SPIARSI TRA ALLEATI: LA NATO NELLA RETE ANGLO-AMERICANA

Pubblicato in: DOPO LA GUERRA - n°2 - 1999

9/04/1999

La guerra del Kosovo ripropone la questione dello spionaggio elettronico. Il trattato UkUsa è la base di un rapporto privilegiato fra britannici e americani, che si dividono le sfere di competenza geopolitica su scala mondiale. Il caso Echelon.

di Luca Mainoldi

QUALI SONO I RAPPORTI DI FORZA FRA Stati Uniti ed Europa in termini di spionaggio elettronico? La guerra tra Serbia e Alleanza atlantica e la riorganizzazione della Nato pilotata dagli Usa impongono una riflessione su questo delicatissimo tema. Infatti, molti in Europa sono convinti che il Grande Fratello americano carpisca tutte le conversazioni riservate. La presunzione di essere intercettati è diventata una specie di status symbol. Come dimostreremo, gli Stati Uniti applicano una rigorosa politica di controllo unilaterale nei confronti dei propri partner, anche se alcuni di questi, come la Francia (per non parlare di Israele), intraprendono attività spionistiche a danno di Washington.

Per affrontare questi argomenti occorre anzitutto chiarire alcuni termini tecnici. La raccolta di informazioni a fini di spionaggio si divide in tre categorie, a seconda delle fonti e delle metodologie impiegate: uso di spie e informatori, nel qual caso si parla di Humint (Human intelligence), elaborazioni di dati reperibili attraverso le cosiddette

«fonti aperte» (Osint, Open sources intelligence), infine spionaggio con l'ausilio di mezzi tecnici. In questo ultimo caso particolare rilevanza rivestono le attività Sigint (Signal intelligence), ovvero la raccolta di segnali elettromagnetici emessi intenzionalmente da paesi, enti o organizzazioni di cui si vogliono carpire i segreti. Il Sigint, a sua volta, si distingue in Elint (Electronic intelligence), che intercetta e analizza le emissioni non di comunicazione (radar eccetera), e Comint (Communications intelligence) che raccoglie, eventualmente decritta e analizza i segnali di comunicazione (radio, telefonici e così via). A partire dagli anni Sessanta, i bersagli del Comint sono, oltre le comunicazioni militari e diplomatiche, quelle commerciali e finanziarie e quelle relative al terrorismo, alla criminalità organizzata, ai traffici di droga e armi, al riciclaggio del denaro sporco. Con lo sviluppo delle telecomunicazioni e della telematica tali attività sono diventate sempre più importanti. Si vedrà di seguito che numerosi paesi sono oggi attrezzati per il Sigint.

UkUsa

Gran Bretagna e Stati Uniti hanno una gloriosa tradizione nel campo dello spionaggio elettronico. Durante la seconda guerra mondiale britannici e americani ottennero risultati strategici di rilievo grazie all'intercettazione delle emissioni nemiche: dalla battaglia dell'Atlantico a quella delle Midway, dall'abbattimento dell'aereo di Yamamoto allo sbarco in Normandia gli Alleati dimostrarono la loro netta superiorità in questo campo.

La nostra analisi deve dunque cominciare dalla descrizione della più importante organizzazione dedicata al Sigint a livello mondiale. Si tratta di quell'insieme di agenzie spionistiche legate fra di loro dall'accordo UkUsa (United Kingdom-United States of America). Tale accordo risale agli albori della guerra fredda (1947), ed era rivolto a spiare l'Unione Sovietica e i suoi alleati. Come si può intuire dal nome questo patto è stato inizialmente stipulato dagli enti Sigint dei paesi anglosassoni. Infatti, i firmatari sono gli Stati Uniti attraverso la Nsa (National security agency), il Regno Unito tramite il Gchq (Government communications headquarters), il Cse (Communications security establishment) canadese, il Dsd (Defence signals directorate) australiano e il Gcsb (Government communications security bureau) neozelandese.

Al centro di questo patto si colloca, ovviamente, l'Agenzia per la sicurezza nazionale americana (Nsa), che dispone di mezzi finanziari e tecnologici di gran lunga superiori agli altri partner. La Nsa impiega 20 mila dipendenti solo nel quartier generale di Fort Meade, cui si aggiungono altre decine di migliaia appartenenti alle agenzie di sicurezza elettronica delle quattro forze armate americane. Il suo budget

si aggira sui 10 miliardi di dollari annui. A titolo di paragone, la più famosa Cia ha un bilancio di circa 3 miliardi e 16 mila dipendenti. Sul piano tecnologico la Nsa è all'avanguardia nel mondo nel campo dei supercomputer, della criptologia e dell'intelligenza artificiale.

I partner di UkUsa dipendono strettamente dagli Usa per quanto riguarda la tecnologia di punta e, forse, per alcuni aspetti finanziari. Un esempio di quali siano i reali rapporti di forza all'interno di UkUsa è dato dalla base di Pine Gap in Australia, nella quale metà del personale è americana e l'altra metà australiana. Sembra esserci un equilibrio paritario, ma non è così: il personale australiano include anche gli addetti alle pulizie, i cuochi e i guardiani, mentre quello americano è composto solo da tecnici qualificati.

All'interno di UkUsa c'è una divisione di competenze per aree geopolitiche. Secondo Ball e Richelson[1], la Dsd copre l'Oceano Indiano orientale, parte del Sud-Est asiatico e il Pacifico sud-occidentale; l'Africa e l'ex Unione Sovietica fino agli Urali sono coperti dal Gchq; il Nord dell'ex Urss e parti dell'Europa dal Cse,una piccola parte del Pacifico sud-orientale dal Gcsb, e tutto il resto dalla Nsa e dalle agenzie militari a questa collegate [2].

Esistono anche delle «terze parti» firmatarie, tra cui l'Italia [3], che sono solo «portatori d'acqua» e non hanno diritto a ricevere informazioni su basi regolari da inglesi e americani. Altri paesi, come la Cina [4], ospitano centri di ascolto UkUsa o forniscono informazioni in base ad accordi ad hoc.

UkUsa ha quindi una capacità di intelligence globale che si avvale di una rete di basi e postazioni di ascolto ad alta tecnologia sparse in tutto il mondo, integrate da mezzi mobili (navi, aerei) e dai sofisticati satelliti Sigint americani.

Echelon

In questo contesto ha destato scalpore la pubblicazione del libro *Secret Power – New Zealand's Role in the International Spy Network* di Nick Hager [5], che descrive il funzionamento di Echelon, un sofisticato sistema di ascolto globale delle comunicazioni internazionali gestito da UkUsa. Tale sistema spia tutti, nemici o alleati delle potenze anglosassoni. Le informazioni raccolte riguardano non solo e non tanto questioni militari ma anche diplomatiche, commerciali, finanziarie, tecnologiche fino ad arrivare, in alcuni casi, a spiare il singolo cittadino di un paese terzo [6]. Ogni tipo di comunicazione è oggetto d'intercettazione da parte di Echelon: conversazioni telefoniche e radio, fax, e-mail, Internet.

Costruito a partire dagli anni Settanta e aggiornato più volte, Echelon è costituito da

una serie di postazioni d'ascolto volte innanzitutto ad ascoltare le comunicazioni che passano attraverso i satelliti Intelsat. Le stazioni di intercettazione dei sistemi Intelsat e Inmarsat sono ubicate a Yakima (costa del Pacifico) e Sugar Grove (costa atlantica) negli Usa, Morwenstow in Gran Bretagna, Geralston in Australia (che ha assunto anche le funzioni della stazione Gchq-Dsd di Hong Kong ora abbandonata) e Waihopai in Nuova Zelanda.

Le comunicazioni passanti attraverso i satelliti russi e regionali sono raccolte da sette altre stazioni ubicate in Gran Bretagna (la base Nsa di Menwith Hill che gestisce tra l'altro il progetto Moonpenny d'intercettazione dei satelliti Raduga russi), Canada (Leitrim), Australia, Germania, Giappone (Misawa, progetto Ladylove per spiare i satelliti russi Molnya, Raduga e Gorizont), Puerto Rico (Sabana Seca) e negli Usa (Rosman nel North Carolina). Altre basi sparse in tutto il mondo (dall'Alaska alla Thailandia) intercettano le comunicazioni radio e quelle telefoniche che passano attraverso i cavi sottomarini. Sono sotto controllo le torri costiere a microonde che collegano i cavi alle reti telefoniche nazionali, ma si sfruttano anche congegni a induzione posati sui cavi stessi. I cavi a fibre ottiche pongono dei problemi, dato che non emettono radiazioni spurie, ma c'è la possibilità di servirsi delle emissioni dei dispositivi che rafforzano il segnale lungo il percorso.

Installazioni come Menwith Hill, Bad Aibling in Germania, Buckley in Colorado e Pine Gap in Australia servono come *relay* per i satelliti Sigint americani. Si tratta di mostri di diverse tonnellate posti in orbita geostazionaria in grado, con la loro antenna grande come un campo da calcio, di intercettare persino i segnali emessi dai telefoni cellulari [7]. Infine, nelle ambasciate dei paesi UkUsa vi sono centri d'ascolto clandestini che forniscono ulteriori informazioni.

Tutti i dati così raccolti vengono filtrati attraverso un sistema integrato di computer, chiamato Dictionary, che ricerca determinate parole-chiave. Questo filtro funziona solo per i testi scritti (e non a mano); per le comunicazioni vocali ci si limita a usare un sistema di riconoscimento della voce per rintracciare determinate persone. In ogni stazione tutte e cinque le agenzie partecipanti hanno una propria *library* di parole-chiave. Ad esempio, i segnali raccolti dalla stazione neozelandese di Waihopai sono filtrati da cinque banche dati diverse, ognuna dotata di una propria sequenza di parole-chiave. Queste basi sono collegate da una rete simile a Internet, per cui le informazioni raccolte sono immediatamente disponibili a migliaia di chilometri di distanza. La nazione ospite della base ha accesso solo alla propria sequenza, dunque non sa quali informazioni gli altri partner raccolgono a partire dal proprio territorio. Risulta evidente, per rimanere nell'esempio citato, che la lista di parole-chiave americana sia più sostanziosa di quella neozelandese.

Dirty tricks

Uno dei modi migliori per finire nel mirino di Echelon è quello di criptare le proprie comunicazioni; è chiaro che sono proprio i segnali in codice a destare per primi la curiosità dei computer di Dictionary. La Nsa ha una capacità molto sviluppata di rompere codici sconosciuti [8], ma gli ultimi ritrovati pongono problemi di difficile soluzione. Così la Nsa cerca di esercitare uno stretto controllo sui produttori americani [9] di sistemi di crittografia, fino a pretendere di installare una *back door* sui chip destinati a questi scopi. Lo stesso fanno le altre agenzie del patto UkUsa.

Un paese o un'industria consapevoli di questi rischi tenderanno, quindi, ad evitare di comprare prodotti occidentali o anche russi, e si rivolgeranno a un paese neutrale come la Svizzera. Ma il principale produttore svizzero di macchine cifranti è accusato di essere, in realtà, in combutta con la Nsa. La Crypto AG elvetica è sospettata da anni di avere stretto un rapporto di collaborazione con la Nsa.

Dopo la guerra di Suez (1956), nel corso della quale aveva rotto i codici usati dagli anglo-francesi e dagli israeliani, la Nsa intuì che gli alleati della Nato si sarebbero attrezzati per cercare di prevenire le intercettazioni americane. Un alto funzionario dell'Agenzia intraprese nel 1957 un viaggio in Europa che lo portò prima in Gran Bretagna, dove ricucì lo «strappo» con il Gchq (se mai ci fosse stato), e poi in Svizzera, dove incontrò il proprietario della Crypto AG (che all'epoca aveva sede in Svezia e in Svizzera per poi spostare tutte le attività in quest'ultimo paese). È probabile che in questa occasione si siano poste le basi per un accordo secondo il quale la ditta elvetica fornisce i codici impiegati dai propri clienti (tra cui molti membri della Nato) agli Usa [10].

L'accordo c'era dall'inizio, dalla nascita della azienda

Inoltre, in tempi recenti è emerso che anche la Germania partecipa a questa operazione. Secondo un articolo di *Covert Action Quarterly* [11], apparso nel 1997, la Crypto AG sarebbe gestita dalla Nsa e dal BND tedesco insieme con la Siemens e la Motorola, due aziende che forniscono ai governi tedesco e americano sistemi crittografici. Dalle testimonianze raccolte presso i tecnici della ditta elvetica si deduce che ogni loro nuovo prodotto prima di essere messo sul mercato veniva inviato in Germania e negli Stati Uniti, dove tecnici di questi paesi suggerivano modifiche volte a rendere più facilmente decrittabili i messaggi inviati tramite queste macchine. In pratica, il congegno invia clandestinamente prima del messaggio la chiave con la quale è protetto; a sua volta questa chiave è protetta da un'altra in modo che solo la Nsa possa riceverla. Dall'indagine di *Covert Action Quarterly* si ricava che quest'operazione coinvolge le ditte Crypto AG e Gretag in Svizzera, Transvertex in Svezia, Nokia in Finlandia e un'azienda ungherese privatizzata da non molto.

Un caso analogo si è verificato con alcuni sistemi di trasmissione «protetti» fabbricati dal Sudafrica al tempo dell'apartheid e venduti ad alcuni paesi africani, che formalmente non avevano alcun legame con Pretoria ma non disdegnavano di comprare sottobanco tecnologia strategica sudafricana [12]. La Nsa aveva collaborato con il Sudafrica nella seconda metà degli anni Settanta inviandogli sistemi Sigint tramite una società di copertura [13]; non si può escludere, quindi, che la vendita di sistemi sudafricani truccati rientrasse in questo accordo. In questo ambito, infine, i servizi d'intelligence statunitensi avrebbero promosso la diffusione di software avanzato per la gestione di banche dati presso servizi alleati, neutrali e nemici, contenente al suo interno una sorta di *back door* che permetterebbe agli agenti americani l'accesso clandestino alle informazioni contenutevi. Questo è quanto si ricava da una complicata vicenda giudiziaria che vede una software house, la Inslaw, contrapposta al ministero della Giustizia americano circa la proprietà di un sofisticato programma per la gestione delle banche dati, chiamato Promis. Secondo i proprietari della Inslaw il furto del Promis da parte di persone legate al ministero della Giustizia americano sarebbe stato promosso con la complicità dell'intelligence americana e israeliana che lo avrebbero modificato per poterlo usare come «cavallo di Troia» nelle loro attività [14]. Operazioni del genere sono facilitate, indubbiamente, dal monopolio quasi esclusivo americano nel settore dell'informatica di alto livello.

L'ultima frontiera della Nsa è la sorveglianza di Internet che avviene soprattutto spiando i nodi strategici passanti per gli Stati Uniti, come quelli della Nasa a Sunnyvale in California e College Park nel Maryland. Uno studio francese [15] sull ospionaggio economico avverte infatti le imprese transalpine di non fidarsi troppo del Web e propone che lo Stato promuova lo sviluppo e l'uso di sistemi di sicurezza di origine francese.

UkUsa nel contesto della geopolitica americana

UkUsa era nata nel contesto della guerra fredda e il suo bersaglio principale erano le potenze comuniste. Qual è ora il compito di questa organizzazione e più in generale dello spionaggio americano?

Con la fine della guerra fredda gli Stati Uniti hanno rivisto la loro politica di sicurezza. Le priorità americane in questo campo possono così essere schematizzate [16]:

• Mai più un'altra superpotenza deve esercitare una minaccia vitale simile a quella che le armi nucleari sovietiche hanno posto durante gli scorsi decenni agli Usa.

• Mai più gli Stati Uniti devono essere coinvolti contro la loro volontà in un conflitto mondiale come fu, per colpa degli europei, due volte in questo secolo.

• Il multilateralismo non è più accettabile: l'Onu e le altre organizzazioni

internazionali non devono più sfuggire al controllo degli Stati Uniti e non possono imporre decisioni contrarie ai loro interessi nazionali.
• Il modello di società fondato sul mercato, la libera impresa, la mondializzazione e la deregolamentazione implica la difesa e la promozione degli interessi economici americani pubblici e privati in tutto il mondo. La priorità strategica passa, quindi, dall'ambito militare a quello economico. Il compito degli organismi di intelligence americani si orienta pertanto secondo queste priorità strategiche. La promozione degli interessi economici statunitensi è stata codificata dalla dottrina sulla sicurezza economica. Uno dei punti-chiave di questa dottrina è il consolidamento e l'aumento del vantaggio strategico americano nel campo delle tecnologie avanzate, che sono oramai duali – a doppio uso civile e militare – tramite, tra l'altro, un'aggressiva politica commerciale di esportazione. A questo fine è stato creato un nuovo organismo, il Nec (National economic council) per coordinare gli sforzi in questo campo di tutti i dipartimenti coinvolti e consigliare il presidente su queste tematiche. La politica di esportazione viene seguita da un apposito ufficio in seno al Dipartimento del Commercio, chiamato non a caso *war room*.

Parallelamente, l'intelligence community è impegnata alacremente sia a livello difensivo che offensivo. Qualche anno fa destò scalpore la pubblicazione di *Friendly Spies* [17], un libro che accusava alcuni degli alleati degli Stati Uniti di condurre azioni di spionaggio economico contro gli interessi americani. Nel 1995 l'allora senatore Cohen (attuale segretario alla Difesa) presentò una proposta di legge (approvata nell'ottobre 1996) volta a preservare la sicurezza nazionale proteggendo le informazioni economiche dal furto, dalla distruzione e modifica non autorizzata «da parte di governi stranieri, dei loro agenti o dai loro strumenti». Cohen invoca l'uso delle intercettazioni elettroniche nel campo dello spionaggio economico alla stessa stregua di quanto avviene nel caso della lotta al terrorismo e alla criminalità organizzata. Questa legge va inoltre applicata anche all'estero se il criminale o la vittima sono americani e se l'infrazione «sia destinata ad avere, o abbia avuto, un effetto sugli Stati Uniti». Naturalmente, secondo Cohen il furto di informazioni da parte statunitense non costituisce un'infrazione se legalmente autorizzato.

Lo spionaggio elettronico viene visto come il mezzo politicamente più discreto e sicuro per sorvegliare gli alleati (e allo stesso tempo concorrenti economici), come sostiene l'ex consigliere per la sicurezza nazionale Brzezinski [18].

La stampa internazionale riporta alcuni esempi di importanti contratti internazionali che sarebbero stati influenzati dall'uso di informazioni raccolte elettronicamente. È il caso del sistema Sivam per la sorveglianza dell'Amazzonia, vinto dalla Raytheon americana dopo che Clinton aveva fatto pervenire al governo brasiliano informazioni su presunte tangenti pagate dal rivale francese Thomson Csf.

L'amministrazione americana ha lanciato un'offensiva sulle tangenti nei contratti internazionali. Essa si basa su un rapporto della Cia ed è rivolta soprattutto contro l'industria aerospaziale e degli armamenti europea [19] in generale e il consorzio Airbus in particolare [20]. Si tratta di un'offensiva strategica da parte americana nell'ambito del concetto di sicurezza economica prima ricordato. L'appartenenza della Gran Bretagna a UkUsa, dunque, mal si concilia con la partecipazione a Airbus (un contratto con l'Arabia Saudita sarebbe stato vinto da Boeing anche grazie alle informazioni raccolte elettronicamente sulla proposta del concorrente europeo) e più in generale alla definizione di una industria della difesa europea. In realtà, i rapporti all'interno dell'intelligence anglo-americana sono più complessi di quanto si possa credere; per esempio la Gran Bretagna ha dato prova in un'occasione recente di una certa autonomia. Vediamo.

Il caso Unscom

Gli Stati Uniti si sono serviti della missione di controllo dell'Onu (Unscom) del disarmo iracheno per condurre azioni di intelligence. I ponti radio usati da Unscom erano stati dotati segretamente di congegni di intercettazione elettronica. Questa operazione era gestita dallo Special collection elements (Sce), una organizzazione congiunta Cia-Nsa che esegue le operazione di raccolta elettronica da installazioni clandestine, come quelle collocate nelle ambasciate.

Nel caso iracheno gli americani, però, per non esporsi eccessivamente, avevano richiesto che personale inglese conducesse alcune di queste missioni. La Gran Bretagna, non avendo ricevuto tutti i dettagli su come queste informazioni sarebbero state utilizzate, rifiutò di partecipare all'operazione. Questo rifiuto sarebbe stato anche una rappresaglia per la decifrazione, avvenuta qualche anno prima, da parte americana di un codice usato dalle truppe anglo-francesi in Bosnia (probabilmente per proteggere i traffici di armi con i musulmani). Gli australiani subentrarono quindi agli inglesi permettendo a Washington di aggirare la mancata collaborazione di Londra. In questa missione spionistica, inoltre, il team americano-australiano sarebbe stato aiutato da una nota multinazionale delle telecomunicazioni svedese, che ha costruito l'infrastruttura telefonica irachena e che ha fornito sistemi di crittografia a Baghdad [21].

È evidente, quindi, la complessità e la ramificazione dei rapporti che si sono creati nell'ambito UkUsa, che vedono comunque gli Stati Uniti in posizione di predominio.

E l'Europa…

Le rivelazioni sulle potenzialità di Echelon hanno spinto il parlamento europeo a commissionare un primo studio al riguardo, seguito da uno più approfondito [22].

Naturalmente anche i servizi segreti europei si dedicano al Sigint. Sulla base di quanto pubblicato, i paesi europei – Regno Unito a parte – non hanno un'agenziaapposita per il Sigint; in genere queste attività sono svolte dai reparti tecnici dei servizi di spionaggio estero. Questo può essere un indicatore del ritardo europeo in questo campo. Non esiste, inoltre, ancora una politica comunitaria in materia, anche se, per quanto riguarda lo spionaggio satellitare (immagini), è stato creato il centro di Torrejón in Spagna, appartenente all'Ueo e all'Unione Europea.

In Italia il Sismi gestisce, tra gli altri, il centro di Cerveteri che sarebbe anche in grado di intercettare segnali satellitari [23].

In Francia la Direction générale pour la sécurité extérieure (Dgse) è incaricata del Sigint strategico. In particolare [24], essa gestisce attraverso la sua Divisione tecnica un articolato sistema d'intercettazione delle comunicazioni satellitari tramite le basi ubicate in Dordogna (a Domme), in Nuova Caledonia e, grazie ad un apposito accordo con le autorità locali (ottime clienti dell'industria bellica francese), negli Emirati Arabi Uniti. Queste ultime due installazioni intercettano i satelliti che coprono l'area pacifico-asiatica e quella mediorientale. Infine la stazione di Kourou nella Guyana francese (da dove si lancia Arianne) copre l'area americana. Quest'ultima base è gestita insieme al BND tedesco.

Altri centri d'ascolto si trovano a Gibuti, nella Repubblica Centrafricana (questo centro sembra sia stato chiuso), a Guadalupa e nell'isola di Réunion. L'ex base missilistica di Platon d'Albion nell'Alta Provenza è stata trasformata in un'ulteriore stazione Sigint, gestita da una cinquantina di specialisti della Dgse. L'aeronautica francese vi ha, invece, installato un centro d'osservazione dei satelliti. La Dgse ha intensificato negli ultimi anni la sorveglianza dell'Algeria, usando anche strutture dispiegate nei paesi confinanti e la nave spia *Berry* che è stata sostituita recentemente dalla *Boungaiville* ritirata dalla Polinesia. La Direction du renseignement militaire (Drm) gestisce attività Sigint più propriamente militari e dispone, tra gli altri, del segretissimo centro di Mutzig, denominato Centre de guerre éléctronique (Cge) [25]. I servizi francesi si servono, a similitudine di quelli anglosassoni, di potenti computer e di un software particolare per l'analisi delle emissioni intercettate. Il programma Taïga (Traitement de l'information géopolitique d'actualité) messo a punto nel 1987, però, non si basa su parole-chiave, ma è in grado di risalire alla radice delle parole.

La Francia starebbe negoziando nel corso della guerra contro Belgrado uno scambio informativo più ampio con le controparti anglo-americane, ma permangono sospetti

sul suo ruolo, anche alla luce dell'arresto, alla fine del 1998, di un ufficiale francese in servizio presso il comando Nato di Bruxelles, accusato di passare informazioni ai serbi.

La Germania, come si è visto, collabora sia con la Nsa americana che con la Dgse e le sue attività Sigint strategiche sono appannaggio dell'Agenzia federale perla sicurezza delle informazioni (la sigla tedesca è BSI, che costituisce anche il dipartimento 62 del BND). Il BND è più legato all'agenzia americana che a quella francese; infatti alcune delle informazioni raccolte dalla stazione franco-tedesca di Kourou vengono fornite dal BND alla Nsa, mentre il servizio tedesco collabora nella gestione di una centrale di ascolto a Taiwan frutto di uno sforzo congiunto con la Nsa e il servizio segreto militare di Taiwan. Se si pensa all'interscambio commerciale Cina-Germania, si può intuire quale genere di informazioni raccolgano i tedeschi nell'area.

La collaborazione spionistica tedesco-americana ha una radice storica, essendo il BND erede dell'organizzazione Gehlen, una struttura semiufficiale finanziata dalla Cia che riciclava le spie del Terzo Reich. La recente controversia tra Stati Uniti e Germania sull'accesso da parte di quest'ultima agli archivi della Stasi, acquisiti dalla Cia qualche anno fa, dimostra inoltre un certo grado di dipendenza da parte dei servizi tedeschi di fronte alle controparti americane che persiste dalla fine della guerra fredda.

La Svizzera, territorio neutrale del quale si servono servizi segreti e corporazioni legali e illegali per le proprie transazioni finanziarie coperte [26], è uno dei bersagli prioritari della sorveglianza elettronica [27]. La Confederazione a sua volta si è, però, attrezzata per sorvegliare i suoi vicini. Il Groupe renseignement (Gr) gestisce due basi d'ascolto a Merihausen e a Ruthi i cui dati sono analizzati presso il centro di Zimmerwald. A questa installazione faranno capo i sistemi che verranno collocati in due basi vicino a Berna e che diverranno operativi dal 2004 per lo spionaggio delle comunicazioni satellitari, in particolare delle nuove reti Iridium e Globalstar 28 e dei satelliti utilizzati dalle Telecom di Francia, Germania e Italia. Lo «splendido isolamento svizzero» evidentemente non è più tale e i servizi elvetici cercano di ottenere informazioni importanti da scambiare con quelli stranieri. In primo luogo con Echelon [29]? Il sistema Iridium e simili hanno una copertura del segnale molto stretta; la Nsa e le altre agenzie saranno così obbligate ad aumentare le stazioni di ascolto per coprire questi nuovi mezzi di comunicazione. La Svizzera potrebbe rientrare in un programma ad ampio raggio che coinvolge gli Statiaderenti a UkUsa e quelli dell'Unione Europea.

…si difende

Il predominio americano nel campo del Sigint viene visto con sempre più insofferenza da parte europea. L'esplosione di Internet, che è dominato da tecnologie made in Usa e i cui nodi principali sono controllati da Washington, pone ulteriori interrogativi ai governi e alle industrie europee. Di fronte al rifiuto statunitense di permettere la vendita all'estero di sistemi di crittografia «forte» (con chiave di lunghezza superiore ai 56 bits) l'Europa cerca di sviluppare i propri sistemi.

La Francia ha recentemente liberalizzato la vendita di queste tecnologie superando l'obiezione che queste possano favorire le attività criminali [30]. La priorità è passata alla difesa delle imprese francesi dallo spionaggio elettronico altrui. In ogni caso Parigi continua ad aderire alla regolamentazione internazionale (accordi di Wassenaar) ispirata dagli Stati Uniti, che vieta l'esportazione di sistemi con chiave superiore ai 56 bits. Questo significa che i paesi del Terzo Mondo non hanno alcuna difesa contro lo spionaggio da parte dei paesi più forti, e non solo quelli occidentali.

In Italia, l'Istituto di ricerche e comunicazioni sociali di Torino (Ircs) ha sviluppato Ermes, un sistema in grado di nascondere un documento su Internet. In pratica l'informazione potrà raggiungere qualsiasi luogo nascosto in un «micropunto» digitale celato in un testo reperibile nel Web [31].

Al di là di questi provvedimenti, è opportuno definire una politica europea sull'argomento e affrontare la questione con Stati Uniti e Gran Bretagna nelle sedi appropriate, anche in riferimento al ruolo delle basi UkUsa presenti in Europa e al coinvolgimento statunitense nel progetto Enfopol.

1. D. BALL-J. RICHELSON, *The Ties That Bind: Intelligence Cooperation Between the UKUSA Countries,* Sydney 1988, Allen & Unwin, pp. 137-138.

2. Infatti, la Nsa coordina le attività Sigint delle tre forze armate americane, che dispongono di apposite agenzie e reparti dedicati.

3. G. DE LUTIIS, *Storia dei servizi segreti in Italia*, Roma 1991, Editori Riuniti, p. 43. 4. Dai primi anni Ottanta, la Nsa gestisce due stazioni spionistiche nel Xinjiang (a Chi Tai e Korla) per sorvegliare le comunicazioni russe e i loro esperimenti missilistici. Cfr. M. DE ARCANGELIS, *La storia dello spionaggio elettronico*, Milano 1987, Mursia, p. 84.

5. N. HAGER, *Secret Power – New Zealand's Role in the International Spy Network,* Nelson l996, Craig Potton Publishing. A onor del vero il primo articolo su Echelon è del 1988. Cfr. D. CAMPBELL, «Somebody's

Listening», *New Statesman*, 12/8/1988.

6. Ma anche i cittadini anglosassoni possono essere spiati: la Nsa non può legalmente spiare un cittadino americano senza mandato di un giudice, ma questo non impedisce ad esempio al Cse canadese di farlo; poi, in base agli accordi UkUsa, queste informazioni giungono all'ente americano.

7. Gli Usa sono gli unici a disporre di simili sistemi. Il tentativo inglese di realizzare il satellite Comint Zircon è stato superato da un accordo con la Nsa per l'accesso alle informazioni raccolte dai satelliti Magnum americani.

8. Si calcola che i supercomputer della Nsa occupino uno spazio di 11 ettari in un complesso sotterraneo presso la sede centrale dell'Agenzia a Fort Meade nel Maryland, dove vengono smistati tutti i segnali raccolti dalle postazioni di ascolto. La Nsa è il secondo utilizzatore mondiale di supercomputer.

9. La Nsa esercita uno stretto controllo sui sistemi di crittografia «forte», al punto che nemmeno gli inglesi sono messi a conoscenza dei sistemi più delicati. Cfr. P. LACOSTE, «Une nouvelle stratégie pour le renseignement?», *Politique Etrangère*, n. 1/1997, p. 89.

10. Cfr. J. BAMFORD, *The Puzzle Palace: A Report on America's Most Secret Agency*, New York 1983, Penguin Books, pp. 391-425.

11. W. MADSEN, «Crypto AG: NSA's Trojan Whore?», *Covert Action Quarterly,* inverno 1998, reperibile presso http://www.caq.com/CAQ/caq63/caq63 madsen.html.

12. E. KOCH, «Armoscor Hoppers Became Africa's Eavesdroppers», *Weekly Mail & Guardian,* 15/12/1994.

13. A. FRIEDMAN, *La madre di tutti gli affari,* Milano 1993, Longanesi, pp. 114-116.

14. Cfr. F. CALVI-TH. PFISTER, *L'oeil de Washington,* Paris 1997, Albin Michel. Fra gli enti spiati con questo sistema vi sarebbero anche alcuni importanti istituti di credito internazionale.

15. AA. VV., *Economie et sécurité: de l'industrie de défense et de l'intelligence économique,* Paris 1996, Fondation de l'étude de défense, pp. 188-189.

16. Cfr. P. LACOSTE, «Une nouvelle stratégie...», cit., p. 88.

17. P. SCHWEITZER, *Friendly Spies*, New York 1993, Atlantic Monthly Press.

18. V. JAUVERT, «Nous avons fait le choix de tout savoir», *Le Nouvel Observateur*, 16/12/1998.

19. Soprattutto quella francese, accusandola anche di fornire armi agli Stati fuorilegge. La Nsa ha accusato la Microturbo di vendere motori per missili all'Iran.

20. A. PLATEROTI, «Accuse Usa agli europei: maxi tangenti sugli appalti», *Il Sole 24 Ore,* 24/2/1999. Si può intuire il potenziale rappresentato dalle informazioni Sigint in quest'area. Lo spionaggio economico è stato citato come motivo dell'espansione della stazione di Waihopai da parte dei responsabili neozelandesi. Cfr. *Jane's Defence Weekly*, 13/8/1997.

21. J. VEST-W. MADSEN, «A Most Unusual Collection Agency», *The Village Voice,* 2/3/1999. Si veda anche S. HERSH, «Saddam's Best Friend», *The New Yorker,* 5/4/1999.

22. PARLAMENTO EUROPEO, STOA, *An Appraisal of the Technologies of Political Control,* 6/1/1998, seguito da *Development of Surveillance Technology and Risk of Abuse of Economic Information*, aprile 1999.

23. A. SISTO-F. SORTI, «Echelon: Italia nel mirino», *Il Mondo,* 10/4/1998.

24. Cfr. J. GUISNEL, «Les Français aussi écoutent leurs alliés», *Le Point,* 6/6/1998.

25. J.-P. HUSSON, «La Brigade de Renseignement et de Guerre Éléctronique», *Panorama Difesa,* dicembre 1998.

26. Il Mossad per esempio si è servito per anni della Banque de Crédit International di Ginevra (Cfr. R. T. NAYLOR, *Denaro che scotta*, Milano 1986, Comunità, p. 32), mentre la Zimex Aviation di Zurigo era la sua compagnia aerea clandestina.

27. La Nsa impiega per questo scopo le basi di Ramstein, Augsburg, Bad Aibling in Germania e Sorico in Italia (J. ZIEGLER, *La Svizzera lava più bianco,* Milano 1990, Mondadori, p. 42).

28. A. VACCARELLA, «In Svizzera l'orecchio elettronico del "grande fratello"», *Il Tempo,* 28/2/1999.

29. Cfr. *L'Hébdo*, 25/2/1999. Sulla partecipazione svizzera a Echelon si veda «Schweizer Nachrichtendienst bestreitet Beteiligung an US-Spionageprojekt», *SonntagsZeitung*, 8/2/1999.

30. E. ICYAN, «L'espionage éléctronique, priorité de sécurité informatique», *Le Monde,* 21/1/1999.

31. Si veda l'intervista al coordinatore di questo progetto su *Famiglia Cristiana* del 25/4/1999 (pp. 104-106). Notiamo che questa intervista è apparsa su Internet nella stessa settimana di pubblicazione, tradotta in inglese dalla Cia.
