

Gli articoli, le foto e i disegni presenti in questa monografia sono protetti dalle vigenti leggi sul diritto d'autore. Pertanto non possono essere copiati, stampati o riprodotti con nessun mezzo meccanico, elettronico ecc. né usati a scopi commerciali. Qualsiasi deroga, anche parziale, a quanto sopra sarà possibile solo dietro autorizzazione scritta dell'autore ed a condizione che i contenuti non vengano in alcun modo alterati con modifiche o aggiunte. E' inoltre richiesto di menzionare esplicitamente l'autore degli stessi.

**Nota importante
da leggere con attenzione prima di proseguire:**

Gli utilizzi impropri di alcune delle informazioni contenute in questa monografia, potrebbero portare alla violazione della legge 8 aprile '74 n° 98, artt. 615 bis, 617, 617 bis, e della legge 226 c.p.p. sulla riservatezza della vita privata e sulle intercettazioni delle comunicazioni, nonché la legge n°675 del 31/12/96 sulla raccolta dei dati personali e sul diritto alla privacy.

L'autore del presente articolo declina ogni responsabilità sull'eventuale uso illecito delle apparecchiature descritte. Infatti, questa monografia vuole avere solamente uno scopo didattico ed esplicativo, teso a illustrare le modalità con le quali è possibile effettuare una intercettazione telefonica o ambientale e non un invito o un incoraggiamento a mettere in pratica quanto descritto.

Il semplice fatto di proseguire nella lettura, implica l'accettazione di quanto sopra.

N.B.: Questo NON è un sito commerciale. I dispositivi descritti e/o fotografati, presenti nell'articolo, sono di proprietà dell'autore e non sono in vendita. I link a siti di interesse, visibili a fine articolo, hanno il solo scopo di consentire, a chi lo desiderasse, un approfondimento dell'argomento. I relativi siti, commerciali, non sono in nessun modo collegati economicamente con l'autore della presente monografia.

Le microspie dell'ultima generazione; sempre più efficienti e ipertecnologiche

George Orwell, scrittore di origine scozzese della prima metà del secolo scorso, ci aveva avvisati: nel suo romanzo "1984" il genere umano viveva in un mondo controllato da un'autorità governativa centrale che lasciava poco o niente spazio alla vita privata. Come spesso accade, la realtà supera la fantasia: telecamere piazzate in ogni punto delle nostre città, nelle banche, nei supermercati, ci seguono ci controllano...ci spiano!

Il telefono cellulare che ognuno di noi ha in tasca, (complemento "vitale" della nostra esistenza a partire dall'età di undici/dodici anni), trasmette frequentemente al gestore telefonico la nostra posizione topografica con un'approssimazione che va dal centinaio alle decine di metri, a seconda della dimensione della "cella" del ripetitore radiotelefonico più vicino. Questa, ci piaccia o meno, è una condizione essenziale per il funzionamento del sistema cellulare che deve sempre sapere dove si trova un certo telefonino per poter essere raggiunti da una chiamata in arrivo.

Meno essenziale è la registrazione, sempre da parte del gestore, in uno speciale "log", dei numeri telefonici chiamati o ricevuti, nonché degli SMS che hanno interessato quel certo telefonino.

La carta di credito, il bancomat, raccolgono informazioni sui nostri spostamenti e, potenzialmente, sulle nostre scelte di acquirenti. Apposite organizzazioni raccolgono, e commercializzano, dati sulle nostre abitudini di consumatori, sui nostri interessi socioculturali, sulla solvibilità del nostro conto corrente ecc. Dimenticate, anche una sola volta, di barrare la casella "non consento che i miei dati personali vengano usati per....." in calce ai tanti moduli per la richiesta di informazioni, di iscrizioni o di acquisti a distanza, che passano per le nostre mani, e siete immediatamente "schedati".

Alcune persone credono, per sentito dire, che il proprio telefono cellulare potrebbe essere attivato a distanza, anche se spento, per spiare le conversazioni che si svolgono nei pressi. Conosco persone che, quando debbono parlare di argomenti estremamente riservati, in riunioni commerciali, industriali o d'altro genere, tolgono la batteria dal loro telefonino! Quando la paranoia raggiunge il livello di allarme, ecco nascere la "leggenda metropolitana", vera spia delle nostre paure più o meno inconsce. I dispositivi per spiarci, controllarci, ci sono e sono ben attivi! Semmai è la conoscenza delle loro potenzialità che scarseggia.

Le microspie, ad esempio, soprannominate anche "cimici", sono un subdolo mezzo per carpire informazioni, segreti industriali, o per inguaiare mariti troppo "farfalloni". Se fino a pochi anni addietro erano solo i paranoici a temere di essere osservati o spiati, oggi la tecnologia produce apparati miniaturizzati nascosti negli oggetti più banali e davvero capaci di sorvegliare chiunque, a volte anche a costi accessibili.

Le dimensioni di questi dispositivi sono sempre state molto contenute, per l'ovvia necessità di nasconderle nei pressi della vittima di tali attenzioni. Il principale problema da risolvere è sempre stato quello relativo al sistema di alimentazione, ossia alle pile. Le dimensioni di queste ultime, infatti, superavano spesso abbondantemente quelle della microspia vera e propria, a causa della necessità di disporre di una sufficiente autonomia di funzionamento. Non sempre è facile tornare sul luogo dove è installata una "cimice", per provvedere al cambio delle pile. Dunque, o si opta per un'alimentazione tramite la rete elettrica, sopportandone le relative difficoltà di installazione e le perdite di tempo che mal si conciliano con l'azione spionistica, spesso illegale che, al contrario, richiederebbe un intervento rapido e che non dia troppo nell'occhio, o si ricorre a batterie di dimensioni tali da rendere difficoltoso l'occultamento di tutto il marchingegno. Anche oggi la pila di alimentazione rappresenta un notevolissimo problema, nonostante i rilevanti progressi fatti intorno a questo dispositivo.

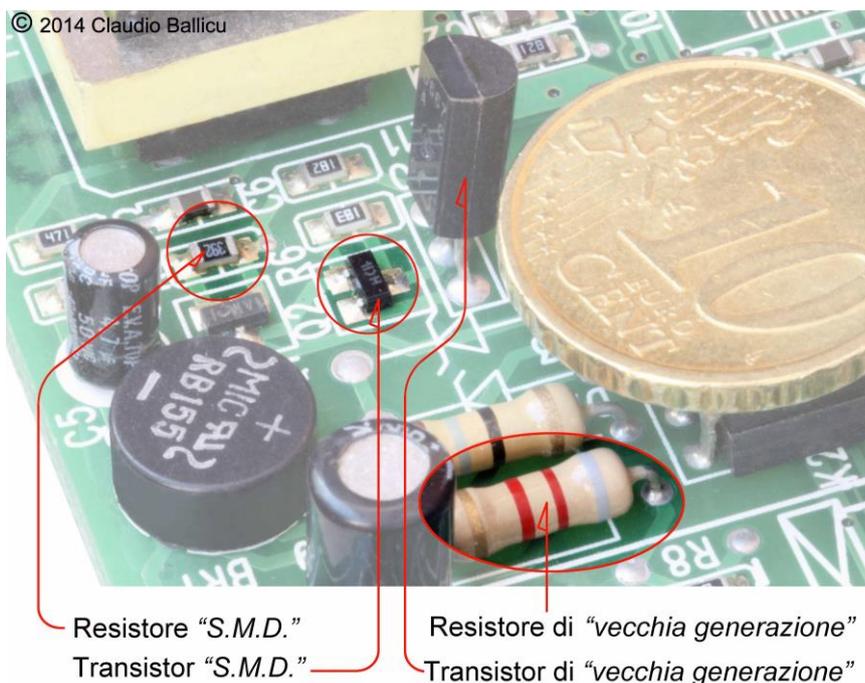
La miniaturizzazione dei circuiti:

Diciamo subito che i progressi più eclatanti sono stati appannaggio dell'elettronica, sia nella direzione della miniaturizzazione dei circuiti, sia in quella della sempre maggiore integrazione di semiconduttori sulla minuscola piastrina di silicio che costituisce il cuore dei circuiti integrati.

L'aggettivo "integrato" sta ad indicare che tutti i circuiti sono inseriti nello stesso contenitore, delle dimensioni di una ventina di mm², ed il numero di componenti realizzati sulla piastrina di silicio che ne

costituisce il cuore, delle dimensioni di 1mm², ha largamente superato, al giorno d'oggi, i 3mila elementi semplici, cosa che sino a pochi anni fa sembrava un livello di integrazione irraggiungibile. Ovviamente questa corsa all'integrazione e alla miniaturizzazione dei circuiti non si è fermata qui ma prosegue attivamente. Probabilmente, quando leggerete queste righe, il livello di integrazione sarà ancora maggiore di quello che ho indicato.

La recente tecnologia "S.M.D.", acronimo inglese di "dispositivi montati in superficie", ha consentito di spingere la miniaturizzazione a livelli tali che, oramai, un tecnico che operi su tali circuiti, usa strumenti che assomigliano più a quelli di un chirurgo, che non a quelli di un laboratorio di elettronica. E' la tecnologia "S.M.D." che ha reso possibile la diffusione di telefoni cellulari sempre più piccoli e sottili, nonostante la notevole complessità della loro elettronica, al punto che il loro dimensionamento è limitato, (non sto scherzando), dalla distanza fra la bocca e l'orecchio della specie umana, dimensione quest'ultima che nessuno ha ancora pensato a ridurre.



Le batterie, al confronto, hanno avuto la parte di Cenerentola. Infatti, pur se innegabilmente ci sono stati dei progressi, non sono stati altrettanto rapidi né rilevanti rispetto a quelli dell'elettronica. Siamo passati dalle pile allo zinco/carbone degli anni cinquanta, alle alcaline, poi alle pile al mercurio, all'argento e successivamente alle moderne nickel/cadmio ricaricabili e, per finire, alle nickel/mercurio/idrogeno o a quelle agli ioni di litio. Le loro dimensioni, tuttavia, sono tutt'altro che trascurabili, superando spesso abbondantemente quello della microspia vera e propria, a causa della necessità di disporre di una sufficiente autonomia di funzionamento. Anche le pile a "bottono", all'argento o al litio, ossia quelle comunemente usate negli orologi da polso, nelle calcolatrici tascabili o nelle macchine fotografiche, sono state via via migliorate dal punto di vista delle dimensioni e della durata, senza tuttavia raggiungere l'optimum della capacità.



Una microspia di livello professionale, made in U.K.



Una microspia di fabbricazione "artigianale", ma non per questo meno insidiosa.

È stata scoperta durante le operazioni di bonifica nello studio di un noto avvocato penalista, fissata con del biadesivo dietro un cassetto della scrivania. La sua portata non supera i 10/15 metri e, probabilmente, veniva ascoltata da una stanza adiacente.

Le microspie ambientali e telefoniche:

Se il vostro lavoro comporta la conoscenza di segreti industriali o d'altro genere e temete perciò di essere spiati da qualche infernale marchingegno o che le vostre telefonate siano registrate, provate a seguire con me un ragionamento logico riguardo alla tecnologia delle microspie in commercio; vi renderete così conto che non è affatto semplice spiare i discorsi che avvengono nel vostro ufficio, a meno che il "nemico" non abbia conoscenze tecniche di buon livello ed usi dispositivi di ascolto abbastanza sofisticati, e quindi di alto costo, che oltre ad essere di difficile reperibilità, si giustificano solo con la rilevanza dei segreti da carpire.

Attenzione! qualsiasi comunicazione è intercettabile! Si tratta solo di valutare il rapporto costo/benefici.

Voglio rivelare uno dei limiti principali di molte microspie di livello modesto: supponiamo di trovarci in una stanza dove siano riunite diverse persone che discutono animatamente fra loro. Una di tali persone sta parlando con noi e, magari, per complicare ulteriormente la cosa, la finestra è aperta e dalla strada sale il rumore di fondo del traffico cittadino.

La situazione descritta non è certo ideale per sostenere una conversazione, tuttavia riusciamo a capire quello che ci dice il nostro interlocutore, grazie all'uso di due strumenti di eccezionale sofisticazione: l'orecchio ed il cervello. Infatti, purché il livello delle voci intorno a noi sia leggermente inferiore a quello di chi ci parla, spostando istintivamente il capo selezioneremo con un orecchio ciò che ci interessa, passando da un ascolto stereofonico ad uno monofonico. Il cervello farà il resto, concentrando su ciò la nostra attenzione e considerando tutto il resto come rumore di fondo. Qualcosa di simile avviene per una madre che dorme tranquillamente nonostante la televisione accesa ed altri rumori ambientali, ma viene risvegliata al minimo accenno di pianto del bambino.

Facciamo ora un esperimento d'altro genere: lasciamo un comune registratore acceso, in posizione "record" ovviamente, in una stanza dove parlano più persone. Potremo constatare, riascoltando le voci incise, che i risultati sono assolutamente deludenti e spesso è addirittura impossibile capire ciò che viene detto. Le cause di una qualità di registrazione così bassa sono molteplici e poco influenzate dalla qualità dell'apparecchio. Se la stanza dove si svolge la prova è priva di tendaggi o con poco arredamento, come spesso sono gli uffici o gli studi professionali, un certo riverbero delle voci renderà queste assai poco chiare. Se le persone parlano fra di loro in modo appena animato, tenderanno ad alzare la voce ed a parlare tutti contemporaneamente. Questo fatto provocherà la saturazione dei circuiti di amplificazione del microfono con la conseguenza che il parlato risulterà cupo e privo dei toni acuti.

E' pur vero che i registratori di buona qualità sono dotati di un circuito elettronico che regola automaticamente il guadagno dell'amplificatore microfonico in funzione del rumore ambientale, ma anche questo dispositivo ha dei limiti nelle sue possibilità di controllo e questi possono essere facilmente superati quando si verifica il caso precedente.

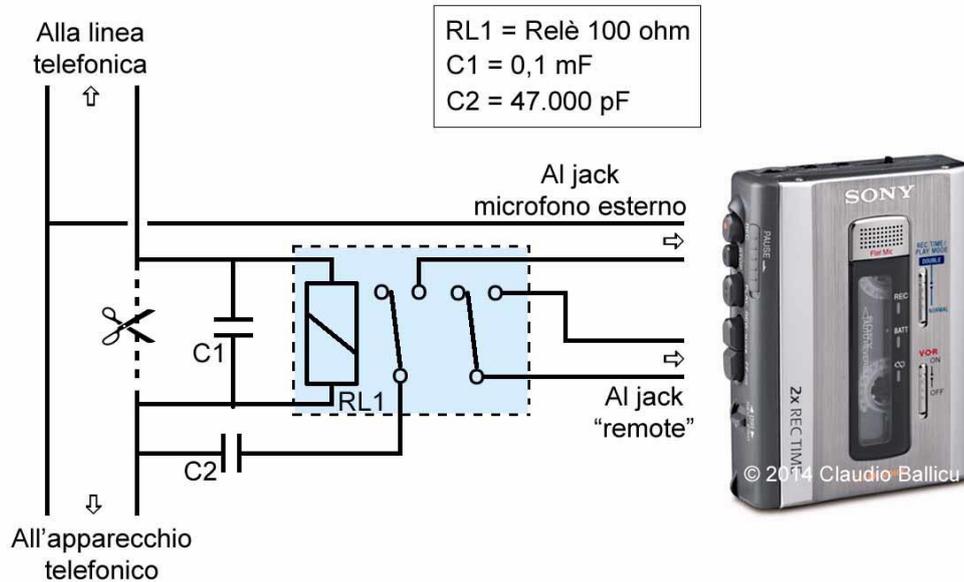
Soprattutto il fatto che i suoni siano riprodotti da un altoparlante, rende impossibile per il cervello umano sfruttare la diversa direzione di provenienza delle varie voci, ossia l'effetto stereofonico, per selezionarne una in particolare. Ogni rumore di fondo giungerà all'orecchio mescolato alle voci registrate in modo talmente omogeneo da impedirci di "escluderlo" dall'ascolto.

Bene, ho portato questo esempio per chiarire uno dei più pesanti problemi tecnici che limitano notevolmente la funzionalità sia delle "cimici" sia di eventuali registratori nascosti.

Spesso la qualità audio di questi dispositivi, a causa dei problemi di cui ho appena parlato, è tale da renderli inutili, a meno che nella stanza dove è nascosta la microspia non vi sia una sola persona che parla al telefono, ma, in questo caso, più che una trasmittente ambientale sarebbe preferibile un registratore telefonico. Quest'ultimo in particolar modo è facilmente applicabile, poiché è sufficiente usare un comune registratore a cassette accessorizzato di un semplice dispositivo elettronico che permette di avviare il nastro ogni volta che viene alzata la cornetta del telefono e di fermarlo alla fine della telefonata. Ciò è molto importante, poiché permette di prolungare la durata del nastro che altrimenti si esaurirebbe in un paio di ore al massimo.

Nelle foto seguenti, e nelle relative didascalie, viene dimostrato come sia facile modificare, a titolo sperimentale, un comune registratore. **Ma attenzione! Non dimentichiamo che le vigenti leggi in materia di tutela della privacy, proibiscono questo tipo di intercettazioni. Ignorarle espone a**

rilevanti sanzioni penali. Inoltre i regolamenti delle società telefoniche vietano espressamente qualunque tipo di manomissione della linea che non sia effettuata da personale autorizzato, **quindi voglio sottolineare che lo schema elettrico seguente ha solamente uno scopo didattico/dimostrativo e non deve essere considerato un incoraggiamento a mettere in pratica comportamenti illegali.**



Un semplice circuito per l' intercettazione telefonica:



Un registratore digitale con memoria SD-card, progettato per l'uso telefonico

Malauguratamente, i divieti legali che ho ricordato più sopra sono tali soltanto per le persone oneste mentre, nell'ipotetica azione di qualche "curioso" troppo disinvolto, le cose sono ben diverse.

E' successo infatti, in qualche caso, che tecnici della società telefonica scoprissero, del tutto casualmente, durante una riparazione o una normale manutenzione, un collegamento abusivo ed illegale nel doppino telefonico al di fuori di un appartamento o di un ufficio o, peggio, una microtrasmittente all'interno di qualche centralina di derivazione Telecom.

E' possibile difendersi dalle intercettazioni telefoniche?

Di una cosa potete essere certi: non è facile difendersi da questo genere di intercettazioni. Esistono, per la verità, dispositivi che, inseriti fra la cornetta e l'apparecchio telefonico, provvedono a codificare la voce invertendo la banda audio nel dominio della frequenza o, più recentemente, modificandola opportunamente dopo averla trasformata da segnale analogico a digitale. Tali dispositivi, chiamati in gergo "scrambler", rendono la voce del tutto inintelligibile ma presuppongono che, dall'altro capo della linea, ci sia un interlocutore munito del medesimo congegno in grado di decodificare la voce rendendola di nuovo comprensibile.

Vi è mai capitato di ascoltare una voce o una canzone registrata, attraverso un nastro che gira al contrario, ossia dalla fine verso il principio anziché nella direzione consueta? Ebbene, un eventuale intruso sulla linea telefonica, ascolterebbe qualcosa di simile, ovvero dei fonemi che sono indiscutibilmente voce umana, ma senza poter capire una sola parola. Nella lingua inglese, la parola "scrambler" significa "mettere in disordine, mescolare alla rinfusa". Il dispositivo elettronico di cui sto parlando opera in tal modo, campionando varie parti dell'involuppo audio, ossia della forma d'onda del parlato, e "mescolandole" fra loro, non in maniera disordinata o casuale, come la traduzione dall'inglese potrebbe far supporre, ma secondo un codice prestabilito, affinché lo "scrambler" dell'interlocutore possa "ricostruire" opportunamente l'involuppo, riportando il parlato ad una forma identica all'originale.

Le sale operative della Polizia di Stato e dell'Arma, quando debbono comunicare qualcosa di riservato verso le radiomobili, usano un sistema "scrambler" di codifica del parlato. Attenzione però: le tecniche di codifica di cui sopra possono essere realizzate, come ho accennato poc'anzi, tanto per via analogica quanto digitale.

Nel caso della codifica digitale, per ragioni tecniche piuttosto complesse sulle quali sorvolo, è possibile operare delle modifiche estremamente sofisticate. Una vera e propria "criptazione" del parlato, attraverso l'uso di algoritmi generati da circuiti a microprocessore appositamente realizzati. Ne consegue che la "decriptazione" di una trasmissione siffatta è pressoché impossibile. Peccato che il costo di uno "scrambler" digitale sia più che decuplicato rispetto ad un corrispondente modello analogico.

Nel caso invece di una modificazione ottenuta per via analogica, (questa è la situazione più comune in virtù del prezzo di acquisto del codificatore che si aggira intorno ai 150/300 euro), è possibile pervenire alla "decriptazione" del parlato, semplicemente registrando la conversazione per poi sottoporla alla decodifica tramite dispositivi "scrambler" programmabili. Non occorrono apparati tanto sofisticati, dal momento che le possibilità di codifica che uno "scrambler" analogico può ottenere sono relativamente poche, per cui la "decriptazione" è solo una questione di tempo.

Le forze di Polizia sono ben coscienti di questo limite, tanto è vero che affidano alle comunicazioni così modificate, segreti che è sufficiente restino tali per qualche ora, ossia fino a quando una certa operazione sia stata portata a termine. Se, al contrario, una comunicazione riguarda indagini riservate che si protrarranno nel tempo, allora verranno usate altre vie per darne conoscenza ai destinatari, ben sapendo con quanta facilità è possibile ascoltare le comunicazioni radio delle Forze dell'Ordine attraverso l'uso di speciali ricevitori detti "scanner", facilmente reperibili nei negozi di apparati per radioamatori.

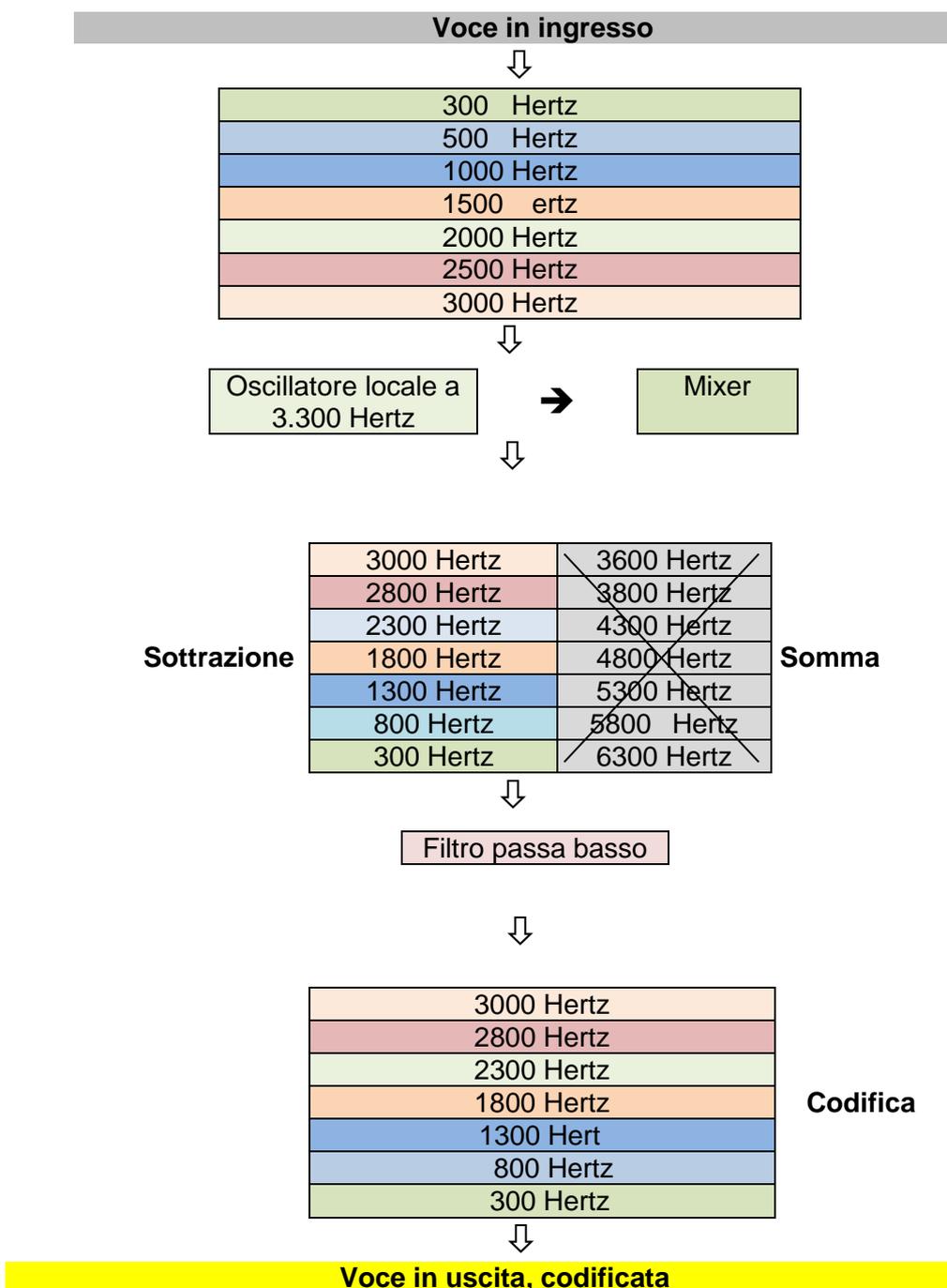
Quindi, se avete cose riservate da comunicare telefonicamente sempre allo stesso interlocutore e pensate di usare uno "scrambler" telefonico, valutatene attentamente i limiti, alla luce di quanto ho appena detto.

Qualora invece le comunicazioni riservate siano dirette a parecchie persone, caso assai più frequente, tale soluzione non appare attuabile per gli ovvi problemi pratici e non esiste altra soluzione se non quella di evitare di parlare di argomenti riservati per telefono, contattando direttamente le persone interessate. Addirittura, se il livello di sicurezza lo richiede, facendo precedere l'incontro da una verifica dell'ambiente

nel quale si svolgerà il colloquio, da parte di un tecnico specializzato in "bonifica ambientale" ossia un esperto dotato di dispositivi idonei a rilevare la presenza di microspie.

Nella tabella seguente, completa di didascalia, fornisco una descrizione del principio di funzionamento di uno "scrambler" a inversione di banda.

Il codificatore di voce:



Apro qui una breve parentesi per ricordare a tutti coloro che ritengono, erroneamente, che i telefoni cellulari dell'ultima generazione siano inintercettabili e quindi adatti e sicuri per effettuare comunicazioni riservate.

L'intercettazione è perfettamente possibile ma riservata agli enti che ne hanno legale diritto, ad esempio Polizia di Stato, Carabinieri ecc. e solamente a seguito di autorizzazione del Magistrato che svolge determinate indagini.

In questo senso è possibile anche la richiesta al gestore telefonico, dei tabulati delle chiamate effettuate e/o ricevute da un certo utente, così come degli sms ecc.

I tabulati saranno, ovviamente, completi dei vari "ponti radio" agganciati durante le conversazioni, in modo da poter risalire alla posizione geografica del cellulare e ai suoi spostamenti sul territorio con un livello di accuratezza subordinato alla orografia del terreno, ad esempio formazioni montuose o collinari, o alla presenza di ostacoli di natura antropica, quali edifici ecc.

In tale contesto, la precisione della posizione rilevata del telefono cellulare può variare fra poche decine di metri fino a qualche centinaio di metri.



Il ricevitore programmabile multibanda: Icom ICR2500



Il ricevitore programmabile multibanda: AoR 3000

Per quanto riguarda i diffusissimi telefoni “cordless” casalinghi, è opportuno spendere due parole: questi apparecchi furono progettati negli anni '70 ma si dovette aspettare, in Italia, un decennio prima che rispondessero alle caratteristiche tecniche richieste dal gestore telefonico nazionale, che all'epoca era la SIP. La tecnologia era denominata CT1 ed attualmente non sono più usati (salvo rare eccezioni). Il passo successivo fu l'introduzione della tecnologia CT1+, il cui funzionamento è terminato, nel nostro paese, nel 2008.

Entrambi i sistemi trasmettevano in modo analogico e le frequenze usate erano intorno a 40 MHz, 49MHz e 72MHz, a seconda delle marche e dei modelli. Grazie al loro costo, tutto sommato non eccessivo, conobbero una enorme diffusione anche se le dimensioni del portatile li facevano annoverare fra i “laterizi”. Mattoni, insomma.

Intercettare le conversazioni dei pochi che ancora usano questi apparecchi è un gioco da ragazzi: qualsiasi ricevitore “scanner”, anche il più modesto, è in grado di captare le loro trasmissioni, quindi: riservatezza pari a zero! E questa è la “buona notizia”; la cattiva è che, usando un vecchio portatile modificato, è facile usare la vostra “base” per telefonare “aggratis”. Succede assai più spesso di quanto non si immagini! Questo spiega il mistero di bollette incomprensibilmente alte o con chiamate verso numeri internazionali mai effettuate dall'utente, per così dire “legittimo”.

Non sperate però di contestare eventuali chiamate verso atolli sperduti nel Pacifico , tipo Tuvalu, Vainatu ecc. I cordless di cui sto parlando non erano omologati, pertanto chi li ha acquistati ed usati lo ha fatto a proprio rischio. Lo so! sulla confezione non c'era alcun accenno a tale difformità con i modelli “regolari”, ma ciò non vale a giustificazione!

Ma c'è di peggio! Alcuni malfattori, stante la facilità odierna di leggere sul display di un moderno telefono il numero del chiamante, hanno pensato bene di usare una “base” telefonica altrui per le loro telefonate connesse con reati quali truffe o ricatti. Basta girare in macchina con un ricevitore scanner acceso e programmato per spazzolare sulle frequenze tipiche dei cordless di quella generazione, per individuare qualche base installata in negozi od uffici, (in provincia sono più numerose).

Si torna poi dopo l'orario di chiusura, (altrimenti il legittimo proprietario, usando il telefono, potrebbe scoprire l'intromissione) ci si parcheggia nel raggio di una decina di metri e si possono commettere tranquillamente ogni genere di reati “telefonici” certi dell'impunità.

Come riconoscere un cordless CT1 o CT1+ analogico? Facile: negli apparecchi moderni, di cui parlerò fra un momento, l'antenna trasmittente non c'è (o meglio, è interna, come molti cellulari) o, al massimo, è lunga un paio di centimetri. Se il vostro telefono ha un'antenna lunga 15/20 cm. o se è vecchio come il peccato, allora è un modello analogico. La soluzione? Una, sola e drastica: se avete un vecchio portatile analogico, aprite la pattumiera e, senza rimpianti, ponetelo delicatamente fra la “monnezza”!

Le cose vanno già meglio (ma solo di poco), con la moderna generazione di cordless con tecnologia DECT. Tale caratteristica è chiaramente scritta sulla confezione e sul libretto di uso (quando si tratta di pubblicizzare una tecnologia positiva i fabbricanti non sono mai avari di notizie). La modulazione usata è di tipo digitale e l'ascolto è fuori dalle capacità dei comuni “scanner”. La loro gamma di frequenze è intorno a 900MHz ma può arrivare, in alcuni modelli, fino a 1200MHz. Purtroppo però, una delle caratteristiche di questa tecnologia, connessa con la riduzione dei disturbi e del fruscio di fondo, prevede l'emissione, ogni pochi secondi, di un segnale radio che sincronizza la base con il portatile.

Nel caso della vecchia tecnologia analogica, quando il proprietario non usava il telefono (ossia quest'ultimo era in stand-by), nessun segnale tradiva la presenza dell'apparecchio quindi, chi girava con lo “scanner” acceso doveva sperare in una telefonata in corso per scoprirlo. Nel caso di un moderno DECT il segnale radio viene emesso, anche se brevemente, parecchie volte al minuto, quindi è più facile scoprire la presenza di questo telefono. Oltretutto, alcuni apparecchi di fascia economica non prevedono alcun sistema di criptazione del parlato né l'invio di codici per il riconoscimento fra la base ed il portatile. Ecco quindi che qualche tecnico, piuttosto “disinvolto”, ha pensato bene di modificare ad arte alcuni telefoni di questo livello per tornare alla caccia di linee telefoniche altrui.

La difesa, in questo caso, sta nello scegliere apparecchi dotati di codici criptati per il riconoscimento della base; in assenza del codice giusto, la linea telefonica non viene agganciata.

Rivolgetevi quindi, per l'acquisto, a negozi qualificati e fatevi consigliare da un commesso davvero competente! Infine, quando non usate il cordless, soprattutto in ore notturne, prendete la buona abitudine di staccare la spina connessa alla rete telefonica.

Un'ultima cosa, prima di tornare a parlare di microspie: è stata avanzata una proposta di modifica che prevede di disattivare l'irradiazione continua dei telefoni cordless DECT, anche se ciò equivale ad apportare delle modifiche sostanziali allo standard mondiale di questa tecnologia. Ciò allo scopo di contribuire al contenimento dell'inquinamento elettromagnetico di cui soffrono tanti agglomerati urbani. Le complicazioni tecniche non mancano e, se questa proposta non dovesse avere seguito, la vecchia tecnologia CT1+, di cui ho parlato prima, potrebbe essere mantenuta attiva ben oltre il 2008, in attesa di un'alternativa al sistema DECT. Con grande gioia dei furbacchioni che continueranno a poter telefonare "aggratis".

Le microspie di seconda generazione:

Come abbiamo visto, esistono limitazioni tecniche ben precise, relative al microfono, che rendono le intercettazioni ambientali tutt'altro che semplici. Questo non è il solo problema; ne esiste un altro, non meno complesso, relativo alla propagazione delle onde radio.

Qualsiasi dispositivo radiotrasmittente ha bisogno di un'antenna, ossia del mezzo per inviare nell'etere le onde radio. La dimensione fisica delle antenne è direttamente proporzionale alla lunghezza d'onda, e inversamente proporzionale alla frequenza sulla quale si vuole trasmettere: perciò, più alta è quest'ultima, più piccola può essere l'antenna. Nel caso di cui sto trattando, la dimensione delle microspie deve essere il più contenuta possibile, per ovvi motivi di occultabilità. Di conseguenza, dovendo ridurre al massimo anche la lunghezza dell'antenna, si opta per frequenze di trasmissione molto elevate, tipicamente nel campo delle microonde.

Questa gamma di frequenze presenta la caratteristica di consentire lunghe portate ottiche del segnale pur usando basse potenze di emissione, il che è l'ideale per un dispositivo che deve usare pile di dimensioni minime, e quindi di capacità contenuta.

Purtroppo le caratteristiche di propagazione delle onde ultracorte risentono fortemente della presenza di ostacoli. Infatti, quando nelle caratteristiche tecniche di un trasmettitore si indica la portata, ci si riferisce sempre a quella "ottica" ossia all'assenza di ostacoli interposti fra il trasmettitore e l'apparecchio ricevente.

Ben difficilmente una microspia potrà soddisfare questa condizione ottimale poiché, dovendo essere nascosta con grande ocultezza per non essere rinvenuta casualmente e posizionata in modo da captare facilmente le parole pronunciate nell'ambiente spiato, quasi sempre verrà occultata in ambienti chiusi, magari circondati da strutture in cemento armato che, per loro natura, attenuano fortemente le onde radio.

Per aggirare queste limitazioni si usa parcheggiare, nelle immediate vicinanze del luogo ove è occultata la "cimice", un'automobile o un furgone al cui interno viene posto un ricevitore sintonizzato sull'emissione che interessa e collegato ad un registratore audio. Sarà così sufficiente recarsi periodicamente a prelevare il nastro registrato, o la scheda di memoria, nel caso di una registrazione digitale, per ottenere le informazioni desiderate senza esporsi eccessivamente.

Parecchi anni fa, ma erano tempi davvero pionieristici, per ascoltare il segnale delle "cimici" si usava una normale radio casalinga o un'autoradio dotata della gamma F.M., modificata in modo da estenderne la ricezione, che normalmente si trova fra gli 88 ed i 108 Mhz, portandola fino a 110 Mhz circa. Le microspie più economiche funzionavano in questo tratto di frequenze.

Purtroppo i normali radioricevitori non possiedono una sensibilità particolarmente elevata, essendo progettati per captare i segnali delle normali emittenti commerciali, che trasmettono con potenze rilevanti. Inoltre la vicinanza della gamma F.M., con le sue numerose stazioni radio, non di rado generava interferenze che "sommergevano" il debole segnale della "cimice" impedendone la ricezione.

Voglio ricordare anche che la "deviazione di frequenza", ossia la porzione di banda occupata da un singolo canale in un ricevitore F.M. commerciale è piuttosto larga, al fine di ottenere una qualità audio eccellente. Questo costringeva a "spalmare" su una porzione di spettro maggiore l'energia trasmessa dalla microspia quando invece, essendo già di per sé modesta, avrebbe dovuto essere sfruttata con la maggiore razionalità possibile.

Le microspie della generazione più recente trasmettono invece su gamme ben più elevate, superiori ai 300 Mhz e fino ai 900mhz e con deviazione di frequenza di soli 5 Khz contro i 75KHz delle emittenti commerciali. Questo tipo di modulazione, definita tecnicamente "FMN", ossia modulazione in frequenza a

banda stretta, dove "N" sta per narrow, ha consentito di realizzare microspie di alta efficienza capaci di "concentrare", per così dire, tutta l'energia trasmessa in una porzione di banda assai piccola.

Sia chiaro comunque che, a dispetto di tutti i progressi tecnici, la portata di questi trasmettitori in miniatura non supera, nell'uso pratico, i cento/duecento metri, poiché la peculiarità dell'autonomia delle batterie è sempre, giustamente, preponderante su quella della potenza d'emissione.

Naturalmente per l'ascolto di queste microspie è stato necessario realizzare appositi ricevitori il che, pur se eleva sensibilmente il costo dell'insieme, consente di pervenire ad un funzionamento affidabile e "professionale", poiché tali ricevitori sono dotati di sensibilità elevatissima e di alta "selettività", ossia la capacità di non subire interferenze da trasmissioni su canali adiacenti a quello in uso.



Un ricevitore portatile per microspie: Icom IC-R20

Ancora una cosa: tuttora possiamo leggere, su alcune riviste, la pubblicità di "cimici" dal costo modestissimo ascoltabili tramite una comune radio casalinga. Alla luce di quanto detto sinora, possiamo annoverare, senza mezzi termini, tali microspie fra le classiche **"bufale"**.

Le microspie dell'ultima generazione

Se volgiamo lo sguardo al recente passato, non possiamo che rimanere colpiti dai progressi inarrestabili, oserei dire "esponenziali", della tecnologia elettronica. Ad esempio, il computer con il quale sto scrivendo questo articolo, poco più di un anno fa era al top delle caratteristiche del settore e aveva un costo adeguato. Oggi si può trovare a meno della metà del prezzo originale, in mezzo a mostri dell'informatica che hanno velocità operative e dimensioni della memoria di massa più che triplicate. Un computer costruito solo sei/sette anni fa viene considerato come risalente al medioevo e non interessa nessuno, nemmeno in regalo.

Le microspie non hanno avuto un'evoluzione altrettanto eclatante, certamente a causa del fatto che la richiesta del mercato non è così elevata come altri apparecchi di largo consumo. Di conseguenza le grandi industrie elettroniche non hanno investito in ricerche su questo particolare dispositivo, lasciando il campo libero a numerose aziende, spesso di dimensioni poco più che artigianali, le quali hanno solo applicato le ricadute tecnologiche di altri settori.

Durante l'esposizione annuale sulle tecniche e sui prodotti per gli investigatori tenutasi recentemente a Washington D.C. ho potuto vedere lo "stato dell'arte", per così dire, delle tecnologie relative.

Nei più recenti modelli di microspie si è incominciato ad abbandonare la trasmissione analogica per passare a quella digitale, realizzando anche dispositivi stereofonici. Il vantaggio di questi ultimi è chiaro:

superare i problemi legati al riverbero che si produce ascoltando, attraverso un microfono, le persone che parlano in un certo ambiente, fornendo all'ascoltatore quel senso di direzionalità spaziale che manca in un sistema monofonico, consentendogli di concentrare l'attenzione verso un punto della stanza piuttosto che verso un altro. Queste soluzioni tecniche, se da un lato limitano leggermente la miniaturizzazione delle microspie che adottano tali recenti miglione, dall'altro esaltano la fedeltà di riproduzione che la trasmissione in digitale permette di raggiungere, paragonabile a quella di un compact-disc, contribuendo così ad aumentare la chiarezza e la comprensibilità di quanto captato. Qualora le intercettazioni ambientali costituissero una delle prove richieste dal magistrato incaricato di una indagine, è palese che l'univocità delle parole registrate è condizione essenziale per lasciare poco spazio ad interpretazioni postume troppo disinvolute da parte dell'indagato.

Al momento dell'ascolto, esistono dei dispositivi chiamati "processori audio", che possono lavorare al massimo delle proprie possibilità quando elaborano un segnale audio digitale, piuttosto che quando sono alle prese con un segnale analogico, tagliando via i rumori estranei alla conversazione che interessa ed esaltandone la comprensibilità in modo impressionante.

Se con queste metodologie si tenta di porre rimedio ai limiti del microfono, altre innovazioni si incaricano di superare i problemi legati alla portata del segnale radio. Le novità, sotto questo aspetto, non mancano: un recente modello di "cimice" lancia il suo segnale, che può anche essere nella banda dell'infrarosso anziché in quella delle microonde, verso un piccolo ponte radio posto nelle immediate vicinanze. Quest'ultimo poi si incarica di ritrasmettere, dopo opportuna amplificazione, alla stazione ricevente che, in tal modo, può essere posta anche a notevole distanza. A tutto vantaggio della riservatezza che in queste azioni di intercettazione è fondamentale e dell'autonomia delle batterie che, grazie alla piccolissima potenza di trasmissione necessaria, può aumentare sensibilmente.

Microtelecamere collegate con un telefono cellulare WAP possono trasmettere le immagini captate da un capo all'altro del pianeta, attivandosi solo dopo un ordine trasmesso attraverso la rete di telefonia cellulare. Web-cam collegate ad internet possono essere telecomandate, brandeggiate su due assi, asservite al movimento delle persone nell'ambiente in modo da inquadrare sempre in modo ottimale le persone spiate. Oggetti supertecnologici a prezzi, tutto sommato, abbastanza abbordabili. Molto più di quanto Orwell abbia mai immaginato nei suoi peggiori incubi.

I processori audio

Come abbiamo già avuto modo di vedere, non di rado l'intercettazione ambientale consente di registrare voci e discorsi assai poco comprensibili, vuoi perché nell'ambiente dove era situata la microspia vi erano più persone che parlavano contemporaneamente, vuoi perché le voci erano disturbate da rumori di varia origine. Si è così posto il problema di come filtrare il segnale utile, depurandolo da tutti i disturbi e migliorando il cosiddetto rapporto S/N (signal/noise).

Un dispositivo costruito a tale scopo è il "processore di segnale audio", del quale ho accennato poc'anzi, o "signal processing": si tratta di un apparecchio contenente una serie di filtri attivi passa-banda e arresta-banda, regolabili, gestiti da un microprocessore, aventi il fine di eliminare quei rumori che, non rientrando nella gamma della voce umana, provocano solo un decadimento della qualità audio a svantaggio della comprensibilità della parola.

Le frequenze acustiche della voce umana si estendono in una banda compresa fra un minimo di 300 Hz ed un massimo di 3000 Hz. In queste frequenze rientrano sia le note squillanti del gentil sesso che le note gravi dei bassi. Inoltre la forma d'onda della voce, che in gergo tecnico si definisce "involuppo", possiede delle caratteristiche peculiari che ben la caratterizzano. Se ascoltiamo una registrazione audio inquinata da rumori di fondo, echi, rimbombi che la rendono poco intelligibile, possiamo migliorarne enormemente la comprensibilità sottoponendola ad uno o più passaggi attraverso il processore audio che, se manovrato da mani esperte, potrà eliminare o attenuare consistentemente tali disturbi.

L'azione del microprocessore poi, farà qualcosa di ancor più fine, riconoscendo le caratteristiche dell'involuppo della voce ed eliminando drasticamente quelle forme d'onda che, non rientrando nelle figure memorizzate, saranno individuate e cancellate. Ovviamente il processore audio non può fare miracoli e pertanto non potrà superare i limiti imposti dalle leggi dell'acustica.

Spiare le telefonate e gli SMS di un cellulare

Esistono almeno due modi per trasformare un qualsiasi telefonino in un'eccellente spia ambientale.

Il primo consiste nell'inviare alla potenziale vittima uno speciale SMS contenente un apposito file; qualcosa di molto simile a un virus informatico. È però necessario che il destinatario apra l'SMS in questione perché il "malware" si installi automaticamente e all'insaputa della vittima.

Da quel momento, quando lo "spione" lo richiederà con un apposito codice di chiamata, il telefonino risponderà con un SMS contenente gli ultimi numeri e i messaggi, completi di testo, chiamati o ricevuti, dalla persona spiata.

Ovviamente nessun indizio segnalerà alla vittima quanto sta succedendo: il telefonino non s'illuminerà né emetterà alcun rumore né segnalerà la ricezione dell'SMS spia.

Come difendersi dunque? Per una volta la cosa non è particolarmente difficile: l'SMS di richiesta, inviato dallo "spione", deve contenere alcuni caratteri speciali, come per esempio il simbolo di cancelletto, l'asterisco e alcuni punti interrogativi. Insomma, è formattato in un modo tipico e, se fosse letto, non avrebbe alcun significato logico.

Sappiamo però che il sistema operativo del telefonino "vittima" è infiltrato dal "malware" in modo da non mostrare mai il testo incriminato. Basta però trasferire la scheda SIM in un altro telefonino sicuramente "pulito" e, quando riceveremo l'SMS che richiede i dati da spiare, vedremo magicamente apparire lo strano testo sul display, completo del numero chiamante! (a meno che lo "spione" non abbia attivato la funzione che nasconde tale numero).

Trasformare un telefonino in spia ambientale

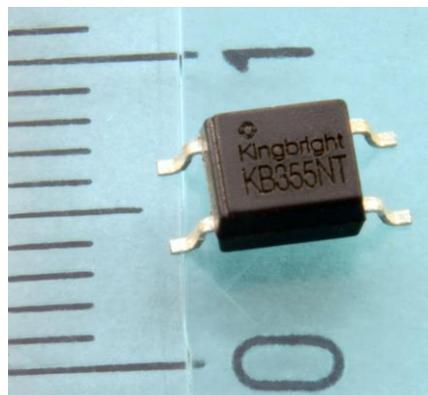
Il secondo sistema per trasformare un qualsiasi telefonino, purché dotato di avvisatore di chiamata a vibrazione, in una sofisticata spia ambientale, prevede lo smontaggio dell'avvisatore e l'installazione, al suo posto, di uno speciale circuito integrato opto-isolatore Darlington reperibile in internet per pochi spiccioli.

I terminali n. 1 e 2 dell'integrato vanno saldati sui contatti del vibro, gli altri due vanno collegati al tasto verde di risposta del cellulare: certo, occorre avere una buona manualità e dimestichezza con il saldatore a stagno per elettronica, stante gli spazi ridottissimi disponibili all'interno dei moderni telefonini.

Successivamente, dal menù del telefonino occorre selezionare la voce "risposta automatica con ogni tasto" e attivare la sola vibrazione, eliminando la suoneria (risposta silenziosa).

Infine, sarà necessario regolare a minimo il volume dell'altoparlante e coprire il display con del nastro adesivo per evitare che al momento della chiamata s'illumini, tradendo la sua presenza.

Tutto qui! Ora, chiamando il telefonino da qualsiasi parte del mondo, si potrà ascoltare tutto quanto viene detto nelle sue vicinanze.



Un circuito integrato utilizzabile per trasformare un normale telefono cellulare in spia ambientale. Si notino le piccolissime dimensioni

Le microspie GSM e i localizzatori GPS

Le moderne microspie hanno ampiamente sfruttato i progressi tecnologici nel campo delle telecomunicazioni e non solo. È il caso delle “cimici” che usano la rete telefonica cellulare per trasmettere a distanze virtualmente illimitate i loro segnali.

Si tratta di dispositivi che si differenziano da un normale telefonino solo per l'assenza di alcuni elementi che sarebbero inutili e inutilmente ingombranti. Ad esempio, il display la tastiera, l'altoparlante e la suoneria ecc.

Tuttavia, pur se ridotte all'essenziale, le microspie GSM sono estremamente efficienti, tanto da occupare gradualmente il posto delle “cimici” di tipo classico, quelle di cui abbiamo trattato sinora.

Un'importante caratteristica delle microspie GSM, dal punto di vista della bonifica, è la loro difficile individuazione con i normali strumenti, siano questi dei misuratori di campo o analizzatori di spettro o altro.

Queste “cimici”, infatti, trasmettono solo quando ricevono una chiamata dall'esterno, dal cellulare usato per spiare. Di norma, le microspie GSM sono “silenti” ad eccezione di quei modelli progettati per attivarsi automaticamente alla presenza di voci o rumori.



Una microspia GSM con la sua scheda SIM

Il problema quindi consiste nella impossibilità di individuare un segnale radio quando non c'è! Come fare, dunque, quando si ha ragione di sospettare la presenza di una spia GSM?

Il funzionamento del sistema telefonico cellulare richiede di conoscere la posizione di ogni telefonino attivo, allo scopo di poterlo raggiungere in seguito ad una chiamata. Per questo motivo, ogni terminale invia, a intervalli programmati, una stringa di dati contenente l'IMEI, ossia il “nome e cognome” univoco di quell'apparecchio, diverso per ogni telefonino sulla faccia della terra, il proprio numero, registrato sulla SIM, e altri dati essenziali al funzionamento del sistema.

Anche le microspie GSM si comportano in tal modo, tuttavia non è pensabile star lì, con gli strumenti accesi, in ascolto per un tempo indefinito, aspettando che la “cimice” si decida a lanciare il suo identificativo. Oltretutto non sapendo se la spia c'è effettivamente, se la sua batteria è esaurita ecc.

La soluzione ideale consiste nel costringerla ad attivarsi al nostro volere tramite un “jammer”. Si tratta di un dispositivo in grado di generare un radiodisturbo, chiamato “rumore bianco” su tutte le frequenze usate dai telefonini, ma anche dai satelliti GPS e dai router Wi-Fi.

Se la microspia GSM si trova nel raggio di azione del “jammer”, perde il segnale della cella telefonica per tutto il tempo che lo strumento è in funzione. In seguito, non appena il jammer viene spento, la “cimice” si attiva lanciando il suo segnale di riconoscimento verso la cella telefonica più vicina e ne attende la risposta.

Se in questo breve momento teniamo acceso l'analizzatore di spettro, vedremo apparire un picco di segnale completo della relativa frequenza e intensità. Lo stesso se stiamo usando un misuratore di campo elettromagnetico.

Nota: In Italia gli Art. 340, 617 e 617 bis del Codice Penale puniscono l'uso e l'installazione per scopi fraudolenti dei Jammer, perché potenzialmente in grado di interrompere un pubblico servizio come quello delle comunicazioni telefoniche cellulari.

Un altro dispositivo in grado di trasmettere i propri segnali a qualunque distanza, sfruttando la rete telefonica cellulare, per segnalare la propria posizione geografica con un'approssimazione di pochi metri, è il "GPS Tracker" o localizzatore satellitare GPS.

In un contenitore poco più grande di un telecomando apri cancello sono inseriti un navigatore satellitare e, appunto, un telefono cellulare, completi delle rispettive antenne.



Un "GPS Tracker", con la sua batteria al litio

L'installazione su un'automobile è semplicissima e veloce. Infatti, il "GPS Tracker" è dotato di un potente magnete al neodimio, per cui basta appoggiarlo sotto il pianale metallico della vettura perché rimanga in posizione, senza pericolo che si distacchi e vada perduto.

Chiamando da un telefono cellulare "smartphone" il numero della scheda SIM inserita nell'apposito alloggiamento del "GPS Tracker", si riceve un SMS contenente le coordinate geografiche del punto in cui si trova il dispositivo.

A questo punto, collegandosi ad internet e accedendo a Google-maps (<http://maps.google.it/>) o, meglio, a Google Earth (<http://www.google.com/earth/>), scaricando il software gratuito e inserendo i dati ricevuti con l'SMS, il sistema restituisce la posizione geografica del "GPS Tracker" inserita in una delle mappe di Google con una precisione semplicemente impressionante.

Il software di controllo del localizzatore satellitare permette inoltre una serie di opzioni estremamente utili: ad esempio, si può programmare con facilità il dispositivo per farlo rimanere in stand-by finché la macchina controllata è parcheggiata, aumentando così in modo considerevole l'autonomia della batteria al litio del localizzatore, che può arrivare a superare i quindici/venti giorni.

Non è tutto: il localizzatore, oltre a inviare i dati su richiesta, può anche inviarli autonomamente a intervalli programmabili, ad esempio, ogni quindici minuti.

Con queste caratteristiche, il dispositivo può essere usato come un moderno sistema antifurto, installandolo all'interno dell'automobile sotto il pianale posteriore e collegandolo con la batteria dell'auto. In questo modo l'autonomia dell'alimentazione è virtualmente illimitata. Anche se una macchina fosse rubata e nascosta in un box o in un garage dove non arrivano i segnali del sistema satellitare GPS, sarà sempre possibile seguirne il percorso, visualizzando l'ultima posizione utile, che può anche essere molto vicina al luogo dove è parcheggiata.

Naturalmente, se l'uso del localizzatore satellitare GPS come antifurto è perfettamente lecito, lo stesso non si può dire quando fosse usato per spiare le persone poiché ciò contrasta con gli stessi articoli del codice penale, menzionati nell'appendice alla fine di questa monografia, a proposito delle "cimici" ambientali.

Alcuni segnali premonitori d'intercettazione

A tutti può capitare, pur senza essere paranoici, di sentirsi spiati.

Ebbene, quali potrebbero essere i segnali premonitori che dovrebbero metterci sull'avviso e farci valutare, serenamente e senza esagerazioni, la realistica dei nostri sospetti o delle nostre sensazioni e considerare la possibilità di prendere contatto con un tecnico esperto in bonifiche ambientali da microspie:

- Avete rilevato tracce di estranei che sono entrati nella vostra proprietà ma nulla è stato rubato/asportato
- Veicoli sospetti sono spesso parcheggiati nei pressi dei vostri locali/della vostra proprietà
- Si sono presentati tecnici, idraulici/termici o della società elettrica/telefonica, per interventi di manutenzione e/o riparazione mai richiesti
- Persone estranee al vostro ambiente di lavoro o familiare, sono a conoscenza di vostre notizie riservate o segrete o dei vostri spostamenti o impegni
- Alcuni vostri documenti aziendali, progetti, preventivi di appalto riservati, sono a conoscenza di terzi, non autorizzati
- Avete notato suoni, rumori insoliti o variazioni improvvise di volume, nella vostra linea telefonica
- Avete sentito suoni dalla cornetta del telefono mentre questa era agganciata
- Il vostro impianto TV o stereo presentano improvvisamente strane interferenze
- Vi è stato regalato, o è apparso ingiustificatamente nei vostri locali, un oggetto d'arredo (radiosveglia, orologio da tavolo, calcolatrice, portapenne ecc.)
- Avete notato spostamenti di placche di prese/interruttori, scatole di derivazione elettrica, cornici, griglie di aereazione, apparecchi telefonici ecc.
-

Qualora abbiate notato uno o più di questi segnali premonitori, è possibile che siate oggetto d'intercettazione telefonica/ambientale.

In tal caso, valutata la realistica dei vostri sospetti, anche in relazione al vostro lavoro o a recenti "disavventure coniugali", se decidete di prendere contatto con un tecnico, specialista nella ricerca di microspie, non parlatene all'interno dei locali sospettati ma chiamate da un telefono pubblico esterno ai locali stessi.

Qualora, in seguito a ciò, concorderete un intervento di bonifica, chiedete che sia eseguito esclusivamente alla vostra presenza o di persona da voi delegata. Chiedete inoltre la compilazione di una lettera d'incarico, con valore di contratto di lavoro tra le parti, completa di preventivo di spesa.

Molti tecnici, seri e qualificati, sono disponibili a effettuare interventi anche in orari serali, festivi e prefestivi per consentirvi la necessaria segretezza nei confronti di vostri eventuali dipendenti. È un ottimo modo di procedere, decisamente consigliabile, anche se farà lievitare il costo della bonifica.

Le contromisure: un campo riservato ai professionisti

Il segnale radio emesso da una microtelecamera nascosta e dotata di trasmettitore è più facilmente rilevabile, da parte di un esperto dotato delle opportune strumentazioni, per almeno due motivi. Il primo è la banda di radiofrequenza occupata da un segnale video, enormemente più ampia di quella di un segnale audio, a causa dell'informazione molto più complessa che il primo segnale contiene rispetto al secondo.

Un segnale audio, infatti, può anche contenere solo un tratto della banda vocale, magari con fedeltà "telefonica", ossia molto ridotta, pur conservando una sufficiente comprensibilità. Un segnale video, invece, deve trasmettere delle informazioni molto più complesse comprendenti, per esempio, il segnale che serve a mettere in sincronia il monitor usato per la ricezione, al fine di produrre immagini non distorte. Deve trasmettere anche informazioni relative alla luminosità, al colore, ove questo sia necessario, e tutto il complesso involuppo dell'immagine.



*Analizzatori di spettro a radiofrequenza e misuratori dell'intensità di campo elettromagnetico.
Apparecchi elettronici usati per la bonifica da microspie*

Il secondo motivo che facilita l'individuazione del segnale di una telecamera è dato dalla maggiore potenza che tale emissione deve avere per poter produrre nel ricevitore una immagine "leggibile" ossia chiara e con sufficiente risoluzione.

Insomma, un'impronta radio più ampia e più intensa sarà più facilmente captata dagli analizzatori di spettro radio o dai misuratori dell'intensità di campo elettromagnetico, di cui si avvalgono gli specialisti in bonifiche ambientali.

Molto più difficile è la loro opera quando si ha a che fare con una microspia audio, poiché la limitata potenza di emissione e la ristretta banda radio occupata, non facilitano di certo la ricerca della loro presenza, inoltre i modelli più sofisticati adottano il circuito VOX, ossia un dispositivo che interrompe automaticamente la trasmissione quando nell'ambiente non vi sono voci.

Adottato per consentire l'economizzazione dell'energia delle pile di alimentazione, il VOX costringe l'esperto in bonifica ambientale ad effettuare la ricerca tenendo una radio accesa a medio volume in modo da essere sicuro dell'attivazione della eventuale "cimice".

L'enorme numero di canali radio utilizzabili dalle microspie dell'ultima generazione, rende necessario, per la loro individuazione, l'uso di sofisticati radiorecettori "scanner" capaci di spaziare fra i 100 Mhz ed i 3

Ghz ed oltre. Chiaramente, una ricerca effettuata su uno spettro così vasto presenta non poche difficoltà tecniche, per cui l'operatore deve possedere una abilità professionale ed una esperienza davvero fuori dal comune. Infatti l'attuale elevatissimo numero delle emissioni radiofoniche costituisce una forma di inquinamento elettromagnetico dal quale è tutt'altro che agevole estrarre ed isolare il piccolo segnale della microspia.

Si tratta insomma di un campo nel quale non vi è assolutamente spazio per il "fai da te".

Cercare e individuare un'eventuale microspia, che ovviamente sarà stata accuratamente nascosta, non è cosa facilissima. È fondamentale operare con metodo razionale, non affidandosi al caso o a una ricerca empirica, improvvisata o, peggio, tirando a indovinare. Il rischio è di non individuare il dispositivo e, di conseguenza, dare al cliente una falsa sicurezza che lo spingerà a parlare liberamente, senza il timore di essere intercettato, con le implicazioni che è facile immaginare.

Naturalmente i metodi usati dai tecnici di bonifica sono svariati e non è detto che l'uno sia migliore dell'altro; molto dipende dal tipo di strumentazione usata e, certamente, dal punto di vista strettamente personale, nonché dall'esperienza.

L'importante è informarsi preventivamente al fine di evitare i "praticoni" del ramo che, spinti dalla possibilità di un facile guadagno e muniti di strumentazioni piene di lucine lampeggianti e bip-bip, più adatte a un videogame che non a una prestazione professionale, tentano di abbindolare le persone inesperte facendo danni, anziché risolvere problemi.

Per terminare queste righe, voglio accennare ad un recente dispositivo per l'ascolto delle conversazioni che avvengono in un ambiente, che non rende necessario accedere, neppure per breve tempo, al locale da controllare, al fine di occultare una microspia. Si tratta di un apparato che sfrutta le caratteristiche di un raggio laser nella banda della radiazione infrarossa, pertanto al di fuori del visibile, che viene puntato contro il vetro della finestra del locale ove avviene la conversazione. Le vibrazioni acustiche del vetro della finestra, causate dalle voci all'interno della stanza, modulano il raggio laser che viene riflesso dalla superficie del vetro stesso, con un angolo eguale a quello incidente. Tale raggio viene ricevuto da un'apposita apparecchiatura, posta in posizione opportuna, che, demodulando il segnale audio, ne estrae l'informazione contenuta.

Successivamente, tale segnale deve essere filtrato tramite un processore di segnali, al fine di eliminare tutti quei fattori di disturbo, come per esempio il rumore del traffico automobilistico, che ne diminuirebbero la comprensibilità. Ovviamente il costo di un apparato così sofisticato è del tutto allineato con le prestazioni che è in grado di offrire. Per di più, il suo uso è decisamente complesso tanto da richiedere l'impiego di personale specializzato: ad esempio, se il raggio laser venisse puntato dalla strada verso una finestra posta, poniamo, al secondo o terzo piano, a causa delle leggi ottiche che prevedono, come dicevo prima, angoli complementari fra il raggio incidente e quello uscente, l'emissione laser verrebbe riflessa verso il cielo rendendone impossibile la ricezione.

In Italia, a quanto mi risulta, l'apparato di cui sopra è usato, attualmente, solo dai corpi speciali della Polizia di Stato, dall'Arma e... dagli immancabili "Servizi".

Appendice

Implicazioni legali sull'uso degli apparati di intercettazione e/o registrazione.

È a tutti noto che anche l'autorità di Polizia, qualora nello svolgimento delle indagini debba effettuare una intercettazione telefonica o un ascolto ambientale, deve essere preventivamente autorizzata dalla magistratura che valuta, per ogni singolo caso, l'opportunità di concedere o meno tale autorizzazione.

Come già scritto all'inizio, l'uso troppo "disinvolto" di microspie o di apparati di registrazione audio o video, può comportare la violazione di precise norme del Codice Penale. Ritengo pertanto utile pubblicare un estratto di tali norme al fine di palesare le implicazioni legali connesse.

Art. 614. Violazione di domicilio

Chiunque si introduce nell'abitazione altrui, o in un altro luogo di privata dimora, o nelle appartenenze di essi, contro la volontà espressa o tacita di chi ha il diritto di escluderlo, ovvero vi s'introduce clandestinamente o con inganno, è punito con la reclusione fino a tre anni. Alla stessa pena soggiace chi si trattiene nei detti luoghi contro l'espressa volontà di chi ha diritto di escluderlo, ovvero vi si trattiene clandestinamente o con inganno. Il delitto è punibile a querela della persona offesa. La pena è da uno a cinque anni, e si procede d'ufficio, se il fatto è commesso con violenza sulle cose, o alle persone, ovvero se il colpevole è palesemente armato.

Art. 615 bis. Interferenze illecite nella vita privata

Chiunque, mediante l'uso di strumenti di ripresa visiva o sonora, si procura indebitamente notizie o immagini attinenti alla vita privata svolgentesi nei luoghi indicati nell'articolo 614, è punito con la reclusione da sei mesi a quattro anni. Alla stessa pena soggiace, salvo che il fatto costituisca più grave reato, chi rivela o diffonde mediante qualsiasi mezzo d'informazione al pubblico le notizie o le immagini, ottenute nei modi indicati nella prima parte di questo articolo. I delitti sono punibili a querela della persona offesa; tuttavia si procede d'ufficio e la pena è della reclusione da uno a cinque anni se il fatto è commesso da un pubblico ufficiale o ad un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o servizio, o da chi esercita anche abusivamente la professione d'investigatore privato.

Art. 617. Cognizione, interruzione o impedimento illeciti di comunicazioni o conversazioni telegrafiche o telefoniche

Chiunque, fraudolentemente prende cognizione di una comunicazione o di una conversazione, telefoniche o telegrafiche, tra altre persone o comunque a lui non dirette, ovvero le interrompe o le impedisce è punito con la reclusione da sei mesi a quattro anni. Salvo che il fatto costituisca più grave reato, la stessa pena si applica a chiunque rivela, mediante qualsiasi mezzo di informazione al pubblico, in tutto o in parte, il contenuto delle comunicazioni o delle conversazioni indicate nella prima parte di questo articolo. I delitti sono punibili a querela della persona offesa; tuttavia si procede d'ufficio e la pena è della reclusione da uno a cinque anni se il fatto è commesso in danno di un pubblico ufficiale o di un incaricato di un pubblico servizio nell'esercizio o a causa delle funzioni o del servizio, ovvero da un pubblico ufficiale o da un incaricato di un pubblico servizio con abuso dei poteri o con violazione dei doveri inerenti alla funzione o servizio, o da chi esercita anche abusivamente la professione d'investigatore privato.

Art.617bis Installazione di apparecchiature atte ad intercettare od impedire comunicazioni o conversazioni telegrafiche o telefoniche

Chiunque, fuori dei casi consentiti dalla legge, installa apparati, strumenti, parti di apparati o di strumenti al fine d'intercettare od impedire comunicazioni o conversazioni telegrafiche o telefoniche tra altre persone è punito con la reclusione da uno a quattro anni. La pena è della reclusione da uno a cinque anni se il fatto è commesso in danno di un pubblico ufficiale nell'esercizio o a causa delle sue funzioni ovvero da un pubblico ufficiale o da un incaricato di un pubblico servizio con abuso dei poteri o con violazione dei doveri inerenti alla funzione o servizio o da chi esercita anche abusivamente la professione di investigatore privato.

Per saperne di più

“Le microspie ambientali e telefoniche; caratteristiche tecniche e metodologie di bonifica”



Una approfondita descrizione delle microspie classiche e dell'ultima generazione. Quali le loro caratteristiche e quali i limiti tecnici? Quanto è facile spiare le nostre telefonate e come ci possiamo difendere? Come si svolge una bonifica da microspie?

Il libro risponde a tutte queste domande, entrando nei dettagli del funzionamento elettronico delle microspie e delle radio trasmissioni in generale, pur rimanendo ad un livello semplice, divulgativo e alla portata di tutti.

130 pagine, 32 foto, tabelle e disegni tecnici a colori.

ISBN : 2120010456272 € 27,50

La pubblicazione è distribuita nella catena di librerie Feltrinelli ed in tutte le principali librerie, anche virtuali (Amazon, Ibis, Google ecc.) È inoltre possibile acquistarlo direttamente dall'autore scrivendo a: infotiscali@claudio-ballicu.it oppure studiotecnicoballicu@gmail.com

È disponibile anche in formato PDF visualizzabile su computer e tablet.

© Copyright 2014 Claudio Ballicu, Tutti i diritti riservati

Torna alla Home Page: <http://www.claudio-ballicu.it>