturalmente se il cellulare è acceso. Ma quello che non è stato ancora completamente capito è che le centinaia di milioni di movimenti ed attività dei telefoni mobili (cellulari e satellitari) e quindi dei loro abbonati sono custoditi nei CED dei fornitori di servizi, molto spesso per un periodo di almeno sei mesi.
Il rapporto STOA nota infatti come, nel 1997, la polizia elvetica abbia monitorato e tracciato gli utilizzi dell’Internet Service Provider SwissCom, il quale custodiva i “movimenti in Rete” di più di un milione di abbonati, andando indietro sino a sei mesi prima dell’inizio dei controlli (notizia riportata anche dalla Reuters il 28 dicembre 1997).

Simon Davies attraverso Privacy International **(30)** spiega che la Gran Bretagna partecipando a un sistema come Echelon avrebbe contravvenuto al trattato di Maastricht, ed in particolare modo all'articolo V del trattato, che ***obbliga i Paesi membri a informare gli altri partner su tutte le questioni relative alla sicurezza e alla politica estera che rivestono un interesse generale.***

Abbiamo quindi avuto (e succederà probabilmente sempre di più nel prossimo futuro) il primo dibattito al Parlamento Europeo sulla ***sorveglianza transatlantica elettronica***, così come un intenso dibattito politico su ***chi o cosa sia legittimamente sorvegliabile*** sia nella UE che negli USA, in che modo, e su che cosa UE e USA possono sorvegliare e dove....

Certo, lo spettro che si va man mano disegnando è molto pesante, e potrebbe avere implicazioni impensabili sino a pochi anni fa. La sorveglianza globale implica l’informazione personale globale, e l’informazione è un potere che va acquistando sempre più velocemente valore. Corriamo velocemente verso il futuro, ma forse torniamo indietro nei secoli, perdendo un elemento fondamentale delle nostre esistenze: ***la libertà.***

(28) CCTV: Closed Circuit Tele Vision; televisione a circuito chiuso
(29) tra i 225 ed i 450 milioni di dollari
(30) CCTV: Closed Circuit Tele Vision; televisione a circuito chiuso

Autore: Raoul Chiesa - *Settembre 1999*

Le Reti di Controllo Globale: un'analisi approfondita dei casi Echelon ed Enfopol in una visione a 360° - Ringraziamenti

9. ringraziamenti

Oltre a Simon Davies e Steve Wright, desidero ringraziare Nicky Hager per il supporto informativo datomi ed il settimanale Il Mondo per l'enorme mole di informazioni disponibili on-line sul loro sito web (http://www.ilmondo.rcs.it/) e la loro "battaglia personale" e giornalistica per fare luce sulla verità.

Un ringraziamento particolare e personale va invece a Enrico Novari (31) per avermi introdotto e sensibilizzato al problema Echelon (consiglio una lettura del suo ottimo articolo sull'argomento, "Il rapporto STOA: alla base del caso Echelon", disponibile alla URL http://www.internos.it/archivio/gi99ppf.pdf), ed a Jusy Accetta di Internos e Salvatore Romagnolo di Apogeo Editore, per la fiducia che continuano a riporre in me e la libertà di pensiero che mi permettono di esprimere attraverso le rispettive testate.

Un secondo ringraziamento va alla Dottoressa Isabella Colace dell'Istituto Nazionale di Fisica Nucleare di Roma, responsabile relazioni esterne dell'Isodarco (International School On Disarmament And Research On Conflicts): ho mantenuto la promessa, Isabella.

Ringrazio infine, per motivi diversissimi tra loro, Eleonora Cristina Gandini e Laura Casanova De Marco, per la spinta datami da entrambe - in anni diversi e per periodi diversi - a proseguire per una strada.

"Last but not least", tutto lo staff **MediaService.net** per il supporto tecnico e morale datomi in questi anni.

Un Grazie di cuore a tutte queste persone.

Raoul Chiesa

(31) ***Autore, tra l'altro, della prima tesi italiana sull'hacking dal titolo "Il Web Oscuro: Origini, sviluppo e percezione dell'hacking in Italia", Università La Sapienza di Roma***

Autore: Raoul Chiesa - *Settembre 1999*

Le Reti di Controllo Globale: un'analisi approfondita dei casi Echelon ed Enfopol in una visione a 360° - Disclaimer

10. Disclaimer