Claudio Ballicu

Le microspie ambientali e telefoniche

Caratteristiche tecniche e metodologie di bonifica

Elaborazione grafica: *Simon Mago*

Le microspie ambientali e telefoniche

Caratteristiche tecniche e metodologie di bonifica

Un’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?

Progetto grafico, copertina, ricerche iconografiche, disegni e foto di Claudio Ballicu

Edizione digitale PDF del gennaio 2014

Indice

Nota importante
da leggere con attenzione
prima di proseguire:

Gli utilizzi impropri di alcune delle informazioni contenute in questo libro, potrebbero portare alla violazione della Legge 8 aprile ‘74 n. 98, artt. 615bis, 617, 617bis, c.p. e della Legge 226 c.p.p. sulla riservatezza della vita privata e sulle intercettazioni delle comunicazioni, nonché della Legge n. 675 del 31/12/96 sulla raccolta dei dati personali e sul diritto alla privacy.
L’autore declina ogni responsabilità sull'eventuale uso illecito delle informazioni fornite. Infatti, questo libro 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 come è possibile difendersi da queste intrusioni nella sfera del privato, e non vuole essere in alcun modo 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.: I dispositivi descritti e/o fotografati, presenti in questa monografia, sono di proprietà dell’autore, non sono in vendita e hanno il solo scopo di chiarire l’argomento di cui trattasi. I relativi fabbricanti e/o distributori, non sono in nessun modo collegati economicamente con l’autore della presente monografia.

Profilo biografico dell'autore

Claudio Ballicu è nato a Roma nel 1949, dove vive e lavora. È perito in elettronica industriale e telecomunicazioni e laureato in Scienze dell'Investigazione.
È autore di pubblicazioni nel campo della meccanica serraturiera e delle casseforti, del misterioso settore dello spionaggio elettronico e dell'indagine sulle cause di incendio, sulla rivista del settore "Force-Security".
Ha tenuto seminari sul tema della ricerca di tracce forensi nelle serrature sottoposte ad apertura clandestina nelle università di Aquila e Camerino e sulle tecniche di bonifica da microspie, presso la Facoltà di Giurisprudenza e presso la Facoltà di Informatica dell'Università di Camerino e presso la facoltà di Scienze della Formazione dell'Università di Macerata.

Oggi, effettua perizie forensi e consulenze nel campo serraturiero-casseforti e dei dispositivi elettronici anticrimine per il Tribunale di Roma, ove è iscritto dal 2005 nelle liste dei Consulenti Tecnici del Giudice, e per privati e compagnie

assicurative.

Si occupa, inoltre, di tecnologie di ricerca e bonifica di microspie ambientali e/o telefoniche e localizzatori satellitari GPS e di tutto quanto concerne la sicurezza della vita privata.

È autore e curatore del sito internet www.perizieforensi.com, ricco di notizie sul mondo delle microspie, della sicurezza anticrimine e della protezione da intrusioni negli archivi dei dati digitali aziendali.

Collabora, su tutto il territorio nazionale, con importanti Studi Legali effettuando consulenze tecniche e indagini difensive (art.11, legge 7 dicembre 2000, n. 397).

Premessa

In Italia le attività di intercettazione telefonica, ambientale, telematica e informatica, sono rigidamente disciplinate dal Codice di Procedura Penale e consentite alla sola Autorità di Polizia Giudiziaria, eventualmente con la collaborazione del gestore telefonico, su provvedimento motivato del Pubblico Ministero che deve preventivamente richiedere l'autorizzazione al Giudice per le Indagini Preliminari secondo il dispositivo di cui all'art. 266 del c.p.p. (*Intercettazioni di conversazioni o comunicazioni*).

L'autorizzazione può essere concessa, secondo i limiti di ammissibilità contenuti nello stesso dispositivo (comma 1, da lettera A a F-bis e comma 2), con decreto motivato, solo in presenza di gravi indizi di reato, solo quando l'intercettazione sia assolutamente indispensabile ai fini della prosecuzione delle indagini e solo per un periodo di tempo limitato (circa quarantacinque giorni, rinnovabili su richiesta, anch'essa motivata).

A tutto ciò si può, parzialmente, derogare nei soli casi di urgenza: *"Quando vi è fondato motivo di ritenere che dal ritardo possa derivare grave pregiudizio alle indagini".*

In tali evenienze, il P.M. può disporre direttamente questo mezzo di ricerca della prova, con decreto motivato che va comunicato immediatamente, e comunque non oltre le ventiquattro ore, al Giudice per le Indagini Preliminari il quale, entro quarantotto ore dal provvedimento, decide, con decreto motivato, sull'eventuale convalida. Se la disposizione del P.M. non viene convalidata, l'intercettazione deve essere immediatamente interrotta, i suoi risultati non possono essere utilizzati e devono essere distrutti.

1. Il diritto alla riservatezza della vita privata

Il Garante per la Protezione dei Dati Personali è l'organo che ha, fra l'altro, il potere di eseguire dei controlli, anche su richiesta degli interessati, sul trattamento dei dati personali effettuato dalle forze di Polizia o dai Servizi di Informazione e di Sicurezza.

Alcune persone si dicono favorevoli alle misure di sorveglianza generalizzata sostenendo che "*m'intercettino pure, se non sto facendo niente di male, non ho nulla da nascondere*", rispondendo in tal modo a chi sostiene l'inviolabile diritto alla privacy.

A costoro basterebbe ricordare gli artt. 2, 14 e 15 della Costituzione Italiana, gli artt. 7 e 8 della Carta dei Diritti Fondamentali dell'Unione Europea e l'art. 12 della Dichiarazione Universale dei Diritti dell'Uomo.

In uno Stato di Diritto è ragionevole aspettarsi che siano controllati i criminali, non i liberi cittadini.

Inoltre, basti pensare alle intercettazioni abusive telematiche e/o informatiche, capaci di fornire a criminali molto ben organizzati, dati sensibili sulle nostre carte di credito o sui codici delle nostre transazioni bancarie effettuate al computer o alle intercettazioni connesse con lo spionaggio industriale, capaci di vanificare in un attimo anni di ricerche e investimenti per arrivare a un brevetto o di insinuarsi, fraudolentemente, nelle offerte di gare d'appalto, per comprendere l'esistenza, e la necessità, degli appositi articoli del Codice Penale che perseguono gli autori di simili reati.

Per terminare questo primo capitolo, voglio spendere due righe per parlarvi di "Super Amanda".

Si tratterebbe, il condizionale è d'obbligo, dell'offerta che Telecom avrebbe fatto al Ministero della Giustizia, proponendo, a fine 2006 un servizio centralizzato finalizzato alle intercettazioni.

Una specie di "Echelon" in versione "spaghetti & pummarola"? Più che di "Grande Fratello" si dovrebbe dunque parlare di una

non meno invasiva “Grande Sorella”!

All’intervista del settimanale L’Espresso all’allora Garante della Privacy on. Stefano Rodotà, alle notizie pubblicate dal quotidiano La Repubblica e a quelle reperibili su Punto Informatico hanno fatto seguito le nette smentite della società diretta interessata.

Tuttavia, se prendiamo in esame quanto afferma l’Istituto Internazionale Max Planck, un ente pubblico tedesco di ricerca scientifica che collabora, in svariati campi di studio, con molte università, anche italiane, il nostro paese occupa il primo posto nella “*Hit-Parade*” delle intercettazioni in Europa con la bellezza di settantadue intercettazioni ogni centomila abitanti. Il Ministero della Giustizia conferma che le intercettazioni in Italia sono salite dalle 32mila del 2001 alle 107mila del 2005! A conti fatti siamo sulla media di circa 1.500.000 intercettazioni l’anno.

Bisogna ammettere comunque che la cronica carenza nell’organico delle Forze dell’Ordine nel “Bel Paese” spinge i magistrati a preferire l’installazione di una “cimice” o l’intercettazione di una linea telefonica alla disposizione di appostamenti e pedinamenti.

Resta tuttavia il fatturato Telecom Italia che, per il solo settore riguardante le intercettazioni richieste dai P.M. si aggira sui 15 milioni di euro/anno, pertanto non c’è da sorprendersi se un simile flusso di denaro può spingere a un salto di qualità del fenomeno, con buona pace dell’equilibrio tra le esigenze investigative e il rispetto del diritto alla privacy dei cittadini sottoposti a intercettazione.

2. Le possibilità di intercettazione

I moderni dispositivi elettronici per le intercettazioni telefoniche, ambientali, telematiche e informatiche consentono, non solo teoricamente, a chiunque sia dotato di un minimo di manualità e di conoscenze tecniche anche superficiali, di effettuare con facilità e a costi contenuti, delle intercettazioni.
Anche coloro che non avessero la benché minima dimestichezza con questa tecnologia, possono facilmente trovare qualche tecnico, troppo disinvolto, disponibile a effettuare per loro conto tale incombenza.

Quando parlo di "disinvoltura", mi riferisco al fatto che le intercettazioni, ambientali, telefoniche o telematiche che siano, se abusive, sono perseguite da precise sanzioni del Codice Penale (vedi l'appendice al termine di questo libro), oltre a essere, ovviamente, del tutto inutilizzabili in ambito processuale.

Fino a non molti anni addietro, il costo di una microspia professionale, a differenza di quelle classificabili a livello di "bufala", era a dir poco proibitivo.

Oltre alla microspia vera e propria, infatti, occorreva fornirsi di apparecchi radio appositamente progettati per ricevere le loro frequenze, invero un po' "speciali" e dotati della necessaria sensibilità per far fronte alle basse potenze di emissione proprie di questi dispositivi spionistici.

Al contrario, le microspie a basso costo, poco più che giocattoli, trasmettevano su frequenze ascoltabili con una comune radio o autoradio FM, allo scopo di evitare l'acquisto, e la spesa, di un ricevitore dedicato.

Purtroppo una comune autoradio è progettata per ascoltare trasmissioni commerciali che, di norma, sono emesse con potenze rilevanti, allo scopo di coprire una vasta area geografica e non

hanno bisogno quindi di una sensibilità eccessivamente spinta. Inoltre la selettività, ossia la capacità di separare due emissioni con frequenze vicine tra loro, non ha ragione di essere troppo elevata.

Diversamente da ciò, un ricevitore dedicato all'ascolto delle microspie, o anche un "radio scanner", nasce per ricevere segnali anche debolissimi e/o adiacenti ad altre emissioni di potenza ben maggiore. Quindi la selettività di questi apparati deve essere molto elevata, con conseguente incremento della complessità circuitale e, in ultima analisi, del costo finale.

Oggi le cose sono alquanto cambiate: le ricadute tecnologiche dovute, principalmente, allo sviluppo della telefonia cellulare e dell'informatica, hanno permesso un abbattimento dei costi, anche per gli speciali ricevitori denominati "radio scanners", tali da mettere le microspie alla portata di quasi tutte le tasche.

Modificare un telefono cellulare per trasformarlo in una spia ambientale attivabile da qualunque distanza è un'operazione abbastanza semplice e, tutto sommato, anche poco dispendiosa (vedi cap.14.1). Unica condizione: il telefonino deve essere dotato dall'origine di avvisatore a vibrazione, un dispositivo presente in quasi tutti gli apparecchi.

A questo punto, sorge spontanea una domanda: quanto è lontana la società del "Grande Fratello"? Quanto controlla ogni nostra singola azione?

3. Quanto è privata la nostra privacy?

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 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, secondo la 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 poterlo raggiungere con una chiamata in arrivo.

Meno essenziale, almeno dal punto di vista tecnico, 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, registrano 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 siano usati per….." in calce ai tanti moduli per la richiesta d'informazioni, di

iscrizioni o di acquisti a distanza, che passano per le nostre mani, e sarete 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 devono 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 è largamente approssimativa!

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 assolutamente 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 sceglie l’alimentazione tramite la rete elettrica, sopportandone le relative difficoltà d’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 e nonostante le microspie di elevata qualità siano dotate di circuito VOX.

Si tratta di un sistema elettronico che mette la spia in stand-by quando non ci sono voci nell'ambiente intercettato, per riattivarla non appena il microfono percepisce dei rumori.

In tal modo, pur non risolvendone alla radice le limitazioni, viene economizzata l'energia della pila di alimentazione con un considerevole incremento della sua durata efficace.

4. La miniaturizzazione dei circuiti

Diciamo subito che i progressi più clamorosi 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 a indicare che tutti i circuiti sono inseriti nello stesso contenitore, delle dimensioni di pochi mm^2, e il numero di componenti realizzati sulla piastrina di silicio che ne costituisce il cuore, delle dimensioni di $1mm^2$, ha largamente superato, al giorno d'oggi, un numero di elementi semplici con cifre a sei zeri, cosa che, sino a pochi anni fa, sembrava un livello d'integrazione irraggiungibile.

La nuova 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.

È 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 di 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 "preistoriche" pile allo zinco/carbone degli anni cinquanta, alle alcaline, poi alle pile al mercurio, all'argento e successivamente alle moderne nickel/cadmio ricaricabili o alle

nickel/mercurio/idrogeno fino a quelle agli ioni di litio, attualmente le più efficienti, derivate dagli studi nel campo della telefonia cellulare.

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 "bottone", 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.

Nella seguente fig.1, che mostra una scheda nella quale convivono i semiconduttori "classici" insieme con i più recenti, possiamo vedere un circuito integrato in tecnologia S.M.D. a paragone con uno della "vecchia generazione". La moneta da 10 cent. fornisce un'idea delle dimensioni.

La successiva fig.2 mette a confronto la grandezza di un transistor e di un resistore in tecnologia S.M.D. con quelle degli omologhi componenti realizzati con la "vecchia tecnologia". La differenza dimensionale è evidente.

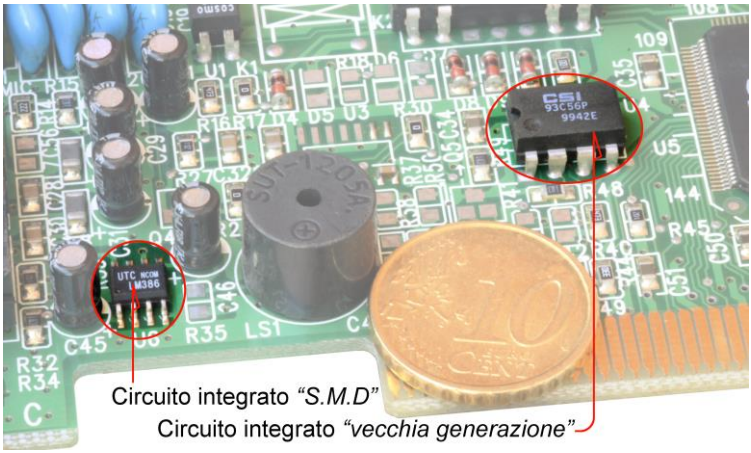

Fig.1

Un circuito integrato S.M.D. a confronto con la "vecchia" generazione

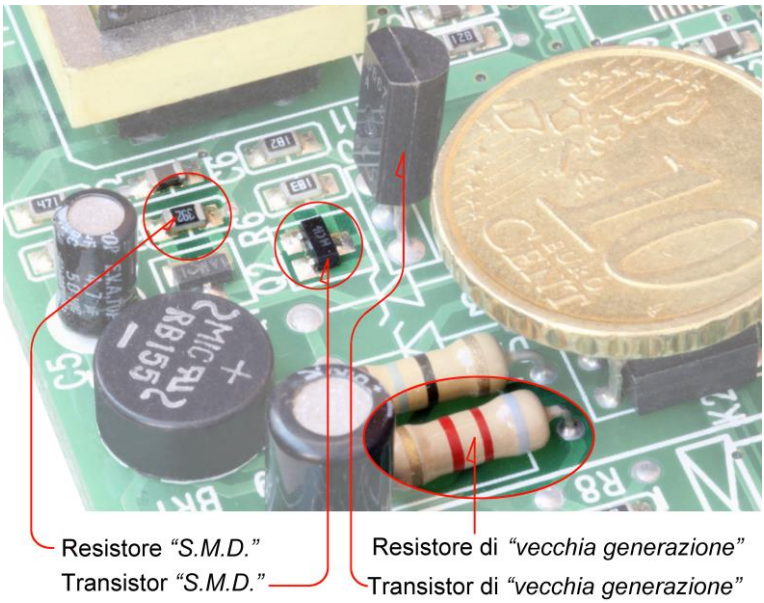

Fig.2

Un transistor e un resistore S.M.D. a confronto con la "generazione" precedente.
La moneta fornisce un'idea delle dimensioni

5. Un po' di tecnologia

Questo non è, né vuole essere, un testo di elettronica. Tuttavia, nei capitoli che seguono, pur volendo rimanere a un livello semplice e divulgativo, si dovranno usare alcuni termini tecnici riguardanti il mondo dell'elettronica e delle radiocomunicazioni. Sarà quindi necessario avvicinarsi un minimo a questi argomenti, al fine di comprenderne il significato.

Poiché parleremo diffusamente di onde radio, cominciamo col vedere cosa è un'onda:

In natura le onde, che sarebbe più esatto chiamare "moto ondulatorio", hanno una grande varietà di forme: le increspature sulla superficie di uno stagno dove è caduto un sasso e che si allargano a cerchio a partire dal punto d'inizio o le onde acustiche, che si propagano nell'aria esattamente alla stessa maniera, pur risultando invisibili.

Perfino la luce non è altro che un'onda di tipo elettromagnetico, capace di propagarsi a distanze indefinite e, poiché non comporta un'oscillazione di molecole d'aria, può attraversare anche il vuoto assoluto dello spazio cosmico.

Un'onda non è qualcosa di localizzato, ma è diffusa in tutta una regione dello spazio ed è formata da creste e avvallamenti che si spostano a una determinata velocità.

Prendiamo ancora l'esempio dell'onda in uno stagno: se mettiamo un sughero a galleggiare sulla superficie lo vedremo ballonzolare su e giù, spinto dalle onde che lo investono, ma non lo vedremo spostarsi nella direzione delle onde stesse.

Dunque, non c'è un movimento complessivo dell'acqua in quella direzione! L'onda non trascina con sé della materia anche se, indubbiamente, è un movimento oscillatorio, in questo caso di un liquido, ma trasferisce energia cinetica alle molecole che incontra davanti a sé.

La distanza massima, rispetto alla posizione media, alla quale

sale e scende il sughero è detta “ampiezza dell’onda” mentre il numero di oscillazioni al secondo è detto “frequenza”.

Un terzo importante parametro, la distanza fra due creste consecutive (o fra due avvallamenti, che è lo stesso), è detta “lunghezza d’onda”.

Abbiamo così definito, mi pare con grande semplicità, tre parametri fondamentali di qualunque moto oscillatorio, compreso quello proprio delle onde radio.

Naturalmente, quando parliamo di onde radio, stiamo descrivendo una forma particolare di moto oscillatorio che definiamo “spettro elettromagnetico”, costituito da pura energia interessata da una rapida e ripetuta inversione della polarità.

6. La corrente alternata

Al contrario della corrente continua, che è un flusso di elettroni lungo un conduttore, sempre nella medesima direzione, dal polo negativo verso quello positivo, la corrente alternata ha un carattere oscillatorio e varia continuamente e periodicamente tra un valore massimo positivo e un valore massimo negativo, invertendo il proprio verso.

Una corrente alternata può avere varie forme d'onda, ma qui prenderemo in considerazione solo quella sinusoidale, della quale possiamo riconoscere alcuni parametri che avevamo già considerato nell'esempio delle onde nello stagno:

- La **frequenza**, ossia il numero di oscillazioni complete dell'onda in un secondo. La sua unità di misura è l'Hertz (Hz) con i suoi multipli kilohertz (KHz = migliaia di Hz), Megahertz (Mhz = milioni di Hz) Gigahertz (GHz = miliardi di Hz) ecc.

- La **lunghezza d'onda**, ossia la distanza fra due punti corrispondenti di due creste successive. La sua unità di misura è il metro (m) con i suoi multipli e sottomultipli.

- L'**ampiezza**, ossia la distanza massima da picco a picco, della cresta della semionda positiva alla cresta della semionda negativa. La sua unità di misura è il volt (V) con i suoi multipli e sottomultipli.

La frequenza e la lunghezza d'onda sono inversamente proporzionali fra loro, ossia, se la frequenza aumenta, la lunghezza d'onda diminuisce e viceversa.

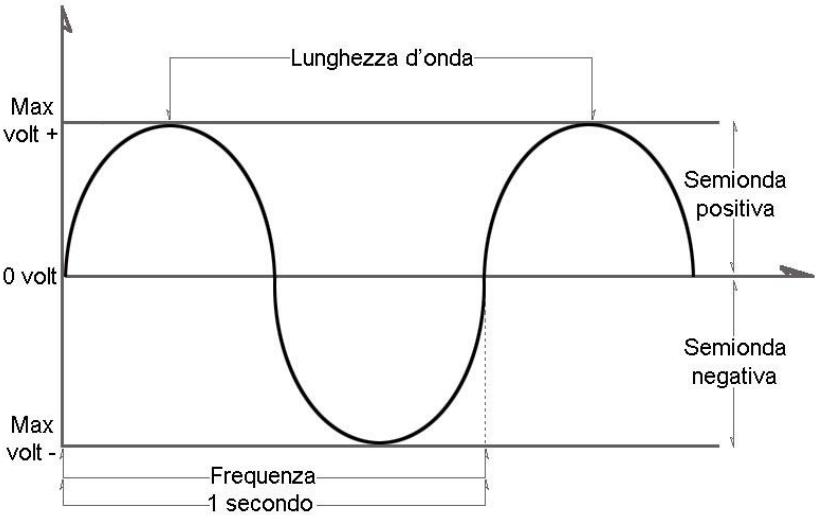

Fig.3

Un'onda sinusoidale con frequenza di 1 Hertz

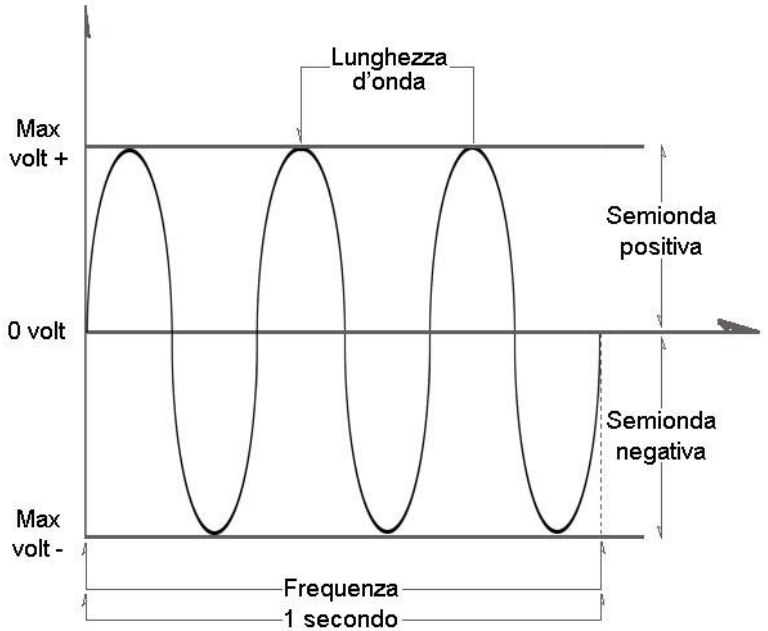

Fig.4

Un'onda sinusoidale con frequenza di 3 Hertz

La lunghezza d'onda è tre volte minore della sinusoide di fig.3

La cosa è più facile da capire, osservando le figg.3 e 4 che rappresentano appunto una corrente alternata: ipotizziamo che la frequenza sia di un Hertz. Un ciclo, ossia una sinusoide, si completerà in un secondo.

Se ipotizziamo che la frequenza sia di 3 Hertz, in quello stesso spazio di tempo (un secondo) vedremo tre sinusoidi complete.

Chiaramente la lunghezza d'onda, ossia lo spazio fra due creste, sarà tre volte minore. La frequenza è aumentata, la lunghezza d'onda è diminuita!

7. Cosa è un'onda radio

La corrente alternata, dunque, varia continuamente e ciclicamente nel tempo da un valore massimo a un minimo.

Ebbene: la legge di Faraday ci dice che, quando in una regione dello spazio un campo elettrico varia rapidamente nel tempo, viene indotto (ossia nasce "spontaneamente") un campo magnetico, perpendicolare al campo elettrico variabile che l'ha prodotto. L'intensità di questo campo magnetico è direttamente proporzionale alla rapidità (ossia alla frequenza) con cui varia il flusso del campo elettrico.

Questo enunciato è alla base della teoria delle onde elettromagnetiche, formate cioè, contemporaneamente, da un campo elettrico e da un campo magnetico strettamente correlati e interdipendenti, come rappresentato schematicamente nella seguente fig.5

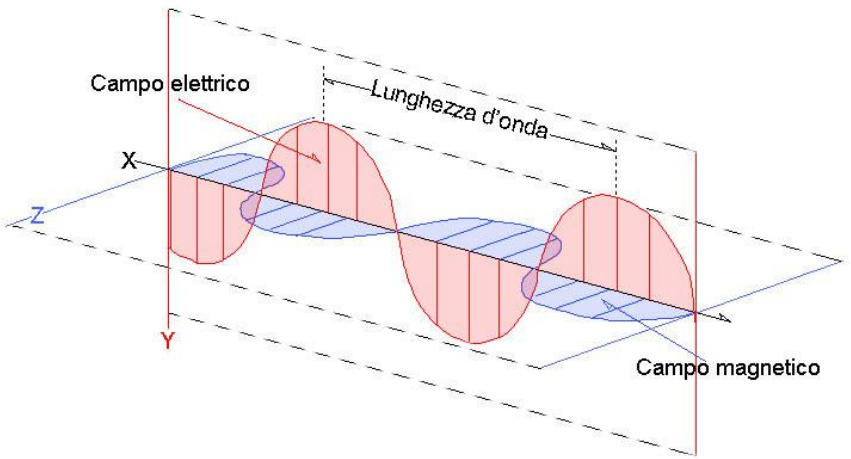

Fig.5

Rappresentazione schematica di un'onda elettromagnetica

Ebbene, un'onda radio è esattamente questo: un campo elettromagnetico variabile che ha la proprietà di propagarsi nello spazio e, poiché non è costituito da particelle in movimento, ma è un'oscillazione di energia allo stato puro, si propaga anche nel vuoto cosmico esattamente come la luce (che è anch'essa un'onda elettromagnetica pura).

Un'onda elettromagnetica assume vari aspetti, e produce vari effetti, a seconda della sua frequenza. Nella parte più bassa troviamo le onde radio, che partono dalle onde lunghissime e lunghe per salire gradualmente alle onde medie, alle corte, alle cortissime fino alle microonde. In questa gamma di frequenze ci sono quelle che fanno funzionare il nostro telefonino.

La potenza impiegata nei telefonini è abbastanza modesta, tuttavia sono in corso studi scientifici per stabilire la pericolosità per la salute di tali microonde che, essendo appunto di frequenza elevatissima, possiedono intrinsecamente una notevole energia.

Ancora più alta è la frequenza di lavoro dei forni a microonde, quindi tanto maggiore l'energia di tali onde elettromagnetiche, che riescono, infatti, a cuocere i cibi in pochi minuti.

Anche la luce non è altro che un'onda elettromagnetica, esattamente come un'onda radio, solo di frequenza enormemente maggiore, formata da una parte visibile, che noi percepiamo appunto come luce. Lo spettro delle frequenze che la compongono viene da noi visto come gamma di colori.

C'è anche una parte che non possiamo vedere: la luce infrarossa, che appartiene alla parte più bassa dello spettro luminoso e che noi percepiamo come onde termiche, ossia calore.

L'enunciato di Faraday afferma inoltre che l'intensità di un campo elettromagnetico è direttamente proporzionale alla sua frequenza. Infatti, lo spettro di frequenze più alte della luce sono i raggi ultravioletti A e B che hanno energia sufficiente a interagire con le cellule epiteliali del nostro corpo stimolando la produzione di una sostanza difensiva che serve a proteggerci da questa

Sigla	Banda di frequenza	lunghezza d'onda
VLF Very Low Frequen.	3 ÷ 30 KHz	100 Km÷10 Km
LF Low Frequencies	30 ÷300 KHz	10Km ÷ 1 Km
MF Medium Frequen.	300 ÷ 3000 KHz	1 Km ÷ 100m
HF High Frequencies	3 ÷ 30 MHz	100 m ÷ 10 m
VHF Very High Frequen.	30 ÷ 300 MHz	10 m ÷ 1 m
UHF Ultra High Frequen.	300 ÷ 3000 MHz	1 m ÷ 10 cm
SHF Super High Frequen.	3 ÷ 30 GHz	10 cm ÷ 1 cm
EHF Extra High Frequen.	30 ÷ 300 GHz	10 mm ÷ 1mm
Microwaves	300 ÷ 3000 GHz	1 mm ÷ 0,1 mm

Fig.6

La gamma delle onde radio, divisa per bande
e con le relative sigle

energia: la melanina, che è direttamente responsabile della tanto gradita abbronzatura.

Salendo ancora di frequenza, e quindi di energia relativa, troviamo i raggio X, poi i raggi cosmici , le radiazioni gamma ecc. Come vedete, più è alta la frequenza maggiore è la pericolosità delle radiazioni elettromagnetiche che, a partire dal limite dell'ultravioletto e a salire, sono definite "radiazioni ionizzanti".

Torniamo alle nostre onde radio con una tabella (fig.6) che le divide per bande di frequenza, dalle onde lunghissime alle microonde.

Le sigle che indicano queste bande, fra parentesi nelle caselle di sinistra, saranno usate d'ora in avanti per indicare le frequenze di lavoro delle microspie di cui parleremo.

8. La modulazione

Immaginiamo di premere il tasto di trasmissione in un walkie-talkie, senza parlare nel microfono: otterremo l'emissione di un'onda elettromagnetica, ossia di un'onda radio, che definiamo "portante".

Per intenderci, possiamo paragonare una "portante" a un treno che viaggia da una stazione a un'altra, senza trasportare merci né passeggeri. Si sposterà fisicamente lungo i binari, partendo e arrivando regolarmente ma… non servirà in pratica a nulla, non compiendo il lavoro per cui è stato costruito: il trasporto di cose o persone.

Bene: un segnale radio non modulato, pur partendo da un trasmettitore e potendo essere ricevuto a distanza, non trasporta nessuna informazione utile.

Osserviamo ora lo schema a blocchi in fig.7: abbiamo un amplificatore audio, collegato a un microfono e un generatore di portante, ossia una parte circuitale di un trasmettitore. Questi due dispositivi fanno capo a un circuito detto "modulatore", dove la parte a radiofrequenza (la portante) e la parte audio vengono "miscelate" fra loro.

In queste condizioni la parte audio va a "modulare" la parte radiofrequenza in maniera tale che successivamente, nel ricevitore, possano essere separate tra loro prelevando la sola parte audio che, opportunamente amplificata, può essere udita in altoparlante.

Nella realtà le cose sono leggermente differenti, e anche più complesse, ma questo libro non ha la pretesa di essere un testo di elettronica e telecomunicazioni, pertanto gli esempi riportati sopra assolvono sufficientemente lo scopo.

Nella realtà le cose sono leggermente differenti, e anche più complesse, ma questo libro non ha la pretesa di essere un testo di elettronica e telecomunicazioni, pertanto gli esempi riportati sopra assolvono sufficientemente allo scopo.

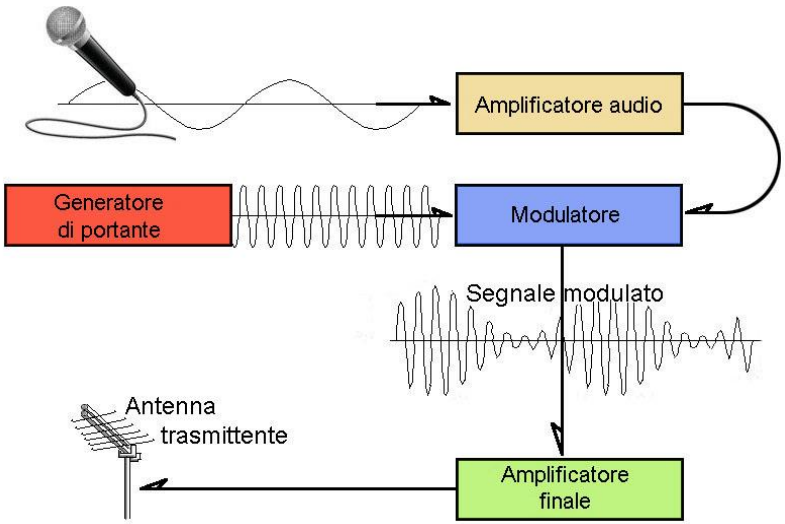

Fig.7
Schema a blocchi di un circuito modulatore

Devo solo precisare che esistono diversi sistemi per modulare una portante ossia, in definitiva, per sovrapporci un'informazione utile. Possiamo modulare in ampiezza (AM), in frequenza (FM), in fase (PM) o con modulazione impulsiva (PAM), ecc. per quanto riguarda le modulazioni analogiche. Esistono poi vari sistemi di modulazione numerica o digitale che prenderemo brevemente in considerazione parlando delle microspie funzionanti in gamma cellulare GSM ecc.

Nell'esempio di fig.7 è presa in considerazione, per semplicità, la modulazione d'ampiezza (AM) ma, nella maggior parte dei casi, le microspie sono modulate in frequenza (FM), grazie al miglior rendimento di questo sistema, alla maggiore fedeltà audio possibile e alla minore larghezza della banda occupata.

9. La lunghezza fisica dell'antenna

Questo capitolo potrà sembrare superfluo ma, come vedremo più avanti, nella ricerca pratica delle microspie, cioè nella bonifica, la conoscenza di questo parametro ci permetterà di restringere enormemente il campo di ricerca facilitandoci il compito e accorciando in misura significativa i tempi necessari.

La lunghezza di un'antenna trasmittente deve essere in rapporto matematico con la lunghezza d'onda, un po' come la corda di una chitarra che, pizzicata, produce la nota (e quindi la frequenza) corrispondente. Un'antenna può essere lunga quanto un'onda intera, o anche ½ d'onda o ¼ d'onda ecc.

Un'antenna, in realtà, è costituita da due parti: una metà "radiante" e un'altra di bilanciamento. È, infatti, formata da un dipolo. In questo dipolo scorrono la corrente e la tensione a radiofrequenza, sfasate tra loro di 90 gradi.

I punti dove la corrente o la tensione raggiungono il loro massimo si chiamano "ventri", dove invece raggiungono lo zero, si chiamano "nodi". A noi interessano proprio i ventri di corrente, perché sono questi i punti adatti per collegare la parte finale di un trasmettitore.

Collegandosi al centro di questo dipolo, risonante con la frequenza emessa, in corrispondenza con un ventre di corrente, si ha il migliore accoppiamento d'impedenza fra le parti e, in definitiva, il migliore trasferimento di energia elettromagnetica.

Come si calcola la lunghezza di un'antenna? Basta applicare una formuletta matematica semplicissima:

lunghezza in metri = 300.000/Frequenza in kilohertz (oppure 300/megahertz, che è lo stesso).

Incidentalmente, ricordo che 300.000 rappresenta la velocità della luce (e delle onde elettromagnetiche) nel vuoto.

Procedendo in senso inverso, ossia conoscendo la lunghezza fisica dell'antenna, possiamo risalire alla sua frequenza di

risonanza con la formula:

frequenza in kilohertz = 300.000/lunghezza in metri oppure: frequenza in megahertz = 300/lunghezza in metri.

Normalmente le antenne commerciali sono costruite con una lunghezza fisica di mezz'onda e con la presa per il cavo coassiale (ossia per l'alimentazione) nella loro metà e cioè a 1/4 d'onda, poiché qui troviamo che l'impedenza dell'antenna è molto prossima ai 52 o 75 Ohm dei cavi coassiali normalmente usati.

Ricordiamocelo, poiché ne riparleremo nel cap. 20, "Le frequenze maggiormente utilizzate" e ci sarà estremamente utile nelle operazioni di bonifica da microspie per restringere il campo di ricerca, facilitandoci notevolmente il compito.

Anche le onde stazionarie rivestono una grande importanza in un trasmettitore, e quindi anche nelle microspie di cui ci stiamo occupando.

10. Le onde stazionarie

Immaginiamo di avere una corda legata a un'estremità, di tenere nella mano l'estremità opposta e di farla oscillare. Vedremo formarsi un'onda che si propaga lungo la corda.

Ogni volta che l'onda giunge a un estremo, viene riflessa e capovolta e l'onda risultante è data dall'interferenza tra le onde incidenti e riflesse.

Più precisamente, possiamo affermare che il moto di un punto della corda è il risultato della sovrapposizione di due onde: una progressiva ed una regressiva.

Le onde stazionarie sono oscillazioni che, riflettendosi ripetutamente in una zona limitata di spazio, interferiscono tra loro e sono inoltre generatrici di particolari frequenze di risonanza dette "*armoniche"*.

L'effetto pratico, ai fini della comprensione dell'utilità di un'antenna che abbia una lunghezza fisica in rapporto matematico con la lunghezza d'onda è che, nel caso di perfetta risonanza, tutta l'energia elettromagnetica verrà irradiata nello spazio ottenendo il massimo rendimento.

Nel caso opposto, in un'antenna non perfettamente accordata, parte dell'energia verrà riflessa verso il generatore (quindi verso lo stadio finale di trasmissione) trasformandosi in energia termica secondo il primo principio della termodinamica (legge di conservazione dell'energia).

Quindi, non solo avremo un minor rendimento del

trasmettitore, ma anche un surriscaldamento dello stadio finale che, ove si superassero le sue possibilità di dissipazione termica, andrebbe distrutto.

Nel caso specifico di una microspia, che ha una potenza di trasmissione abbastanza modesta, è evidente la priorità imprescindibile di irradiarla totalmente per ottenere la massima portata del segnale.

Inoltre, nel caso di microspie alimentate a batteria, avremo la necessità di sfruttare al meglio la limitata fonte di energia trasformandola in radiofrequenza e non già sprecandola in calore.

L'analizzatore di parametri d'antenna MFJ-259B

11. Alcuni segnali premonitori d’intercettazione

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

In questo capitolo esamineremo, a grandi linee, quali possono essere i segnali premonitori che dovrebbero metterci sull’avviso e farci valutare, serenamente e senza esagerazioni, la realisticità 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 sono soggetti a 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, 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 realisticità 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.

Chiedete che sia compiuto un sopralluogo per verificare la planimetria dei locali e la tipologia dell'impianto telefonico. Tenete a portata di mano una planimetria dei locali.

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.

12. Dalla teoria alla pratica: le operazioni di bonifica

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.

In queste pagine illustrerò il mio metodo personale, evitando accuratamente di criticare altri approcci che potrebbero essere altrettanto validi. Scopo di queste pagine, infatti, è fornire al lettore le cognizioni necessarie per individuare i "praticoni" del ramo, spinti dalla possibilità di un facile guadagno e muniti di strumentazioni piene di lucine lampeggianti e bip-bip più adatti a un videogame che non a una prestazione professionale.

12.1 La ricognizione visiva

Il primo passo da compiere consiste dunque, per quanto possa essere sorprendente, in una semplice ricognizione visiva dei locali. Alcune microspie, infatti, soprattutto quelle più economiche ma non per questo meno efficaci, possono essere occultate dentro oggetti di uso talmente comune da passare del tutto inosservate.

Radiosveglie, mouse di computer, penne a sfera (funzionanti), (figg.8a, b, c), orologi da parete o da tavolo (fig.9), persino attaccapanni! possono nascondere l'insidia.

Pertanto, una prima ricognizione, effettuata da un esperto, può rapidamente individuare una di queste microspie, generalmente di fabbricazione orientale e dall'aspetto ben conosciuto.

Volete un esempio? Una semplice vite di chiusura di una scatola di derivazione elettrica o telefonica, può raccontare all'occhio esperto molto più di quanto si potrebbe supporre: in genere queste viti sono imbiancate o pitturate insieme alla parete nella quale sono incassate. Se la vernice è incrinata, possiamo sospettare un recente smontaggio del coperchio per occultare una microspia, approfittando della rete elettrica o della corrente telefonica per alimentarla indefinitamente aggirando in tal modo i limiti delle batterie.

Fig.8a
Una penna dotata di micro-telecamera
(evidenziata nel cerchio rosso)

Fig.8b

Fig.8c

Una penna dotata di micro-telecamera (evidenziata nel cerchio rosso) e di scheda di memoria "micro-SD" in grado di registrare ore di filmati e/o centinaia di foto, anche se con una definizione piuttosto modesta.

Fig.9

Un orologio da scrivania con micro-telecamera nascosta (evidenziata nel cerchio rosso). È dotato di scheda di memoria interna in grado di memorizzare ore di filmati.

12.2 La misura dell'intensità di campo

Il passo successivo consiste nel misurare l'intensità di campo a radiofrequenza nel locale da bonificare, tramite il cosiddetto "spazzolone" (vedi figg.10 e 11), non dimenticando di confrontarlo con la situazione all'esterno. Questo perché al giorno d'oggi l'inquinamento elettromagnetico ha raggiunto livelli notevoli, tali da far rilevare segnali radio praticamente ovunque.

Gli onnipresenti segnali della telefonia cellulare, i vari dispositivi Wi-Fi e Bluetooth, le telecamere di sorveglianza wireless, i segnali delle radio e televisioni private ecc. sono inesorabilmente rilevati dai misuratori di campo, inducendoci a sospettare la presenza di una trasmissione radio dall'interno del locale che stiamo controllando.

Fig.10

Un misuratore dell'intensità di campo a radiofrequenza (il cosiddetto "spazzolone") capace di arrivare oltre i 3.000 MHz

Fig.11
Un misuratore dell'intensità di campo a radiofrequenza per misure fino a 13 GHz

Per queste ragioni dobbiamo sempre effettuare un confronto fra il campo a radiofrequenza esterno ai locali e quello all'interno poiché non è la sua presenza a essere determinante, ma un eventuale picco improvviso del segnale che indica la presenza di una trasmissione radio a breve distanza, di cui resta ovviamente da stabilire l'origine.

Insieme allo "spazzolone" è utile un frequenzimetro per campi ravvicinati, come ad esempio il "Digital Scout" della Optoelectronics (vedi fig.12), in grado di segnalare con una vibrazione la prossimità di un trasmettitore, indicandone anche la frequenza, con una fulminea analisi che dura meno di un secondo, spaziando da 10 MHz a 2.600 MHz.

Rivela senza problemi tanto i segnali analogici quanto i digitali, anche con impulsi RF (burst) più brevi 300 microsecondi e persino le futuristiche microspie che modulano in "frequency hopping" o "spread spectrum".

Inoltre, misura i livelli di segnale da -45dBm a -5dBm, una

funzione questa ideale per localizzare i trasmettitori nascosti, determinandone i livelli di potenza.

Una sua peculiarità, coperta da numerosi brevetti mondiali, è la capacità di interfacciarsi con i migliori ricevitori "scanners" tramite una presa RS232 permettendo l'ascolto immediato delle eventuali microspie.

Fig.12
Un frequenzimetro per campi ravvicinati Optoelectronics

12.3 L'analizzatore di spettro

Terminate queste prime indagini si può attivare un analizzatore di spettro, strumento principe in questi casi, insieme con un ricevitore panoramico.

Il primo strumento può "spazzolare" una determinata banda di frequenze, che deve essere programmata opportunamente, restituendo sullo schermo di un computer un diagramma contenente l'intensità dei segnali captati e rappresentati nel dominio delle frequenze. Un segnale elettrico, infatti, può essere

osservato fondamentalmente in due modi: nel dominio del tempo, con il tradizionale oscilloscopio, o nel dominio delle frequenze con l'analizzatore di spettro.

Un analizzatore di qualità, e purtroppo di costo adeguato, mostrerà, oltre ai picchi di segnale e alla loro ampiezza nel modo di misura preferito: decibel-milliwatt, microvolt/metro ecc. anche la loro frequenza, larghezza di banda e altre informazioni aggiuntive (vedi fig. 13).

Non solo le trasmissioni analogiche ma anche quelle con modulazione digitale, come ad esempio quelle del sistema cellulare, saranno mostrate, insieme alla relativa banda passante.

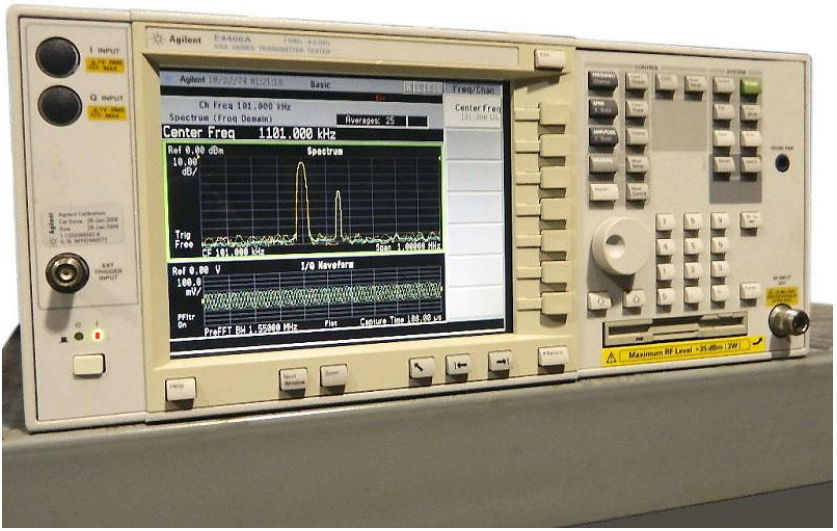

Fig. 13
La schermata dell'analizzatore di spettro da laboratorio Agilent

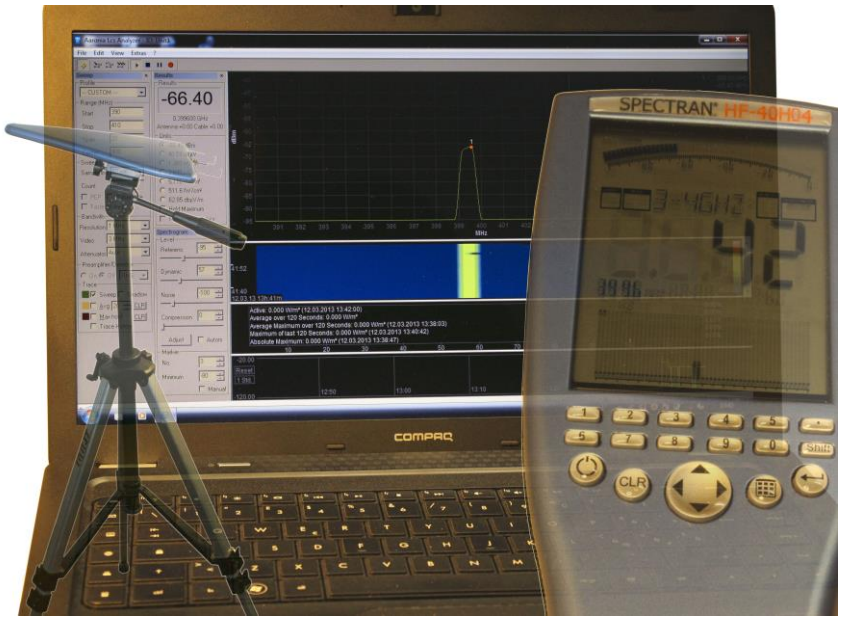

Fig. 14
L'analizzatore di spettro computerizzato Aaronia Spectran

Quando l'analizzatore è accoppiato a un'antenna a banda larga e moderatamente direttiva come per esempio una "log-periodic", potrà fornire anche indicazioni circa la direzione di provenienza del segnale, facilitando in modo determinante la ricerca dell'ubicazione della microspia.

È questo il caso del sistema portatile di analisi "Spectran" della Aaronia GMBH, (vedi fig. 14) importante azienda produttrice di strumenti di misura e di pannelli di schermaggio contro i campi elettromagnetici, con sede nell'area industriale di Euscheid, nel cuore della Germania.

12.4 Il ricevitore “scanner”

Un ulteriore strumento diagnostico è il ricevitore “scanner” multibanda, meglio se panoramico: si tratta di un apparecchio in grado di ricevere segnali dalle onde medie fino ad almeno 3 GHz nelle principali forme di modulazione. Ne possiamo vedere alcuni esempi nelle figg.15a, b, c.

Una volta individuato un segnale e la relativa la frequenza con l’analizzatore di spettro, si potrà sintonizzare con lo scanner per riceverlo direttamente, così da riconoscerne la natura: se stiamo effettivamente ascoltando la microspia o un segnale radiofonico o televisivo o una trasmissione proveniente da un dispositivo di telemisura e telecontrollo, come quelli usati dall’azienda del gas per il monitoraggio delle pressioni nella rete di distribuzione del metano, o del livello di fiumi o laghi o, infine, stiamo ricevendo segnali da radiomobili o walkie-talkie.

Fig.15a *ricevitore multibanda “scanner” AR-3000*

Fig.15b *ricevitore multibanda "scanner" Icom IC-R8500*

Fig.15c *Il complesso computerizzato di ricezione multibanda Icom PC-R-2500. Riceve da 10 kHz a 3300 MHz*

13. Alcuni limiti delle microspie ambientali

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 legato alla tecnologia delle microspie in commercio. Vi renderete così conto che non è per niente semplice spiare i discorsi che avvengono nel vostro ufficio, salvo che il "nemico" non abbia conoscenze tecniche di buon livello e usi dispositivi di ascolto abbastanza sofisticati.

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

Tuttavia, permane un limite tecnico non legato alla qualità della trasmittente quanto piuttosto a limiti fisici del microfono e dell'acustica: 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 e il cervello.

Infatti, anche se il livello delle voci intorno a noi ha un'intensità maggiore rispetto a chi ci parla, spostando istintivamente il capo selezioneremo con un orecchio ciò che ci interessa, passando da un ascolto binaurale a uno monoaurale. Il cervello farà il resto, con la sua straordinaria capacità di discriminazione, concentrando la nostra attenzione sulla voce dell'interlocutore e considerando tutto il resto come rumore di fondo.

Questo fenomeno, lungamente studiato alla ricerca delle sue basi fisiologiche, è conosciuto come “effetto cocktail party” e la capacità di separazione del segnale utile dal rumore di fondo è chiamata, tecnicamente, “capacità di segregazione”.

Nell’esempio precedente, contribuiscono alla comprensione del parlato anche altri fattori: la valutazione, del tutto inconscia, della distanza e dell’angolo di provenienza delle voci, la lettura, sia pur parziale, dei movimenti delle labbra, le caratteristiche fisiche delle voci dei parlanti come la prosodia ossia il ritmo, l’accentazione e l’intonazione del linguaggio.

Facciamo ora un esperimento d’altro genere: lasciamo un comune registratore acceso, in posizione "record" ovviamente, in una stanza dove più persone parlano animatamente.

Potremo costatare, riascoltando le voci incise, che i risultati, assolutamente deludenti, restituiranno un chiacchiericcio piatto e incomprensibile.

Le cause di una qualità di registrazione così bassa sono molteplici e poco influenzate dalle caratteristiche elettroniche 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 contribuirà a renderle meno comprensibili. Se uno degli interlocutori parla molto vicino al microfono o più persone discutono in modo animato, alzando il tono delle voci e parlando tutti contemporaneamente si avrà la saturazione dei circuiti di amplificazione del microfono superando i limiti delle sue possibilità di autocontrollo con la conseguenza che il parlato risulterà cupo, appiattito e privo dei toni acuti.

Infine, è bene ricordare che, nel parlato tra presenti, sono prodotti una serie di gesti tesi a chiarire il senso del discorso, attraverso la comunicazione non verbale: cenni di assenso o dissenso con il capo, gestualità, ammiccamenti, espressioni facciali, movimenti delle mani, servono ad aggiungere sottili

sfumature di significato con effetti comunicativi che si definiscono "paralinguistici".

Alcune espressioni facciali, come la perplessità, l'incredulità, forniscono agli interlocutori una sorta di "feedback" che integra, modifica e arricchisce la semplice comunicazione verbale.

Persino la postura del corpo trasmette, anche se a livello inconscio, segnali d'interesse o di noia o di rilassamento.

Tutte queste peculiarità "accessorie" del parlato, ad eccezione della prosodia, vanno perdute nell'attraversare il microfono che restituirà i contributi di tutte le voci come somma algebrica delle stesse con evidente decremento della comprensibilità.

Esistono, per la verità, dei software per il restauro dei segnali (ne parlerò nel cap. 21) ma questo specifico tipo di corruzione non si presta a un ripristino efficace non potendo attenuare o filtrare selettivamente contributi acustici del tutto indistinguibili l'uno dall'altro.

Ovviamente, tutto questo non vale solo nel caso della registrazione, ma anche nella trasmissione di microspie.

Viceversa, nel caso di colloqui telefonici, non avendo gli interlocutori un contatto visivo e venendo meno la comunicazione non verbale, l'eloquio si svolgerà con altre regole e modalità espressive.

In questo caso, se si tratta di un'intercettazione ambientale, si ascolterà solo uno dei parlanti, con le difficoltà di comprensione che è facile immaginare, mentre se si tratta di un'intercettazione o registrazione telefonica, si potranno ascoltare ambedue gli interlocutori con piena comprensione dei discorsi.

Credo che gli esempi precedenti possano aver chiarito alcuni dei problemi tecnici che limitano notevolmente la funzionalità delle "cimici" ma anche di eventuali registratori nascosti, evidenziando come si abbia piuttosto ragione di temere la presenza, e l'efficienza, di un registratore telefonico abilmente occultato.

14. I registratori telefonici

I registratori progettati appositamente per l'uso telefonico, sono facilmente reperibili nei negozi specializzati o tramite internet. In particolar modo, sul sito di aste E-bay, si trova a un prezzo contenutissimo un modello in grado di avviare la registrazione ogni volta che viene alzata la cornetta del telefono interrompendola alla fine della telefonata (vedi fig.16), in modo da ottimizzare lo spazio occupato in memoria, prolungando in modo determinante la durata della registrazione e abbreviando i tempi del successivo riascolto poiché sono stati eliminati tutti gli spazi morti fra le telefonate.

I files che produce, sono in formato MP3, quindi facilmente trasferibili e archiviabili in un computer. La memoria di massa del registratore è una comune scheda flash e da questa dipende la durata totale delle registrazioni che può arrivare anche a parecchi giorni.

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.

Si vedano, a tal proposito, nell'appendice alla fine di questo libro, le implicazioni connesse all'uso illegale degli apparati di intercettazione e/o registrazione.

Inoltre i regolamenti delle società telefoniche vietano espressamente qualunque tipo di manomissione della linea che non sia eseguita da personale autorizzato.

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.

Fig.16
Un registratore digitale progettato per l'uso telefonico

È successo, infatti, in qualche caso, che tecnici della società telefonica scoprissero, del tutto casualmente, durante una riparazione o una normale manutenzione, un collegamento abusivo e 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.

Ma non è ancora tutto: è possibile realizzare facilmente e con una spesa ridicola una semplice interfaccia tra la linea telefonica urbana e un registratore a cassette o digitale (vedi schema in fig.17).

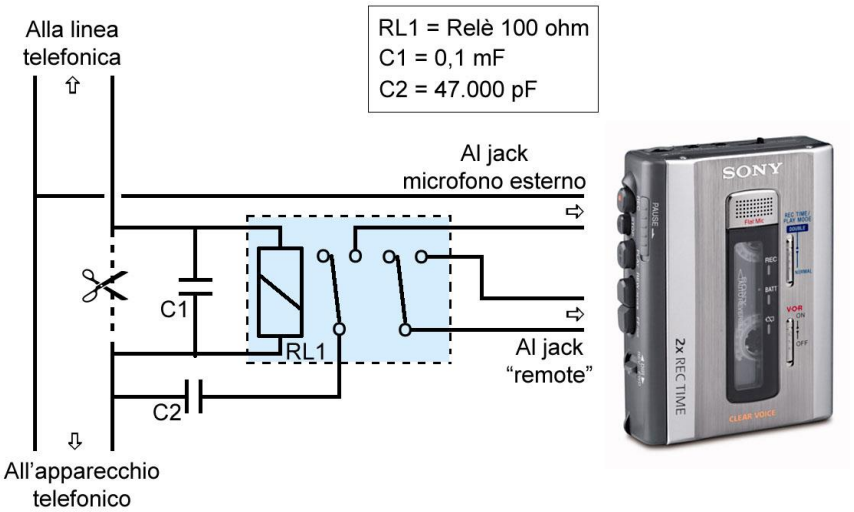

Fig.17
Schema di una semplice interfaccia
tra la linea telefonica urbana e un registratore

Un normale registratore, anche se di modesta qualità, è certamente sufficiente, purché sia dotato d'ingressi jack per il microfono esterno e per il comando a distanza. Quest'ultimo è semplicemente quello denominato "remote", presente su molti apparecchi.

Qui saranno collegati i contatti del relè, visibile nello schema elettrico, denominati "al jack remote". Se in qualche modello di registratore questo ingresso non fosse previsto, niente paura: basta usare lo stesso contatto di scambio per interrompere un polo delle pile di alimentazione ottenendo così lo stesso risultato, ossia far avviare il registratore quando viene sollevata la cornetta del telefono e fermarlo quando la comunicazione termina.

Questa è una condizione essenziale poiché, altrimenti, il nastro si esaurirebbe in poco più di un'ora.

Seguiamo ora con attenzione il disegno del semplice schema elettrico, costituito dal relè (RL1) con bobina da 100 ohm, collegato in "serie" a un capo della linea telefonica, dopo averla interrotta nel punto indicato dalla forbice.

In parallelo alla bobina stessa è posto un condensatore (C1) del valore di 0.1 microfarad. In questo modo, quando viene sollevata la cornetta del telefono, la corrente che scorre nella linea è sufficiente a eccitare il relè e non si causa un'attenuazione apprezzabile dell'audio, tanto da indurre nell'utente il sospetto di essere intercettato.

Appena il relè si eccita, chiude i suoi due contatti. Il primo di questi (quello di sinistra) porta la voce all'ingresso microfonico del registratore attraverso il condensatore (C2) da 47.000 picofarad che ha lo scopo di fermare la componente in corrente continua normalmente presente sulla linea Telecom. Il secondo gruppo di contatti del relè (quello di destra), controlla, come già detto, l'ingresso "remote" del registratore, che deve essere lasciato in posizione "record", avviandolo in modo automatico al momento opportuno.

Nota: *L'intercettazione consiste nella captazione, tramite opportuni dispositivi, di conversazioni che si svolgono a distanza mediante telefono (intercettazione telefonica) o fra presenti (intercettazione ambientale) ad opera di un terzo, non presente al colloquio né destinatario dello stesso.*

Non c'è intercettazione quando uno degli interlocutori registra la conversazione cui sta partecipando e quindi non s'intromette di nascosto nella comunicazione fra terzi o viene a conoscenza d'informazioni a lui precluse.

Allo stesso modo, non c'è intercettazione quando uno dei due interlocutori, al telefono, effettua una registrazione della conversazione, purché avvisi l'altro del fatto che sta registrando, ricevendone il consenso.

In ogni caso, tutto questo non implica la libertà automatica e incondizionata di divulgarne i contenuti.

Infatti, la "ratio" che disciplina le intercettazioni ha per scopo la tutela della riservatezza delle comunicazioni impedendo che un soggetto estraneo venga a conoscenza dei contenuti delle stesse.

Al contrario, quando un soggetto partecipa a una conversazione, vi è l'implicito consenso di tutti gli interlocutori alla condivisione delle informazioni espresse.

15. 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 SMS di chiamata, il telefonino risponderà con un SMS contenente gli ultimi numeri e i messaggini, 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.

Al limite, si potrebbe tenere traccia del credito residuo dopo ogni chiamata effettuata per accorgersi del costo dei messaggini, per così dire "abusivi". Questa però è una cosa poco praticabile a causa della tariffa veramente esigua del singolo SMS, che incide sul credito per poco più di una decina di centesimi.

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).

15.1 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 (vedi fig.18) 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: basta avere un po' di manualità e dimestichezza con il saldatore a stagno per elettronica.

Ora, 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 bene 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.

Purtroppo, se nel primo caso di trasformazione del cellulare in spia ora sappiamo come difenderci, in questo secondo caso non c'è scampo (o quasi).

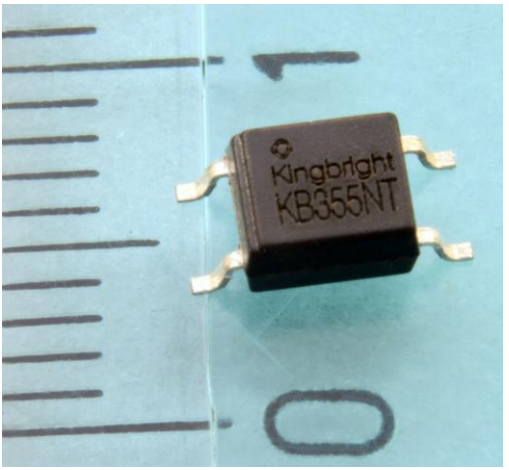

Fig.18
Un circuito integrato utilizzabile per trasformare un normale telefono cellulare in spia ambientale. Si notino le piccolissime dimensioni

15.2 Le schede SIM con falso intestatario

Spesso, chi mette sotto controllo il vostro cellulare provvede a procurarsi una scheda SIM intestata ad altra persona, per evitare di essere individuato. Può usare documenti falsi o sottratti al proprietario, quasi sempre ignaro di avere acceso quel contratto.

In questi casi ricorrono i reati di falsità personale (Art. 494 c.p. sostituzione di persona) e (Art. 497-bis c.p. possesso o fabbricazione di documenti di identificazione falsi) ricompresi fra i delitti contro la fede pubblica.

Alcuni ritengono di non commettere particolari reati offrendo una somma di denaro a un soggetto in difficoltà economiche, affinché acquisti al loro posto una o più SIM.

In effetti, chi si presta a questo scambio, commette solo un illecito amministrativo, poiché non comunica tempestivamente al

gestore del contratto telefonico il cambio d'intestatario della scheda.

Nel caso però le SIM siano successivamente usate per commettere reati, (truffe, intercettazioni illegali, ecc.) il soggetto che si è prestato all'acquisto delle schede passerà i suoi guai nel cercare di dimostrare come non fosse a conoscenza delle reali intenzioni di chi gli aveva commissionato l'acquisto.

Ove le sue argomentazioni difensive non risultassero abbastanza convincenti, potrebbe essere incriminato per il reato di favoreggiamento personale (art. 378 c.p.) o per quello, anche più grave, di concorso di persone nel reato (art. 110 c.p.).

15.3 È possibile difendersi dalle intercettazioni telefoniche?

Di una cosa potete essere certi: non è facile difendersi da questo genere d'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, il verbo "to scramble" significa "mettere in disordine, mescolare alla rinfusa". Il dispositivo elettronico di cui sto parlando opera in tal modo, campionando varie parti

dell’inviluppo 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’inviluppo, riportando il parlato a una forma identica all’originale.

Le sale operative della Polizia di Stato e dell’Arma, quando devono 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 a 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, poiché le possibilità di codifica che uno "scrambler" analogico può ottenere sono relativamente poche, per cui la "decriptazione" è solo una questione di tempo.

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, prendendo contatto direttamente con 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 nel capitolo seguente (fig.19), fornisco una descrizione del principio di funzionamento di uno "scrambler" a inversione di banda.

16. Il codificatore di voce:

È interessante capire il principio di funzionamento di uno "scrambler" anche se, per ottenere ciò, bisogna addentrarsi in termini tecnici un minimo complessi.
Cercherò di semplificare la cosa, nei limiti del possibile, con l'ausilio del disegno seguente, che rappresenta lo schema a blocchi dei principali circuiti elettronici di un codificatore di voce a inversione di banda: nel blocco in alto, identificato dalla scritta "voce in ingresso", sono rappresentate alcune frequenze componenti la voce umana che, come è noto, spaziano fra i 300 e i 3.000 Hertz circa.

Ho arbitrariamente diviso tale estensione di gamma in sette diversi gruppi, a scopo semplificativo. Ognuna di queste frequenze, entrando nel codificatore di voce, viene miscelata, nel circuito "mixer", rappresentato nel blocco successivo, con una frequenza generata localmente all'interno dello "scrambler" dal blocco "oscillatore".

Naturalmente questa frequenza "locale" è modificabile, poiché proprio la sua programmazione permette di determinare la "chiave" di codifica e decodifica.

Nel nostro esempio supponiamo che l'oscillatore locale lavori a 3.300 Hz. Miscelando tale frequenza fissa con quelle prodotte dalla voce, otterremo, all'uscita dello stadio "mixer", due altri gruppi di frequenze, uno ricavato dalla somma della frequenza dell'oscillatore con le frequenze in ingresso e l'altro dalla differenza.

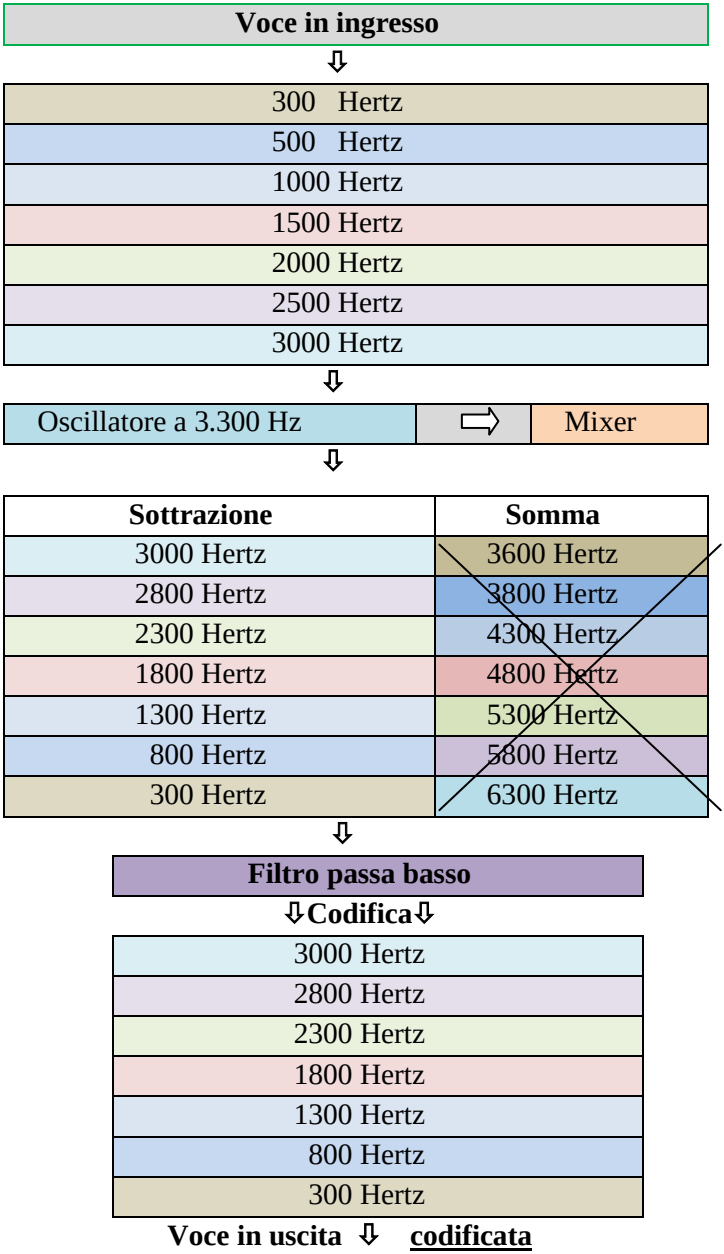

Fig.19

Schema a blocchi di uno "scrambler" audio

Nei due blocchi “somma “ e “sottrazione”, possiamo vedere il risultato di tale mixaggio e notare come si sia ottenuta una vera e propria “inversione di banda audio”.

Nel blocco successivo, denominato “filtro passa basso”, sono eliminate tutte le frequenze maggiori di 3.300 Hz, ossia quelle ottenute per “somma”, mentre sono lasciate passare quelle ricavate per “sottrazione”.

Otteniamo così all’uscita un inviluppo audio codificato, dove una frequenza d’ingresso di 300 Hz diventa di 3.000, mentre una di 500 si trasforma in 2.800 Hz.

Lo “scrambler” è progettato in modo da generare solo frequenze che rientrino nella larghezza di banda delle linee telefoniche, in modo da trasmettere la voce codificata senza apprezzabile attenuazione o distorsione.

Per rendere nuovamente comprensibile la conversazione è sufficiente percorrere tutti gli stadi dello “scrambler” del corrispondente che provvederà alla riconversione del segnale nelle frequenze originali.

Prima di terminare il capitolo sulle intercettazioni telefoniche, desidero aprire qui una breve parentesi per ricordare a tutti quelli che ritengono, erroneamente, che i telefoni cellulari dell’ultima generazione siano inintercettabili e quindi adatti e sicuri per effettuare comunicazioni riservate, che già esistono apparecchi riceventi in grado di ascoltare quanto viene detto con i telefoni G.S.M. Qualsiasi comunicazione affidata alle onde radio è intercettabile! È solo una questione di attrezzature e, in ultima analisi, di spesa.

Attenzione però: una cosa è ascoltare delle comunicazioni G.S.M. a caso, altra è intercettare il telefonino di uno specifico utente. Anche questo è tecnologicamente fattibile, ma il possesso e l’uso degli apparati in grado di raggiungere queste prestazioni è riservato agli enti che ne hanno legale diritto, ad esempio Polizia di Stato, Carabinieri ecc., quindi non sono in libera vendita,

fortunatamente, oltre ad avere prezzi di acquisto decisamente elevati.

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 e attualmente non sono più usati (salvo rare eccezioni). Il passo successivo fu l'introduzione della tecnologia CT1+, che avrebbe dovuto rimanere in commercio non oltre il 2008.

I primi sistemi trasmettevano in modo analogico e le frequenze usate erano intorno a 40 MHz, 49MHz e 72MHz, secondo le marche e dei modelli. I secondi trasmettono nella banda di 885-887 MHz / 930-932 MHz, sempre in analogico.

Grazie al loro costo, tutto sommato non eccessivo, conobbero un'enorme diffusione e se i modelli CT1 sono quasi scomparsi, i CT1+ sono ancora abbastanza diffusi, specialmente in provincia.

Successivamente furono introdotti i cordless CT2, operanti nella banda 864-868 MHz, finalmente con modulazione digitale.

Comunque, a partire dal 2009, sono stati introdotti altri servizi nelle bande usate da questi cordless, cosicché non ne è più garantito il funzionamento privo di interferenze.

Intercettare le conversazioni di chi ancora usa 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 entrare nella vostra "base" per telefonare "aggratis". Succede assai più spesso di quanto non s'immagini! Questo spiega il mistero di bollette incomprensibilmente alte o con chiamate verso numeri internazionali mai effettuate dall'utente, per così dire "legittimo".

Purtroppo però, si sono verificati anche casi di telefonate con fini illegali: estorsioni, truffe stalking ecc. per le quali sono stati indagati ignari cittadini la cui unica colpa era di non conoscere i limiti tecnici dei propri telefoni cordless.

Ricordo il caso di un mio cliente, per il quale partecipai al processo penale in qualità di consulente di parte, accusato di numerose truffe ai danni di commercianti nel settore elettronico e fotografico. La sua unica colpa era quella di aver lasciato la connessione Wi-Fi del suo negozio priva di password e di usare un vecchio telefono cordless.

Qualcuno, dopo l'orario di chiusura del negozio, si collegava abusivamente alla sua rete wireless e alla sua utenza telefonica e acquistava materiale fotografico o elettronico facendolo spedire all'indirizzo di un anziano, e ignaro, pensionato.

Fortunatamente riuscimmo a dimostrare l'estraneità del mio cliente ai fatti criminosi, ma comunque passò un brutto momento, rischiando una pesante condanna penale.

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 10/15 cm. o se è vecchio come il peccato, allora è un modello analogico. La soluzione? Una, sola e drastica: 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 *(Digital European Cordless Telephone)*. 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 1880 ÷ 1900 MHz. Purtroppo però, una delle

caratteristiche di questa tecnologia, connessa con la riduzione dei disturbi e del fruscio di fondo, prevede l'emissione periodica 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 è emesso periodicamente, anche se brevemente, 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 e 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.

17. Scoprire le telecamere nascoste con un telefonino

Il “cuore” (ma sarebbe meglio dire “l’occhio”) di una telecamera per videosorveglianza o di una microtelecamera-spia, è il sensore ottico, ossia il componente posto dietro l'obiettivo che trasforma la luce in segnale video.

Attualmente esistono due tecnologie, entrambe molto utilizzate: il CCD e il C-MOS. Entrambe si basano su un componente elementare comune: il fotodiodo, un elemento fotosensibile in grado di generare una carica elettrica proporzionale alla quantità di luce che lo colpisce.

I sensori CCD e C-MOS sono composti da un numero elevato di fotodiodi, meglio conosciuti come “pixel”. Mediante l’elaborazione del segnale di ogni pixel la telecamera ricompone l'immagine globale che si trova di fronte all'obiettivo.

I fotodiodi, o pixel, che compongono i sensori sono naturalmente sensibili a una gamma di frequenze luminose molto più ampia di quella dell’occhio umano, quindi “vedono” anche la luce infrarossa.

Per questo motivo, molte telecamere per videosorveglianza e moltissime microtelecamere-spia, sono dotate di un sistema d’illuminazione a led infrarossi per metterle in grado di vedere la scena inquadrata anche nel buio più assoluto.

È un sistema semplice e, tutto sommato, economico, anche se limitato a un’area ristretta. Per illuminare zone più estese, esistono appositi fari costituiti da un insieme di numerosi led in grado di arrivare a distanze maggiori.

I led incorporati nelle microtelecamere hanno la particolarità di essere sempre accesi, di notte come di giorno, poiché, avendo un consumo energetico bassissimo e una durata (in ore di vita) elevata, non c’è ragione di prevedere un ulteriore circuito di controllo che li attivi all’occorrenza.

Anche la fotocamera del vostro telefonino è basata su un

sensore C-MOS che, tra l'altro, è meno costoso di un CCD, ed è sensibile anche all'infrarosso!

Se volete fare una prova pratica e immediata della visione infrarossa, inquadrate il telecomando del televisore o dello stereo e premete un tasto qualsiasi. Vedrete una lucetta bianca lampeggiare rapidamente.

Tutto ciò trasforma il nostro telefonino in un semplice rivelatore di telecamere nascoste: se inquadrate un'area dove sospettate la presenza di una microtelecamera-spia e se questa è dotata di led infrarossi, vedrete un'inconfondibile luce bianca che ne rivelerà la presenza.

Ovviamente lo stesso effetto si ottiene con una macchina fotografica digitale. Addirittura, inquadrando di notte una telecamera per videosorveglianza, comprese quelle che controllano le zone a traffico limitato nelle nostre città, sapremo immediatamente se sono attive o meno. Queste telecamere, dovendo inquadrare un'area discretamente ampia, sono affiancate da un faro a infrarossi, che si può riconoscere avendo, generalmente, il vetro anteriore di colore nero. L'illuminatore viene attivato al calare della sera ma, se il sistema non è attivo, non lo è nemmeno il faretto.

18. 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.

Ovviamente, la dimensione delle microspie deve essere la più contenuta possibile, per 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 s'indica la portata, ci si riferisce sempre a quella "ottica" ossia in assenza di ostacoli interposti fra il trasmittente e ricevente.

Ben difficilmente una microspia potrà soddisfare questa condizione ottimale poiché, dovendo essere nascosta con grande attenzione per non essere rinvenuta casualmente e posizionata in modo da captare facilmente le parole pronunciate nell'ambiente spiato, quasi sempre sarà 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 a un registratore audio digitale.

Sarà così sufficiente recarsi periodicamente a prelevare i files tramite un computer portatile, 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 o un'autoradio dotata della gamma F.M., modificata in modo da estenderne la ricezione, che normalmente si trova fra gli 88 e i 108 Mhz, portandola fino a 110 Mhz circa. Le microspie 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 a 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.

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".

Fig.20
L'ICOM IC R20, un ricevitore scanner
in grado di ascoltare qualunque microspia

19. Le microspie GSM

Come dicevo nel capitolo precedente, le 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.

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?

Facciamo un passo indietro: si è detto che queste "cimici" funzionano come un telefono cellulare, pur con le dovute differenze. Dunque, come un cellulare, si attivano a intervalli di tempo più o meno lunghi, per comunicare alla cella telefonica più vicina la loro presenza e posizione in rete.

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. Lo strumento adatto è il "jammer" (vedi figg.21 e 22), 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 di questi prodotti, anche perché potenzialmente in grado di interrompere un pubblico servizio come quello delle comunicazioni telefoniche cellulari.*

Fig.21
Un "jammer" portatile a batterie

Fig.22
Un "jammer" da laboratorio con il suo alimentatore di rete

20. Le microspie GPS

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 (vedi fig.23).

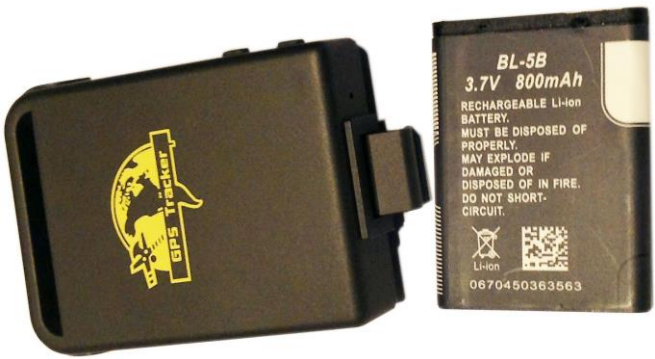

Fig.23
Un "GPS Tracker", con la sua batteria al litio

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.

La sensibilità della sezione satellitare è esaltata dalla preamplificazione dell'antenna in modo che possa rilevare i segnali GPS anche da una posizione sfavorevole, quale è la zona inferiore di una macchina.

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 con 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 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 le quarantotto ore.

In ogni caso, quando la batteria sarà prossima all'esaurimento, un apposito SMS avviserà di provvedere alla ricarica.

Il tracker si riattiverà automaticamente non appena l'automobile si metterà in movimento, o non appena supererà un limite di velocità prefissato o, infine, non appena uscirà da un perimetro prestabilito, inviando immediatamente un SMS di allerta, completo dei dati geografici relativi alla latitudine e longitudine.

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 già menzionati a proposito delle "cimici" ambientali.

Come difendersi da questo efficace e intrusivo sistema di controllo?

Abbiamo visto come una parte essenziale del localizzatore sia costituita da un normale telefono cellulare che s'incarica di trasmettere allo "spione" i dati geografici sotto forma di SMS.

Ebbene, gli stessi "jammers", che ho descritto nel capitolo diciannove, sono perfettamente in grado di inibire il collegamento tra il localizzatore e il sistema telefonico cellulare impedendo la trasmissione dei dati necessari per indicare la nostra posizione nelle Google maps.

Inoltre, sono recentemente stati messi in commercio dei "jammers" capaci di inibire, oltre ai collegamenti cellulari, anche i segnali dei satelliti GPS, i dispositivi "Bluetooth" e perfino il sistema di accesso senza fili alla rete internet, denominato "Wi-Fi".

20.1 Come funziona il sistema GPS

Voglio terminare questo capitolo, illustrando per grandi linee come funziona il sistema GPS, acronimo di "Global Positioning System" ossia sistema di posizionamento globale.

Il progetto, finanziato dal Dipartimento della Difesa USA e

classificato a lungo come “top secret”, prese il via durante gli anni della guerra fredda per scopi esclusivamente di carattere militare.

In seguito, il governo statunitense, prendendo atto della fine della cosiddetta “guerra fredda” decise di renderne pubblici i parametri di accesso consentendone così l’uso in ambito civile come ausilio alla navigazione aerea, navale, terrestre e in numerosi altri ambiti.

Il sistema GPS è attualmente composto di ventiquattro satelliti operativi e tre definiti “latenti”, attivabili in caso di malfunzionamento di uno fra quelli operativi.

A completamento del sistema ci sono cinque stazioni di controllo a terra, dislocate nei pressi dell’equatore, alle Hawaii, sull’isola di Ascension, a Diego Garcia, a Kwajalein e a Colorado Springs. Quest’ultima rappresenta la stazione “master”.

I satelliti GPS, che orbitano a 20197 km dalla terra, non sono satelliti geostazionari, contrariamente a quanto comunemente si crede, ma orbitanti, con un periodo di rivoluzione di circa dodici ore e con una velocità di spostamento, relativa al suolo terrestre, attorno ai 3mila Km/h e una velocità sul piano dell'orbita di circa 13mila Km/h.

I sei piani orbitali della costellazione sono ininterrottamente monitorati da un centro di controllo tecnico, ubicato presso il Dipartimento della Difesa USA, per correggere gli influssi esterni, come per esempio l’attrazione gravitazionale della Luna o le lievi irregolarità della terra, che non è perfettamente sferica, che possono generare differenze fra l’orbita pianificata e quella reale, in grado di compromettere il delicato equilibrio su cui si basa il sistema GPS. La precisione richiesta nelle orbite è dell’ordine dei centimetri! Questo la dice lunga sul livello di tecnologia raggiunta dal sistema GPS.

Insieme all’accuratezza dei piani orbitali, un altro fattore

chiave per il buon funzionamento del sistema GPS sono sincronismi temporali e i parametri di navigazione, detti "Almanac".

Infatti, il servizio offerto dal GPS è fondato su algoritmi trigonometrici aventi come base di riferimento delle rette virtuali la cui lunghezza è calcolata in base alla velocità di propagazione delle onde radio (circa 300mila Km/s).

L'accuratezza del calcolo dei tempi intercorrenti tra la partenza del segnale dal satellite e il suo arrivo a terra, nel "GPS Tracker", è affidata a orologi atomici, gli unici sistemi in grado di garantire una precisione nell'ordine dei nanosecondi.

Contemporaneamente il ricevitore a terra, che non è dotato di un proprio orologio atomico, genera uno speciale codice, che sincronizza continuamente il proprio orologio interno con quello del satellite in conformità ad apposite informazioni che il satellite stesso periodicamente invia.

In tal modo, il ricevitore a terra conosce l'istante esatto di partenza di ogni segnale trasmesso dal satellite e può compararlo con quello di effettiva ricezione, con un margine di errore di circa un miliardesimo di secondo.

Il ricevitore GPS, in poche parole, compie gli opportuni calcoli conoscendo la posizione orbitale e la distanza in linea ottica che lo separa da ogni satellite, applicando la nota formula sulle leggi della dinamica elaborata da Isaac Newton: velocità=spazio/tempo.

La frequenza di trasmissione radio del GPS civile, detta "L1 coarse acquisition", è di 1,57542 GHz. Si tratta di segnali superiori al limite entro il quale le radiotrasmissioni dallo spazio possono essere fortemente condizionate da fattori naturali ionosferici e/o troposferici, ma inferiore al limite oltre il quale le onde elettromagnetiche divengono eccessivamente sensibili a eventuali ostacoli ambientali, generando troppe riflessioni parassite.

Questa gamma di frequenze, inoltre, risente solo in modo marginale delle condizioni meteorologiche.

Fino alla metà del 2000 l'errore medio di calcolo della posizione geografica si aggirava sui 100-150 metri in condizioni operative ottimali ma, nella realtà reale, poteva facilmente arrivare a 250-300 metri.

Successivamente un particolare limitatore del segnale radio, la cosiddetta "disponibilità selettiva", è stato ritoccato per aumentare la precisione del GPS civile dando così un notevole impulso al suo successo commerciale, che ha portato alla fabbricazione dei navigatori, oramai di uso comune a bordo di molte automobili.

Attualmente, il margine d'errore del sistema di navigazione GPS si stima indicativamente in 15-20 metri, anche se le sue potenzialità reali possono arrivare molto al di sotto di un metro.

Tuttavia è necessario sottolineare che, per raggiungere un così basso margine di errore, sono necessari appositi ricevitori GPS militari in grado di decifrare contemporaneamente sia le trasmissioni GPS sulla gamma L1 (1,57Ghz Coarse Acquisition) che sulla gamma L2 (1,22Ghz Precise Acquisition). L'utilizzo della gamma L2 è però precluso ai ricevitori per uso civile, mediante la criptazione del codice "Precise Acquisition".

Tale procedura, detta "anti spoofing" è stata messa in atto allo scopo di impedire a potenze militari ostili di usufruire di potenzialità di localizzazione GPS pericolosamente accurate.

Per finire, è importante sapere che esistono notevoli differenze qualitative fra marche e modelli diversi di ricevitori GPS, dovute fondamentalmente ai tempi per l'aggancio dei satelliti, all'accuratezza della rilevazione ma, principalmente, al mantenimento dell'aggancio stesso durante il transito del ricevitore fra ostacoli ambientali.

La precisione di un ricevitore GPS aumenta in base al

numero di satelliti ricevuti contemporaneamente. In realtà, i satelliti che possono essere "visti" in un determinato momento, anche se particolarmente favorevole, non superano la decina.

È per questa ragione che alcuni navigatori che vantano, almeno sulla carta, sedici o più satelliti ricevibili contemporaneamente, non forniscono, in realtà, alcun particolare miglioramento riguardo alla precisione del punto geografico individuato.

21. I processatori 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 ottimo testo in proposito, che consiglio vivamente a chi volesse approfondire il tema a livello forense, è "Intercettazioni telefoniche e ambientali", di A. Paoloni e D. Zavattaro).*

Un dispositivo costruito a tale scopo è il "processatore di segnale audio" o "signal processing", del quale ho accennato poc'anzi. Si tratta di un apparecchio elettronico contenente una serie di filtri attivi passa-banda e/o 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 e 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 "inviluppo", 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 a uno o più passaggi attraverso il processatore audio che, se manovrato da persone esperte, potrà eliminare o attenuare consistentemente tali disturbi.

L’azione del microprocessore poi, farà qualcosa di ancor più fine, riconoscendo le caratteristiche tipiche dell’inviluppo della voce ed eliminando drasticamente quelle forme d’onda che, non rientrando nelle figure memorizzate, saranno individuate e attenuate.

Ovviamente il processatore audio non può fare miracoli, pertanto non potrà superare i limiti imposti dalle leggi dell’acustica né ricostruire voci o suoni non presenti nel segnale originale.

22. Le frequenze di normale utilizzo

Chi realizza delle microspie a livello industriale si propone, ovviamente, di esportarle in tutto il mondo, al fine di realizzare un guadagno che giustifichi l'impegno finanziario connesso con la progettazione e realizzazione del prototipo e con l'avvio di una catena di montaggio, sia pure in scala ridotta.

Di norma, i fabbricanti di microspie tendono a usare sempre le medesime frequenze, spesso di libero uso nei vari paesi del mondo, per le trasmittenti di debole potenza, quali sono appunto le cosiddette "cimici".

Scopo di questa scelta è evitare di esportare dispositivi "fuorilegge" e quindi passibili di sequestro da parte degli organi di controllo (di questo si occupa, in Italia, la Polizia Postale e delle Comunicazioni) ma anche evitare di interferire o essere interferiti da altri servizi di radiotrasmissione che renderebbero inascoltabile il debole segnale delle microspie.

Ovviamente questo dovrebbe facilitare, in qualche misura, il compito del tecnico della bonifica, riducendo sensibilmente la gamma delle frequenze da esplorare.

A questo potrei aggiungere un ragionamento logico basato sulla ovvia necessità di nascondere accortamente la "cimice" per evitarne il ritrovamento, magari casuale, da parte del soggetto intercettato.

Si tratta della lunghezza fisica dell'antenna trasmittente: abbiamo già visto, nel cap. 9, che esiste un rapporto matematico tra la frequenza usata e la lunghezza della relativa antenna. In particolare, al crescere della frequenza corrisponde un'antenna più corta.

Possiamo quindi affermare che non deve essere facile nascondere una microspia fornita di un'antenna lunga due metri e, di conseguenza, possiamo ipotizzare che la nostra ricerca può concentrarsi, prevalentemente, su quelle frequenze che

consentono l'uso di un'antenna non più lunga di un venti/trenta centimetri.

Guarda caso, i canali più bassi, usati da un importante fabbricante di microspie professionali nel Regno Unito, sono situati intorno ai 399,000 MHz.

Quindi, applicando la formuletta di cui al cap. 9 (lunghezza in metri = 300/Frequenza in megaHertz), avremo 300/399 = 0,75 cm. Poiché le antenne possono essere realizzate in ¼ d'onda, mantenendo un discreto rendimento, dividendo questa lunghezza per quattro avremo: 0,75/4=0,18 ossia un'antennina di circa 18 centimetri.

Per la verità è possibile ridurre ulteriormente le dimensioni di un'antenna, senza alterarne apprezzabilmente la frequenza di risonanza, inserendo alla base del conduttore una bobina di filo con funzione di reattanza induttiva (in tal caso si parla di antenna "caricata"), tale che l'impedenza sia riportata nei valori ottimali, anche se questo artificio abbassa il rendimento del sistema poiché aumenta la resistenza di radiazione.

All'atto pratico, tutto ciò estende verso il basso le frequenze utilizzabili nelle microspie, a parità di lunghezza dell'antenna.

Tuttavia, sulla base dell'esperienza sul campo, non solo personale ma anche di alcuni colleghi con i quali ci scambiamo notizie e aggiornamenti, mi sento di affermare che è estremamente raro trovare una "cimice" con frequenza più bassa di 174 MHz, a parte qualche eccezione che troverete nella tabella del cap.21.

Infatti, scendendo di frequenza, troviamo la gamma assegnata alle comunicazioni fra aeromobili, militari e civili, e fra questi e le torri di controllo.

In particolare, incontriamo alcuni sistemi di radionavigazione o per l'avvicinamento alla pista, quali il VOR (VHF Omnidirectional Range), che lavora da 112.000 a 117.900 MHz e da 108.000 a 111.900 MHz e L'ILS (Instrument Landing System), che lavora da 108.100 ÷ 111.950 MHz, fornendo i segnali per la

guida sul piano orizzontale mentre, sul piano verticale trasmette da 328.600 a 335.400 MHz.

Nessuna persona sana di mente si sognerebbe di costruire una microspia che trasmetta in questa gamma.

Poiché gli aerei sorvolano le nostre città, sarebbe facilissimo interferire con le loro comunicazioni o, peggio, con i citati strumenti di radionavigazione, con gravissime conseguenze.

Al di sotto, fra 88,000 e 108,000 MHz troviamo la gamma delle radio commerciali in FM. Nessuna microspia è in grado di competere, quanto a potenza di emissione, con questi trasmettitori. È pur vero che, nel passato, si potevano trovare in commercio alcune "cimici" che operavano su questa gamma di frequenza allo scopo di evitare l'acquisto di un ricevitore dedicato. Infatti, si poteva usare una comune radio casalinga o un'autoradio.

Erano però tempi pionieristici, prima dell'affermarsi delle cosiddette "radio libere", quando la gamma FM era semivuota e impegnata solo da un paio di stazioni RAI e da Radio Montecarlo.

Scendendo ulteriormente di frequenza troviamo i vari servizi di comunicazione radiomobile della Polizia di Stato, dei Vigili del Fuoco ecc.

In conclusione, è assolutamente ragionevole cercare le microspie inserendo come frequenza minima, nell'analizzatore di spettro, i 120,000 ÷ 140,000 MHz, circa e salendo gradualmente fino ad almeno 3000,000 MHz (ossia 3 GHz). L'esperienza dell'operatore, in ogni caso, avrà l'ultima parola in merito a quali gamme di frequenza esplorare.

22.1. Le microspie artigianali

Un discorso a parte va fatto per le microspie di realizzazione artigianale. In questo caso non è necessario preoccuparsi del numero di pezzi destinati all'esportazione o di leggi e regolamenti del paese di destinazione o di problemi di natura doganale.

Quasi sempre la microspia sarà realizzata in unico esemplare o comunque in un numero ridottissimo pezzi con l'unica preoccupazione di trovare un canale libero, relativamente alla zona geografica dove è destinata a essere usata.

Le frequenze sono comunque superiori ai 174,000 MHz di cui al capitolo precedente, anche se con alcune eccezioni delle quali si deve tener conto per eseguire una bonifica professionalmente corretta.

Alcune microspie artigianali usano, devo dire molto furbamente, frequenze inserite fra i canali UHF della TV digitale terrestre (DVB-T), magari non utilizzati nella zona.

Non è per niente facile trovare queste "cimici" con le loro piccole potenze, inserite fra emittenti che irradiano potenze molto rilevanti. In questi casi è prezioso l'aiuto dell'analizzatore di spettro purché di ottima qualità.

Le TV digitali appariranno sullo schermo come picchi di segnale intenso, ma con limitata banda passante, grazie alla modulazione di tipo digitale, mentre una microspia apparirebbe con un picco d'intensità modesta, ma con una larghezza di banda maggiore, dovuta alla sua modulazione in F.M.

Si tratta comunque di frequenze molto elevate, comprese fra i 510 e gli 860 MHz, con una notevole efficienza di trasmissione e che consentono l'uso di antenne di piccole dimensioni: l'ideale per una microspia!

Fra l'altro il sistema TV digitale terrestre prevede un sistema di modulazione di tipo OFDM che produce un flusso audio/video digitale della famiglia MPEG-2.

In parole semplici: se qualcuno stesse risintonizzando il proprio televisore nell'area di azione di una microspia artigianale che trasmetta in vicinanza dei canali DVB-T, non ascolterebbe nulla poiché la de-modulazione dei televisori è del tutto incompatibile con la modulazione FM usata dalle microspie.

Altre frequenze, utilizzate a volte in realizzazioni artigianali,

sono quelle riservate agli apparati di debole potenza, deregolamentati da qualche anno in Italia e quindi in libera vendita, chiamati LPD (Low Power Devices).

Realizzando una microspia sulle frequenze LPD, che vanno dai 433,075 ai 434,775 MHz con 69 canali, si utilizzano, ancora una volta, frequenze elevate e di notevole efficienza con l'uso di antenne di piccole dimensioni.

Inoltre non è necessario munirsi di un ricevitore scanner, che comunque avrebbe un costo notevole, ma si può acquistare un ricetrasmettitore LPD per una cifra molto contenuta.

Certamente qualche ricetrasmittente LPD sarà stata usata come microspia, bloccandola in trasmissione e collegandola con un alimentatore alla rete elettrica per superare il problema della durata delle batterie, nonostante le dimensioni, pur contenute, non siano esattamente minimali e nonostante il microfono sia poco sensibile, poiché progettato per essere tenuto vicino alla bocca.

La portata di queste ricetrasmittenti è, in campo aperto, di 2 o 3 Km. Nell'uso come microspia, dovendo occultare l'apparecchio e considerando la presenza delle pareti e di altro ostacoli, il raggio di azione è sicuramente molto inferiore. Maggiore comunque di una classica microspia.

Tuttavia, non è stato ancora scoperto, in Italia, un simile uso di un LPD.

Nota: *Dal gennaio 2007 la banda LPD a 433 MHz si è spostata sulla nuova banda SRD (Short Range Devices) intorno gli 860 MHz. La vecchia banda LPD 433 resterà comunque liberamente utilizzabile per tutte le ricetrasmettenti vendute in precedenza. È ipotizzabile che alcune microspie artigianali siano state realizzate anche su questi nuovi canali, con le stesse caratteristiche di efficienza e con l'uso di antenne di dimensioni ancora minori.*

Un'altra gamma di frequenze dove "nascondere" una microspia è una serie di canali situati intorno ai 450 MHz. Si tratta della banda di telefonia cellulare TACS (Total Access Communication System) dismessa nella notte tra il 30 e il 31 dicembre 2005 e sostituita in un primo tempo dal sistema ETACS, dove la E iniziale sta per "Enhancement", avanzato e poi dalle successive tecnologie di comunicazione: GSM, GPRS, UMTS, 3G ecc.

I canali così liberati sono stati ceduti a servizi di tipo militare ma ne restano alcuni tutt'ora inutilizzati, adattissimi al funzionamento, illegale, di una "cimice" artigianale.

Altre frequenze che possono essere usate per le microspie (sempre in maniera illegale, sia chiaro) e che possono sfuggire a una ricerca frettolosa, sono le cosiddette "frequenze VHF per la nautica da diporto".

Si tratta di 88 canali da 156.050 a 162.025 MHz di cui solo una ventina usati con continuità. Oltretutto, essendo frequenze impiegate per il collegamento fra navi e fra navi e terra e avendo una portata media non superiore a una trentina di km (tenuto conto di una serie di fenomeni che interessano le onde radio, quali l'altezza dell'antenna rispetto al suolo e il suo guadagno, la propagazione, l'assorbimento, ecc.) si può essere certi che, nelle zone dell'entroterra, queste frequenze non interferiranno con i servizi cui sono naturalmente dedicate.

Per chi dispone di un ricevitore "scanner", basta fare un po' di ascolto in qualche zona dell'entroterra, per trovare chi ne fa un uso "abusivo" come walkie-talkie per tenere in collegamento la casa con l'officina o per parlare fra automobili o camion.

È chiaro quindi che esistono numerosissime frequenze utilizzabili, anche se in modo totalmente illecito e, parallelamente, una vastissima gamma da esplorare accuratamente tramite l'analizzatore di spettro.

Soprattutto in questi casi emerge la necessità di affiancare a questo strumento un misuratore di campo elettromagnetico, in

grado di segnalare la presenza di una microspia a breve distanza, a prescindere dalla frequenza usata, mettendoci così sull'avviso e spingendoci a una ricerca più esaustiva e approfondita.

Nel prossimo capitolo, riporto una tabella con le bande di frequenza maggiormente usate dalle microspie commerciali e/o artigianali, redatta in conformità a esperienze personali e/o su scambi di notizie fra colleghi, anche di altri paesi europei, a seguito del ritrovamento di uno di questi dispositivi d'intercettazione. (Nota: l'alta incidenza di microspie nella banda 902.000 ÷ 1000.000 dipende dall'uso, oramai comune, delle "cimici" in gamma GSM).

Non deve essere presa alla lettera, ovviamente, essendo solo un'indicazione di massima da cui partire e che potrà essere veramente utile a chi volesse iniziare l'affascinante lavoro di tecnico per la bonifica da microspie.

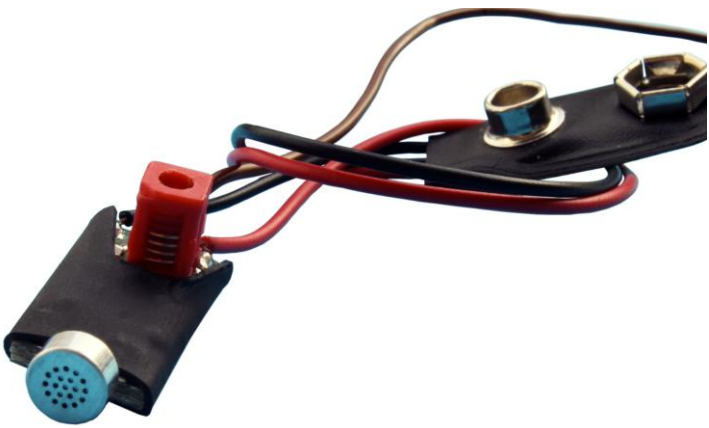

Fig.24

Una microspia "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.

23. Le frequenze maggiormente utilizzate

Frequenza (MHz)	% di ritrovamento microspie
46.610 → 49.970	1 ÷ 2 %
76.500 → 77.000	1 ÷ 2 %
134.000	5 %
134.000 → 140.000	9 %
139.900	9 %
139.940	11 %
139.970	20 %
140.000	22 %
140.000 → 144.000	9 %
144.000 → 146.000	1 ÷ 2 %
146.000 → 148.000	9 %
156.050 → 162.025	10 ÷ 15 %
160.215 → 162.025	1 ÷ 2 %
298.500 → 299.500	3 ÷ 5 %
360.000 → 398.500	1 ÷ 2 %
398.605	35 ÷ 40 %
398.455	25 ÷ 30 %
398.605	30 ÷ 35 %
399.455	45 ÷ 50 %
433,075 → 434,775	30 ÷ 35 %
442.000 → 459.975	10 %
510.000 → 860.975	1 ÷ 2 %
861.000 → 894.000	3 ÷ 5 %
902.000 → 1000.000	75 %
> 1000.000	0,3 %
> 2000.000	0,1 %
> 3000.000	0,1 %

Nota: *Quando è indicata una frequenza precisa, ciò significa il ritrovamento di microspie su quel canale, mentre l'indicazione di una gamma di frequenze mostra la percentuale di ritrovamenti segnalati da vari tecnici in quell'ambito.*

24. Le microspie del futuro

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 libro, 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 è 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, quando non addirittura al singolo tecnico, le quali hanno solo applicato le ricadute tecnologiche di altri settori, specialmente quello della telefonia cellulare.

Durante l'esposizione annuale sulle tecniche e sui prodotti per gli investigatori tenutasi recentemente a Washington D.C. è stato mostrato 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 le adottano, 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 un'indagine, è palese che l'univocità delle parole registrate è condizione essenziale per lasciare poco spazio a interpretazioni postume troppo disinvolte da parte dell'indagato.

Al momento dell'ascolto, e della trascrizione da parte del perito incaricato, esistono dispositivi chiamati "processatori audio", che possono lavorare al massimo delle proprie possibilità quando elaborano un segnale 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 s'incaricano di superare i problemi legati alla portata del segnale radio. Le novità, sotto quest'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 e alimentato direttamente dalla rete elettrica. Quest'ultimo poi s'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 d'intercettazione è fondamentale

e dell'autonomia delle batterie che, grazie alla piccolissima potenza di trasmissione necessaria, può aumentare sensibilmente.

Impressionanti le microspie funzionanti in FHSS, (frequency-hopping spread spectrum). Si tratta di dispositivi che dividono il segnale in brevi segmenti prima di trasmetterlo su una serie di frequenze diverse e non adiacenti, generate in modo "random", all'interno di un vasto spettro radio. Simili microspie sono virtualmente inintercettabili, tanto è vero che trovano applicazione in ambito militare e satellitare, anche a causa del loro prezzo di acquisto, altrettanto "satellitare"!

Microtelecamere collegate con un telefono cellulare WAP *(Wireless Application Protocol)* 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 a internet possono essere telecomandate, brandeggiate su due assi, asservite al movimento delle persone nell'ambiente in maniera da inquadrarle sempre in modo ottimale. Oggetti supertecnologici a prezzi, tutto sommato, abbastanza abbordabili. Molto più di quanto Orwell abbia mai immaginato nei suoi peggiori incubi.

Per quanto riguarda le batterie, che ancora oggi costituiscono uno dei maggiori limiti all'autonomia delle microspie, le novità davvero eclatanti sono dietro l'angolo.

I moderni telefoni "smart phone", sempre più affamati di energia, hanno riportato l'autonomia media dei cellulari ai valori del 1995. Questo, lungi da essere un difetto, costituisce un forte stimolo per l'industria a studiare nuove soluzioni per batterie sempre più piccole e sempre più efficienti.

Anche l'industria automobilistica, alla ricerca di veicoli elettrici in grado di percorrere molto più degli attuali 150 Km, quando va bene, e con tempi di ricarica che superano le sei ore, sta investendo grosse cifre sperimentando nuove soluzioni energetiche.

Nel dipartimento di chimica dell'Università La Sapienza di Roma, sono allo studio nuovi accumulatori al litio-aria in grado di immagazzinare, per ogni Kg di peso della batteria, intensità di corrente quattro volte maggiori rispetto alle precedenti agli ioni di litio.

L'ultima frontiera della ricerca nel settore degli accumulatori si chiama "grafene", un materiale basato sul carbonio che, nel suo straordinario rapporto peso/superficie attiva, racchiude il segreto di un'efficienza straordinaria nell'immagazzinare energia.

Infine, il ricorso alle nanotecnologie promette l'arrivo in un futuro non troppo remoto, di batterie realizzabili con una stampante 3D, oggi allo studio nella prestigiosa Università statunitense di Harvard, o di accumulatori flessibili e spruzzabili come una normale vernice, in fase di sperimentazione nella Rice University, di Houston, Texas.

Voglio terminare questo capitolo con una curiosità, accennando a 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 del vetro della finestra, causate dalle voci all'interno della stanza, lo trasformano in una sorta di grande microfono che modula il raggio laser che viene riflesso dalla superficie del vetro stesso, con un angolo eguale a quello incidente. Tale raggio è ricevuto da un'apposita apparecchiatura, posta in posizione opportuna, che, demodulando il segnale audio, ne estrae l'informazione contenuta.

In seguito, tale segnale deve essere filtrato tramite un processatore 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 sicuramente complesso tanto da richiedere l'impiego di personale specializzato: ad esempio, se il raggio laser fosse 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 sarebbe riflessa verso il cielo rendendone impossibile la ricezione. Quindi il posto di ascolto deve essere posizionato all'incirca alla stessa altezza del locale dove avviene la conversazione.

In Italia, a quanto mi risulta, l'apparato di cui sopra è usato, attualmente, solo dai corpi speciali dell'esercito e... dagli immancabili "Servizi".

25. Dal mondo analogico al digitale

I computers parlano, almeno fra loro, il "computerese". La grammatica, cioè l'insieme delle regole che riguardano gli elementi costitutivi del computerese, è basata sul "digitalese" che è composto di soli due segni: l'1 e lo 0.

Nonostante quest'apparente povertà di linguaggio, i computers sono in grado di esprimere concetti anche molto complessi e, soprattutto, si capiscono benissimo (sempre fra loro).

Gli esseri umani, al contrario, nonostante siano in grado di usare linguaggi molto più diversificati, o forse proprio a causa di ciò, non si sono mai intesi troppo bene, come la storia può ampiamente dimostrare.

Se un uomo iniziasse improvvisamente a esprimersi con due soli suoni, sarebbe rapidamente ricoverato in un centro d'igiene mentale, cosa che ai computers non è mai accaduta.

La parola italiana "digitale" proviene dalla traduzione del vocabolo inglese "digit", che significa "cifra" e che non ha un vero corrispettivo nella nostra lingua.

Le dita, infatti, nonostante l'assonanza linguistica, in questo caso non c'entrano nulla. Forse sarebbe stato meglio tradurre con "numerico" anziché "digitale", com'è stato fatto nella lingua francese, dove si usa il vocabolo "numerique" per indicare quello che noi chiamiamo "digitale".

Qualcosa di analogo (ma non di analogico) era già accaduto oltre cento anni prima, nel 1911, quando il bostoniano Percival Lowell redasse un articolo per il New York Times traducendo, dall'italiano, uno studio dell'astronomo Giovanni Schiaparelli che illustrava, anche con dei disegni, la sua scoperta dei "canali" sul pianeta Marte.

Anche in quel caso, non esistendo, in inglese, un vero corrispettivo del vocabolo “canali”, fu usato il termine “canals” che però indica canali di origine esclusivamente artificiale. Meglio sarebbe stato tradurre con “channels”, ossia canali naturali.

Ovviamente l’articolo del “Times”, avendo un taglio decisamente scientifico, suscitò un grande clamore avvalorando l’ipotesi del pianeta rosso abitato da marziani/ agricoltori dediti allo scavo di gigantesche strutture d’irrigazione.

Bene, dopo questa divagazione a metà fra lo storico e il surreale, torniamo al mondo digitale, detto anche “binario” perché basato sui due soli segni matematici 1 e 0.

Nei precedenti capitoli si è accennato alla tecnologia digitale che rappresenta la naturale evoluzione del mondo dell’elettronica e la direzione verso la quale ci si sta muovendo. Pertanto, mi sembra opportuno introdurre qualche nuovo concetto per spiegare di cosa si tratta, rimanendo però a un livello semplice e divulgativo, com’è nello spirito di questo libro.

Il suono è costituito da onde meccaniche di pressione che si propagano in un mezzo, quale può essere l’aria, l’acqua o un metallo. Nel vuoto non è possibile percepire alcun suono, mancando un mezzo di propagazione.

Le onde sonore possono essere prodotte da una sorgente che emette una sola frequenza e in tal caso si parla di “tono puro” o possono essere il risultato della combinazione di più frequenze, come nel caso della voce umana.

La prima registrazione della voce umana fu quella incisa sul fonografo di Thomas Edison nel 1878, poco meno di due secoli addietro. Da allora sono certamente cambiati, e si sono evoluti, i mezzi di registrazione ma, in sostanza, si è sempre trattato di trasformare la variazione di pressione sonora in un’analoga variazione della corrente elettrica in un circuito.

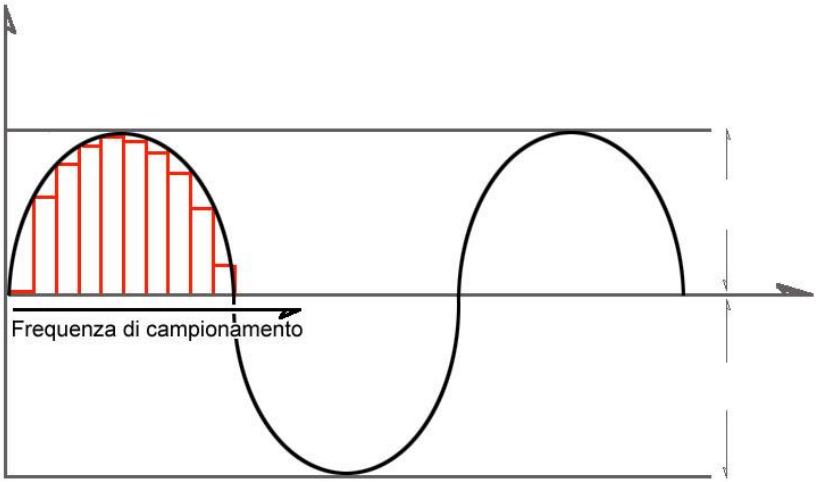

Fig.25a

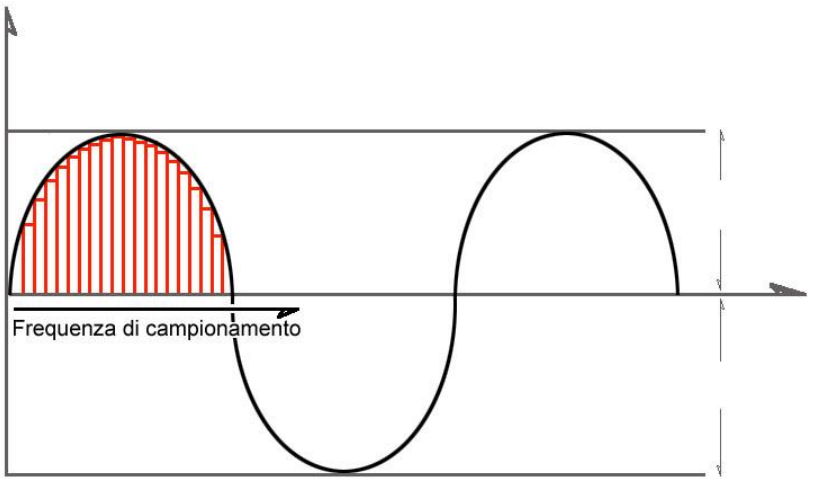

Fig.25b

Proprio per questo si parla di registrazione “analogica” perché il segnale elettrico risultante è simile (analogo) a quello meccanico di partenza.

Nella registrazione digitale, al contrario, la variazione di

pressione sonora viene scomposta in forma numerica binaria campionandola a intervalli regolari.

Vediamo le figg.25a e 25b che tentano di chiarire questo concetto: per trasformare in digitale un segnale analogico che varia nel tempo, occorre misurarne l'ampiezza a intervalli regolari, un'operazione che si definisce "campionamento".

È evidente, confrontando la fig. 25a con la fig. 25b, che tanto più breve sarà l'intervallo temporale tra due campionamenti successivi, (e quindi più elevata la frequenza di campionamento) tanto più la forma d'onda digitale sarà simile a quella originale analogica.

Ovviamente, in tutto questo, esistono dei limiti teorici, determinabili con il teorema di Shannon, il quale afferma che la massima frequenza riproducibile tramite un campionamento digitale è pari alla metà della frequenza di campionamento usata. Ad esempio, usando il campionamento tipico dei CD musicali a 44.100 Hz si potranno riprodurre le frequenze fino a 22.050 Hz.

Abbassando la frequenza di campionamento si va incontro a una riproduzione sempre più scadente, tuttavia, se si tratta semplicemente di registrare delle voci, non è necessaria una fedeltà elevata come nell'ascolto di un brano musicale. Accettando una minore qualità audio si potrà ottenere un risparmio della memoria necessaria alla registrazione. Infatti, un altro parametro basilare è il numero di bit necessario alla traduzione in valori numerici dell'ampiezza di ciascun punto campionato, che va sotto il nome di "quantizzazione". Ad esempio, usando 8 bit potremo "quantizzare" al massimo 256 livelli (infatti, 2^8 =256), mentre con un numero doppi di bit, ossia 16, potremo quantizzare 65.536 livelli (infatti 2^{16} =65.536).

All'aumento dei livelli di quantizzazione corrisponde quindi un miglioramento della qualità audio riprodotta che assomiglierà in maniera sempre maggiore alla forma d'onda originale fino a diventare indistinguibile da questa.

Naturalmente, se a un più alto numero di bit corrisponde una più alta la qualità del suono, nello stesso tempo corrisponde una maggiore quantità di memoria necessaria per la registrazione digitale.

Quanti bit sono necessari per contenere un certo tempo di registrazione? Facile da calcolare: N° di bit = bit di codifica x secondi di registrazione x frequenza di campionamento.

Ad esempio: 10 minuti (600 secondi) di registrazione a 16 bit con frequenza di campionamento 44.100 Hz occupano 16 x 600 x 44.100 = 423360 Kbit.

Nel caso di una registrazione stereofonica, essendo due i canali, lo spazio di memoria occupato si raddoppia.

Alcune fra le più recenti microspie GSM si limitano a registrare su una scheda di memoria e in formato digitale, i suoni prodotti nell'ambiente avviando il campionamento solo alla presenza di voci e interrompendolo quando nessuno parla.

La parte telefonica GSM è normalmente spenta e si attiva solo a un orario prefissato, per inviare i files registrati, che sono in formato compresso MP3, poi si spegne di nuovo.

Questo nuovo tipo di microspia è stato studiato proprio per renderla inintercettabile. Infatti, è perfettamente inutile cercarne il segnale con l'analizzatore di spettro o sollecitarla con uno jammer: quando la parte telefonica della "cimice" è spenta, non emette alcun segnale rilevabile, né riceve nulla.

Al momento dell'accensione, l'invio dei files dura solo pochi minuti ed è solo in questi brevi momenti che la microspia potrebbe essere individuata.

26. Le “microspie” nel computer

In questo capitolo non si parla di microspie “fisiche” nascoste all’interno di computer, anche se in qualche caso è realmente successo di rinvenire sofisticati dispositivi d’intercettazione in macchine da tavolo “desktop” grazie agli ampi spazi e all’alimentazione disponibile.
Non credo di andare troppo fuori tema, descrivendo sistemi d’intercettazione di tipo telematico, costituiti da immateriali quanto insidiosi software maligni definiti, non a caso, “malware”, contrazione dei termini inglesi “malicious” e “software” con il significato letterale di "programma malvagio".

Volendo tentare una prima classificazione di alcune categorie di “malware” che interessano l’argomento di questo libro e tenendo presente che la linea di separazione che le discrimina, quanto mai labile, è basata principalmente sugli effetti negativi sul computer involontario ospite, possiamo trascurare tutti quei codici maligni come:

- Virus: definizione generale di parti di codice maligno la cui specificità è diffondersi, autoreplicandosi, all'interno di programmi, o in particolari settori dell’hard-disk, in modo da andare in esecuzione ogni volta che il file infetto viene aperto. Si spostano fra computers diversi in seguito alla trasmissione di file infetti operato dagli utenti via internet o tramite supporti di memoria esterni.

- Worm: malware che non basano la propria diffusione sull’infezione diretta di altri file, ma agiscono sul sistema

operativo della macchina che involontariamente li ospita, in modo da essere eseguiti automaticamente e trasmettere copie di se stessi sfruttando il collegamento Internet, rimanendo attivi finché non si spegne il computer. Approfittano di alcuni difetti (bug) di certi programmi di posta elettronica, che rappresentano il veicolo preferito di infezione, e/o sistemi operativi per diffondersi. In linea generale, un worm semplice non causa altri danni se non un rallentamento del sistema con operazioni inutili, ripetitive o dannose. A volte però questi "malware, per evitare di essere individuati ed eliminati, interferiscono con il funzionamento di software di sicurezza, come antivirus e firewall. Inoltre, i worms possono fungere da veicolo per l'installazione di altri malware, come backdoor o keylogger, che potranno poi essere sfruttati da un cracker.

- Hijacker: prendono il controllo del browser di navigazione in rete violando la privacy dell'utente e causando l'apertura automatica e forzosa di pagine web indesiderate allo scopo di incrementare artificiosamente il numero di accessi (e di click) diretti a loro siti incrementando così le percentuali di guadagno collegate ad inserzioni pubblicitarie (banners).

- Rootkit: possiamo definirli come strumenti, coltellini svizzeri, che vanno ad occultare, tanto all'utente quanto a programmi antivirus, sia la propria presenza sia quella di particolari *spyware* e *trojan* tramite particolari impostazioni del sistema o files.

- Adware: contrazione dei termini inglesi "advertising supported software". Sono programmi software,

sovvenzionati da inserzioni pubblicitarie, che mostrano messaggi promozionali durante la navigazione internet, o anche durante l'uso del computer non collegato in rete. Causano malfunzionamenti quali rallentamenti e instabilità del pc e rischi per la privacy, comunicando le abitudini di navigazione dell'utente ad un server remoto appositamente predisposto

Alla fine questi "malware" sono poco più che forme di "cyberbullismo" messe in atto non da hacker, che sono ricercatori informatici positivi e si propongono di segnalare i "bug" dei sistemi ma da cracker maligni desiderosi di mostrare al mondo le proprie capacità informatiche e che si limitano, almeno nei casi citati, a provocare instabilità, malfunzionamenti e interferenze durante le sessioni di lavoro al computer.

Di tutt'altra specie e pericolosità sono i codici maligni elencati di seguito, la cui inoculazione nel computer ospite può avvenire durante collegamenti internet o durante scambi di files attraverso pennette di memoria, CD o altri supporti di memoria esterni, fra computer non adeguatamente protetti da antivirus aggiornati e/o validi firewall:

- Trojan horse: Il nome deriva dal famoso "cavallo di Troia". Si tratta di software composti, generalmente, da due parti: un file "server", che viene installato nel computer della vittima, e un file "client", usato dall'attaccante per inviare le istruzioni che il server deve eseguire. Il malware Trojan esegue istruzioni dannose senza il consenso dell'utilizzatore della macchina. Non possono auto-replicarsi e vengono inviati alla vittima che, involontariamente, non prestando attenzione ai siti

che sta visitando, scarica, un trojan sul proprio computer generalmente, attraverso la posta elettronica o altri applicativi internet.
Sono frequentemente usati come veicolo alternativo a worm e virus per iniettare delle backdoor o dei keylogger sui sistemi bersaglio con il fine di appropriarsi di informazioni sensibili quali numeri di carte di credito, password o anche indirizzi email.

- Backdoor: Sono vere e proprie "porte sul retro" attivate tramite alcuni *malware* ad opera di crackers intenzionati a manomettere il sistema. Permettono un accesso abusivo, tramite internet, alla macchina nella quale sono inoculati, poiché consentono di superare le procedure di sicurezza attivate in un sistema informatico.
  Sono, in genere, attivati da un trojan horse o da un worm.

- Spyware: sono processi maligni generalmente interessati alle chiavi crittografiche dell'utente, alle password utilizzate per le transazioni bancarie e ai dati relativi alle carte di credito utilizzate per i pagamenti in rete. Sono quanto di più simile, sul piano virtuale, alle microspie sul piano fisico.

- Keylogger: sono strumenti di "sniffing" software o anche hardware, predisposti per registrare tutto ciò che è digitato sulla tastiera o mediante il copia/incolla per trasmetterli via internet ad un destinatario interessato. Così come gli Spyware rendono possibile il furto delle chiavi crittografiche dell'utente, delle password utilizzate per le transazioni bancarie e dei dati relativi alle carte di credito utilizzate per i pagamenti in rete.
  Anche i siti internet visitati e le e-mail, inviate o ricevute,

sono facile preda dello spione o dello stalker e non costituiscono un caso infrequente di molestia. Ovviamente, i keyloggers sono progettati in modo da non suscitare sospetti sulla propria presenza, poiché non causano rallentamenti o altri malfunzionamenti della macchina. Esistono anche keyloggers hardware, anziché software, che sono installati sul computer da una persona che ha accesso fisico al pc. Si tratta di oggetti dall'aspetto di una prolunga o di una riduzione, che vanno collegati fra il cavo della tastiera e la relativa presa sul case del computer. Il funzionamento è analogo ai keyloggers software, ma i dati, in questo caso, possono essere prelevati anche collegando fisicamente il dispositivo alla presa USB di un computer e digitando un'apposita password.

I programmi malware appena elencati possono essere considerati l'equivalente informatico delle microspie di cui finora si è occupato questo libro, con la differenza di essere immateriali, virtuali, semplice codice di programmazione e tuttavia capace di spiare in modo subdolo i dati informatici con fini, ovviamente, illegali allo stesso modo con cui una microspia ambientale cattura le voci dei presenti.

Con lo sviluppo attuale dell'informatica, che ha portato il PC in ogni casa, oltre che in ogni ambiente di lavoro, sempre più spesso il tecnico della bonifica da microspie ambientali è affiancato dall'esperto di computer, attrezzato per la ricerca e la neutralizzazione del malware.

Non si tratta semplicemente di difendere il cliente dal pericolo, assolutamente reale, di trovarsi il conto corrente o il plafond della carta di credito prosciugato da malviventi che risiedono, magari, dall'altra parte del pianeta, oggi che la rete

internet rende del tutto ininfluenti le distanze geografiche, ma anche di prevenire il furto di dati sensibili legati all'elaborazione di disegni concernenti dei progetti industriali o all'esito di ricerche in campo farmaceutico, tanto per fare degli esempi.

La realizzazione di un brevetto, che ripagherebbe anni di lavoro e rilevanti investimenti, può essere vanificata in un attimo dalla fuga di notizie altamente riservate.

Naturalmente, anche in questi casi, prevenire è molto meglio che curare. Oggi che l'informazione è, a tutti gli effetti, un bene aziendale concreto, la sicurezza passiva e quella attiva diventano tra loro inscindibili ed entrambe indispensabili per raggiungere il necessario livello di protezione di un sistema.

Ogni organizzazione deve mettersi nelle condizioni di garantire la sicurezza dei propri dati, in un contesto dove i rischi causati dalle violazioni dei sistemi informatici sono in continua ascesa.

Dal punto di vista informatico è prassi comune, e certamente necessaria, far effettuare periodicamente un "penetration test" simulando, da parte di un tecnico di assoluta competenza che si mette nella posizione di un potenziale aggressore, un attacco al sistema informatico o alla rete aziendale da minacce esterne e/o interne, analizzando eventuali deficienze hardware o software. Si tratta quindi di un test dinamico dell'efficacia dei mezzi di difesa predisposti contro ingressi non autorizzati ai server aziendali: antivirus, firewall e quant'altro necessario.

27. Lavorare come tecnico per la bonifica da microspie

Diciamolo francamente: lavorare come tecnico elettronico alla ricerca/bonifica da microspie, non genera quasi mai un fatturato tale da consentire di "portare a casa la pagnotta".

Non si può neanche sperare di recuperare in tempi brevi l'investimento iniziale per l'acquisto delle attrezzature, che supera facilmente i 10mila euro per arrivare anche a oltre 20/30 mila.

Nonostante quest'attività possa essere molto ben remunerata e nonostante i tecnici in grado di eseguire una bonifica in modo professionale siano, in Italia, veramente pochi, altrettanto rarefatti sono i potenziali clienti.

Un ragionevole compromesso potrebbe essere, pertanto, considerare questo lavoro come complemento a un'altra attività come, ad esempio, quella d'investigatore privato o di consulente tecnico di parte (è questo il mio caso).

In effetti, buona parte dei miei incarichi, provengono da avvocati, a favore di loro clienti sottoposti a stalking o altre attività illegali d'invasione della sfera del privato.

Inoltre, alcune agenzie d'investigazione mi chiedono di collaborare in favore di loro clienti che hanno motivo di ritenersi spiati o, addirittura, hanno casualmente trovato una "cimice" nell'ufficio o nell'abitazione e temono ve ne siano di ulteriori, anche al fine di tentare di scoprire l'autore dell'intercettazione.

Nello svolgimento di questi incarichi potrebbe capitare di imbattersi in microspie "legali" installate a seguito di attività d'indagine della magistratura.

La bonifica, in questi casi, andrebbe a intralciare pesantemente gli accertamenti in corso facendo saltare la segretezza degli stessi e aprendo la strada alla concreta possibilità di essere incriminati per il reato di favoreggiamento personale (articolo 378 c.p.).

Purtroppo non è sempre facile capire, anche alla presenza del cliente che ci incarica della bonifica, chi si ha davanti. Non ci si

troverà mai in un sottoscala fumoso con personaggi dalle facce patibolari, pieni di tatuaggi e con la pistola infilata nella cintura dei pantaloni: queste situazioni avvengono solo nei film hollywoodiani!

Nessun cliente vi dirà mai che teme di essere indagato dalla Polizia o dalla Guardia di Finanza. Piuttosto s'inventerà una consorte gelosa che lo controlla a seguito di una sua scappatella extraconiugale o racconterà di essere in procinto di depositare un importante brevetto industriale e sospetta di essere spiato dalla concorrenza.

Sono molto più "sotterranei" i reati commessi dai cosiddetti "colletti bianchi" di fronte ai quali non c'è modo di capire con chi si ha realmente a che fare.

Come comportarsi, dunque, al fine di non essere involontariamente coinvolti nel reato di favoreggiamento?

Nell'ottica che "prevenire è sempre meglio che curare" è consigliabile sottoporre al cliente una "lettera d'incarico" sul modello di quella che trovate alla fine di questo capitolo allo scopo di cautelarsi contro possibili conseguenze penali.

La lettera, oltre a sollevarvi da tali responsabilità, termina con l'invito, nel caso di effettivo ritrovamento della "cimice", a sporgere denuncia contro ignoti per i reati elencati nella lettera stessa.

Al di là delle leggende, più o meno metropolitane, ritengo, questo è il mio sommesso parere, che non sia per nulla facile distinguere una microspia altamente professionale, che potrebbe essere stata installata dalla Polizia Giudiziaria, da un'altra, di caratteristiche tecniche più modeste, installata illegalmente da un soggetto privato.

L'evoluzione tecnologica di questi dispositivi elettronici è tale, come ho già scritto all'inizio di questo libro, da omologare a un livello sicuramente elevato tanto le microspie professionali quanto le "cimici" destinate al commercio al dettaglio o i localizzatori

geografici che uniscono le capacità del sistema satellitare GPS a quelle di trasmissione dei dati delle celle telefoniche.

A questo fanno unicamente eccezione le varie microtelecamere e microfoni ambientali, occultati dentro oggetti di uso comune, orologi, radiosveglie, attaccapanni ecc. di provenienza orientale che potrebbero interessare lo "spione" dilettante.

27.1. Modello di lettera di incarico

Roma, / / 2014

Spett.……
Via…….....
Città……(CAP)……

OGGETTO: Lettera di incarico

Io sottoscritto,……
tecnico in (indicare le proprie qualifiche professionali)
d'ora in avanti chiamato "prestatore d'opera", ho ricevuto
in data / / 2013, dal sig. …… d'ora
in avanti chiamato "committente", residente in
via ……
con codice fiscale /partita IVA ……....
identificato mediante documento…….
rilasciato da ……. in data ……, l'incarico di procedere alla bonifica da eventuali microspie e/o telecamere occultate e/o altri dispositivi d'intercettazione ambientale o telefonica, (nell'abitazione) (nell'autovettura) (nell'attività commerciale) (nell'azienda) sita in via……(indirizzo, città).

Il committente dichiara di avere la legale disponibilità e/o

proprietà (dell'abitazione) (dell'autovettura) (dell'attività commerciale) (dell'azienda) suddetta e, con la propria firma apposta in calce alla presente, s'impegna a manlevare, ovvero tenere indenne da responsabilità legali e/o richieste di rimborsi**,** di danni, ecc. il prestatore d'opera.

descrizione del lavoro richiesto:

Il prestatore d'opera s'impegna a eseguire una ricerca accurata di eventuali microspie e/o telecamere occultate e/o altri dispositivi d'intercettazione ambientale o telefonica, negli ambienti indicati dal committente e citati nel preventivo di spesa accettato dal committente, attraverso l'uso dei dispositivi elettronici ritenuti idonei dal prestatore d'opera stesso, riguardo alle specifiche caratteristiche degli ambienti.

S'impegna inoltre a eseguire il lavoro con diligenza e a regola d'arte e a comunicare tempestivamente al committente eventuali lavori ulteriori e imprevisti, rispetto a quelli preventivati, che si rendessero necessari per il compimento dell'opera e il loro costo, che dovrà essere espressamente accettato dal committente.

data d'inizio del lavoro ……

data stimata di ultimazione del lavoro……

eventuali richieste particolari del committente:

……

……...…….……..

Costo bonifica - I.V.A. ESCLUSA	€	
I.V.A. 22%	€	
TOTALE.:	€	

CONDIZIONI DI PAGAMENTO:

Acconto all'ordine	€	
Saldo a fine lavori	€	

Il saldo, oltre l'iva, dovrà essere versato alla consegna del lavoro.

Questo contratto d'opera, consistente in due pagine e redatto in duplice copia, è sottoposto esclusivamente alle condizioni suesposte e alle leggi vigenti (art. 2222 e segg. codice civile).

Firma del committente Firma del prestatore d'opera

…… ..……...

27.2. Modello di relazione esiti della bonifica

Roma, / / 2014

Spett.……
Via…….....
Città……(CAP)……

OGGETTO: Esiti della bonifica da microspie:

(Barrare la tabella che non interessa)

Esito negativo:

Dalle ricognizioni visive e strumentali compiute nei locali indicati nella lettera d'incarico e lungo la linea telefonica commutata, **non** risultano presenti microspie e/o telecamere occultate e/o altri dispositivi d'intercettazione ambientale o telefonica.

Esito positivo:

Dall'analisi dei dati precedenti e dalle ricognizioni effettuate nei locali indicati nella lettera d'incarico e lungo la linea telefonica commutata, sono stati individuati i seguenti dispositivi d'intercettazione:
Dispositivo: ……
Occultato in: …….
Dispositivo: ……..
Occultato in: ……..
Dispositivo: ……..
Occultato in: ……..

Conclusioni:

A conclusione dello svolgimento dell'incarico, si consiglia al committente di sporgere denuncia (contro ignoti) alle autorità di P.S. ai sensi della Legge n. **98/1974 art. 615-bis c.p.** (*Interferenze illecite nella vita privata*), **617 c.p.** (*Cognizione, interruzione o impedimento illeciti di comunicazioni o conversazioni telegrafiche o telefoniche*) e **617-bis c.p.** (*Installazione di apparecchiature atte a intercettare o impedire comunicazioni o conversazioni telegrafiche o telefoniche*), poiché i delitti citati sono punibili a querela della persona offesa.

Tanto si comunica a conclusione dello svolgimento dell'incarico.

Il tecnico ……

Luogo e data ……

(Copia per il committente)

(Copia per il prestatore d'opera)

28. Costruzione di una stanza a prova di intercettazioni

Eseguire una bonifica, alla ricerca di eventuali dispositivi nascosti d'intercettazione ambientale audio e/o video, per quanto effettuata da persone realmente competenti, con ogni accuratezza e supportata dai migliori e più sofisticati congegni antispia, anche se ha dato esito sicuramente negativo, non può in nessun modo garantire che, a distanza di giorni o anche di poche ore, personaggi interessati a venire a conoscenza di notizie riservate, non installino una microspia.

La situazione sarebbe doppiamente rischiosa per la vittima dell'intercettazione che, sentendosi oramai al sicuro, vista la bonifica da poco realizzata, potrebbe abbassare la guardia e lasciarsi sfuggire particolari riguardanti argomenti riservati.

Quando si trattano, per ragioni di lavoro, dati classificati, non è certo possibile vivere in uno stato paranoico di continua allerta né è realistico pensare di riunire i propri collaboratori al centro di un campo all'aperto per parlare dei progetti in corso di studio o delle offerte per una gara di appalto, al fine di evitare ascolti indiscreti.

La soluzione, pratica e reale, esiste e si chiama "bunker anti-intercettazioni".

Si tratta di attrezzare un locale, o di realizzarne uno apposito, rivestendo le pareti con speciali pannelli in grado di schermare le radiazioni elettromagnetiche in un range di frequenza compreso fra 10 KHz e 18 GHz: in pratica tutta la gamma delle onde radio utilizzate da ogni tipo possibile di microspia ambientale, da telecamere IP nascoste e dai telefoni cellulari gsm, umts, gprs, 3g, 4g ecc.

L'attenuazione che questi pannelli sono in grado di offrire si aggira sui 45 ÷ 70 dB. In concreto nessun segnale è in grado di entrare o uscire dalla stanza anti-intercettazioni.

In effetti, l'efficacia schermante di un pannello, è direttamente legata alla sua "conducibilità elettrica", alla sua "permeabilità

magnetica”, alla frequenza massima che si vuole bloccare ed allo spessore del materiale utilizzato. Il risultato complessivo, dipendente dalla combinazione fra le “perdite per riflessione" e le "perdite per assorbimento", definita “shielding effectiveness” è funzione del rapporto tra l'intensità di campo presente in un punto della stanza, prima e dopo la posa in opera dello schermo.

In origine queste pannellature, realizzate con fibre di carbonio o con fili metallici intrecciati, erano state studiate in ambito militare nella schermatura “Tempest” per impedire l'intercettazione d’informazioni riservate effettuata mediante la captazione dei campi elettromagnetici emessi dalle attrezzature informatiche, in particolar modo dai monitor a tubi catodici.

Naturalmente non bisogna trascurare le superfici vetrate che dovranno essere rivestite con speciali tessuti schermanti con bassa attenuazione della luce, che ricordano molto da vicino certe tende antizanzare.

In alternativa, ove occorra un più marcato effetto schermante, sono disponibili vetri al cui interno è inglobata, con una lavorazione in autoclave, una rete metallica in rame-nickel.

Un buon livello di sicurezza si raggiunge contenendo la dimensione massima di qualsiasi apertura, non schermata, verso l’esterno entro 1/10 della lunghezza d'onda minima che si vuole schermare. Alla frequenza usata dai telefoni cellulari questo significa aperture non più grandi di 3 cm, un valore evidentemente incompatibile non solo con le dimensioni delle porte e delle finestre, ma anche con una semplice presa di ventilazione.

Ecco spiegata la ragione per cui, di solito, è possibile utilizzare il telefonino anche dentro casa.

La rete elettrica, in entrata nella stanza, può comportarsi facilmente come un’antenna, permettendo l’uscita di parte del segnale di un’eventuale microspia.

Purtroppo, non potendo esimersi dal fornire alimentazione elettrica al locale schermato, i cavi dovranno essere dotati di

speciali filtri in grado di arrestare la radiofrequenza.

L'impianto di aerazione o climatizzazione, se necessario, presentando aperture di considerevole diametro, certo superiore ai fatidici 3 cm, deve essere anch'esso munito di appositi schermi nei punti di ingresso al locale.

Al contrario, l'impianto telefonico, anche se solo interno, non deve essere per niente presente, costituendo, ovviamente, l'anello debole della catena. Un ipotetico dispositivo che impedisse l'ascolto delle conversazioni ambientali attraverso questo servizio ne impedirebbe anche l'uso, per così dire, legittimo. Quindi, tanto vale eliminare del tutto l'impianto telefonico rinunciandovi per il tempo della riunione riservata.

Un accessorio praticamente indispensabile nel locale anti-intercettazioni è l'inibitore di registratori e di microfoni in grado di impedirne il funzionamento, siano essi digitali o a nastro magnetico. Lo scopo è, ovviamente, prevenire l'uso di microregistratori nascosti.

La stanza anti-intercettazioni dovrà essere sottoposta a controllo degli accessi H24 in maniera da impedirne la manomissione tesa a diminuirne l'efficacia schermante, e dovrà anche essere insonorizzata per evitare che un semplice origliare alla porta vanifichi in un attimo tanti sforzi e tanta tecnologia.

29. Alcuni casi reali di bonifica:

Fine di un molestatore:

La signora R.C. abitante in un quartiere residenziale di una città dell'Italia meridionale, era insistentemente molestata da un suo "ex".

Telefonate a tutte le ore del giorno e della notte, messaggi al cellulare, pedinamenti ossessivi, violente scenate in pubblico, avevano costretto la signora a denunciare il molestatore per il reato di "stalking" nella speranza di veder terminare questi atti persecutori. Inutilmente.

Arriva il giorno in cui l'uomo, programmatore informatico presso un'importante azienda di telecomunicazioni, è trasferito in un nuovo centro nel nord dell'Italia.

La signora R.C. trova finalmente un periodo di pace che è presto interrotto dal molestatore che sembra a conoscenza di tutti i suoi movimenti: la rimprovera di non essersi recata al lavoro in un certo giorno, vuole sapere il motivo, cosa ha fatto in casa!

Poi riprendono le telefonate ossessive e i messaggi sul cellulare e nella posta elettronica, finché la signora, esasperata, torna dai Carabinieri e sporge una nuova denuncia.

Neanche un'ora dopo lui le telefona, minacciandola per ciò che ha fatto, perfettamente a conoscenza dei suoi spostamenti. Troppo perfettamente!

Conosce il contenuto delle sue e-mail, sa delle sue telefonate e dei suoi SMS. Troppo perfettamente!

Inizia la bonifica:

Veniamo messi in contatto con il legale della signora R. che ci incarica di bonificare l'abitazione, il cellulare il computer e la macchina.

Dopo un breve esame tecnico, scopriamo che il cellulare era stato regalato alla signora proprio dal molestatore, che aveva provveduto a installare uno speciale software in grado di rinviargli il testo di tutti gli SMS e i numeri telefonici chiamati.

Il computer era affetto da un trojan che rilanciava ogni attività, e-mail, siti visitati ecc. A un server situato fuori dai confini nazionali, al quale l'uomo aveva, ovviamente, accesso.

Poco dopo iniziamo la ricerca di microspie occultate: dopo una breve ricognizione, gli strumenti di analisi dello spettro radio individuano una spia GSM/GPS occultata sotto il pianale della macchina, fissata con un paio di fascette da elettricista.

Si trattava di un dispositivo in grado di telefonare a un cellulare dello stalker segnalando la posizione della vettura su una mappa geografica. (Ovviamente ambedue le SIM, chiamante e ricevente, erano intestate a una persona deceduta!).

Evidentemente l'uomo, che aveva una copia delle chiavi della macchina e del passo carrabile dove era parcheggiata, aveva avuto il tempo di fare un lavoro accurato, collegando persino la microspia con la batteria dell'automobile mediante due sottili fili elettrici.

A questo punto occorreva dimostrare l'identità del molestatore: mi viene un'idea: allentare uno dei fili di alimentazione della spia così che sembrasse staccato a causa delle vibrazioni del motore!

Poi, installiamo tre telecamere nascoste. Una riprendeva l'ingresso del passo carrabile, la seconda l'automobile e la terza, occultata in un furgoncino parcheggiato che conteneva anche un videoregistratore "time-lapse", il cancello dall'esterno.

Passano così venti giorni senza che nulla accada poi, alle tre di una notte, arriva il molestatore… apre il cancello, entra, si sdraia sotto la macchina e controlla la microspia: sembra in ordine, nessuno l'ha rimossa! Apre il cofano e controlla i fili vicino alla batteria. Ah ecco cosa è successo! un filo staccato…bene. Provvede quindi a riallacciare il collegamento, armeggia un po',

forse per fissarlo meglio evitando che si stacchi di nuovo costringendolo a un lungo viaggio per ripristinarne il funzionamento.

Il giorno successivo la signora torna, insieme al suo legale, nella locale stazione dell'Arma. Quando lui la chiamerà, furioso, per sapere cosa è andata a raccontare ai Carabinieri, lei soddisferà la sua curiosità morbosa: "Sono andata a consegnare le prove che t'inchiodano alle tue responsabilità!".

Un molestatore "dilettante"

La signora M.T. di Roma, era molestata insistentemente da un corteggiatore, suo collega di lavoro, nonostante fosse sposata già da qualche anno.

Le solite denunce alle autorità non sembravano sortire alcun effetto positivo.

Improvvisamente, l'insistente corteggiatore sembrava conoscere il contenuto delle telefonate della signora M. i cui argomenti riferiva alla stessa vittima.

I coniugi facevano quindi una ricerca in internet, arrivando al mio sito. Ero quindi contattato con una e-mail per fissare un appuntamento.

Inizia la bonifica:

Il giorno stabilito eseguo una verifica elettronica nell'abitazione della signora, senza trovare nulla. Controllo quindi la sua automobile, con il medesimo risultato.

Mi viene in mente di controllare lo sportello di derivazione Telecom, posto nelle cantine del condominio e… bingo!

La serratura è palesemente forzata e all'interno trovo un microregistratore digitale, incartato in un foglio di alluminio da

cucina, collegato ai morsetti telefonici con due pinzette a coccodrillo. Un lavoro banale e dilettantesco ma indubbiamente efficace.

Dopo aver scattato alcune foto del registratore e della serratura manomessa, decidiamo di piazzare, nella cantina della signora M. T. un videoregistratore di sorveglianza con una telecamera puntata sull'armadio Telecom.

Inoltre, mi viene chiesto di redigere una perizia tecnica asseverata a giuramento che descriva quanto ho trovato, per supportare una successiva denuncia.

A distanza di tre mesi, però, il molestatore non è tornato a sostituire le batterie del registratore. Forse avrà "mangiato la foglia", non lo sapremo mai.

Fatto sta che, dopo la scoperta del registratore, le molestie che andavano avanti da più di un anno, sono improvvisamente cessate. Va bene così!

Una multinazionale troppo curiosa

Il sig. R.N. rappresentante di una grossa multinazionale, mi contatta, su indicazione di un comune amico, perché teme che i suoi spostamenti siano controllati dai suoi superiori diretti.

Alcune sue parole, pronunciate mentre viaggiava in macchina con un collega, sono giunte alle orecchie di un dirigente, così come alcuni suoi itinerari, durante le ore di lavoro.

Bisogna precisare che l'automobile da lui utilizzata è un mezzo di proprietà della multinazionale stessa che lui preleva dalla rimessa aziendale il lunedì mattina, per poi riconsegnarlo il venerdì sera, al termine dell'orario di lavoro. Quindi, se qualcuno che ha accesso al garage volesse nascondere una microspia all'interno dell'abitacolo, non incontrerebbe particolari difficoltà né correrebbe alcun rischio.

Inizia la bonifica:

Invito quindi il sig. R.N. a parcheggiare l'automobile in un mio box, appositamente attrezzato, dove inizio le operazioni di ricerca/bonifica che si risolvono rapidamente in una ventina di minuti con la scoperta di una "cimice" audio GSM inserita nella gommapiuma sotto il sedile a lato del conducente e collegata all'alimentazione del sedile regolabile elettricamente.

Inoltre, sotto al pianale del lunotto posteriore trovo un localizzatore GSM in grado di memorizzare gli itinerari percorsi con un'approssimazione di pochi metri.

Nonostante le apparenze, chi ha piazzato le due "cimici" non era certo un professionista nel campo e non ha saputo nasconderle con sufficiente abilità.

Il mio lavoro termina con la consegna di una relazione tecnica debitamente firmata e con l'invito a rivolgersi alle Autorità di Polizia per formalizzare una denuncia contro ignoti, ma il cliente preferisce lasciare le "cimici" al loro posto.

Conoscendo la loro presenza si comporterà adeguatamente. Inoltre teme che una denuncia possa portare a ritorsioni nei suoi confronti e persino al trasferimento in una sede in altra città.

Appendice

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

È a tutti noto che anche l'autorità di polizia giudiziaria, qualora

nello svolgimento delle indagini debba eseguire un'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 del libro, 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 s'introduce nell'abitazione altrui, o in un altro luogo di privata dimora, o nelle loro appartenenze, 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 a 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 d'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. 617-bis. Installazione di apparecchiature atte a intercettare o 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 o 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.

Bibliografia

- R. Baroggi: Elaborazione e trasmissione dei dati a distanza: tecniche e metodologie, Angeli, Milano 1984
- L. Bertoni: Le intercettazioni. Mezzo di ricerca della prova nel processo, Nuova Giuridica, Macerata 2012
- J. Gleick: L'informazione. Una storia. Una teoria. Un diluvio, Feltrinelli, Milano 2012
- D. M. Huber: Robert E. Runstein, Manuale della registrazione sonora: Concetti generali, tecnologia audio analogica e digitale, attrezzature, procedure, Hoepli, Milano 1999
- W. Junghans: Il libro dei registratori audio, Franco Muzzio, Padova 1983
- Nazzaro Giovanni: Le intercettazioni sulle reti cellulari, Mattioli, Fidenza
- A. Paoloni, D. Zavattaro: Intercettazioni telefoniche e ambientali, Centro Scientifico Editore, Torino 2007
- G. Praetzel, E. F. Warnke: Il libro dei microfoni, Franco Muzzio, Padova 1979
- U. Rapetto, R. Di Nunzio: L'atlante delle spie: dall'antichità al "Grande Gioco" a oggi, Rizzoli, Milano 2002
- A. Tessitore, C. Marino: Intercettazioni elettroniche e informatiche, le tecniche, Sandit, Albino (BG)