Sicurezza & Contro-Sorveglianza

Informazione contro lo Stato di Polizia

Strategie repressive e movimenti di resistenza negli USA

NdT
Nota dei traduttori:

abbiamo rimpaginato, illustrato e tradotto integralmente questo opuscolo pubblicato a Vancouver nel 2009, sebbene esponga situazioni per lo più specifiche della repressione nord-americana, perché vogliamo diffondere informazioni sulle ultime frontiere della sorveglianza estera.

L'arte di sorvegliare e di reprimere non è un fenomeno statico ma un continuo evolversi e l'america è l'avanguardia mondiale del controllo sociale, un modello di ispirazione per tutte le polizie d'occidente e un laboratorio per le nuove tecnologie della sorveglianza.

Se abbiamo mantenuto i capitoli sulla repressione dei movimenti di resistenza americani è soprattutto per il peso che questi episodi storici hanno avuto per la consapevolezza dell'attivismo contemporaneo; inoltre vogliamo sottolineare che gran parte di questi movimenti di resistenza agirono secondo approcci politici molto lontani dall'ethos anarchico: l'anarchia implica il rigetto per la gerarchia e l'autoritarismo e di conseguenza si manifesta in una moltitudine di realtà politiche decentrate, senza capimandria ne strutture verticistiche, nell'orizzontalità decisionale e all'insegna della libera iniziativa degli individui.

Non condividiamo necessariamente tutte le dichiarazioni contenute nell'opuscolo da noi tradotto, non intendiamo spargere inutili paranoie tra gli/le attivisti/e nostrani/e e non vogliamo incoraggiare la pratica di alcuna azione illegale; proponendo questa traduzione vogliamo semplicemente informare sulle lotte dei movimenti di resistenza d'oltreoceano, permettendo alle persone di conoscere realtà politiche eterogenee e di elaborare un proprio pensiero critico al riguardo.

Inoltre abbiamo inserito alcune note aggiuntive per completare ed arricchire il contenuto del testo, che spesso presenta contesti e situazioni che potrebbero risultare al/alla lettore/lettrice poco familiari...

gennaio 2013

Traduzione in lingua itagliana dell'opuscolo pubblicato negli USA:

"Security & Counter-Surveillance, Information against Police State"

scaricabile liberamente nella versione originale in lingua inglese dal link:

http://anti-politics.net/distro/2009/warriorsecurity-read.pdf

Traduzioni e grafiche del progetto *Grafica Nera*:

http://graficanera.noblogs.org

GRAFICA NERA

Contenuti

edizione 2009, Vancouver, Canada / zona Coast Salish

1) Introduzione **2**

2) La Sorveglianza **2**

3) La Sicurezza **2**

4) Principi della Sorveglianza **3**

5) Sorveglianza fisica **3**

Operatori e veicoli

Sorveglianza mista

Sorveglianza mobile

Quattro fasi della sorveglianza mobile

Altre forme di sorveglianza

6) Sorveglianza tecnologica **6**

Telecomunicazioni

Dispositivi per la registrazione vocale

Microfoni parabolici

Videocamere

Acquisire fotografie

Apparecchi per il rintracciamento

7) Scovare la Sorveglianza **10**

Sorveglianza fisica

Sorveglianza tecnologica

8) Aggirare la Sorveglianza **18**

9) Informatori ed Infiltrati **19**

Come comportarsi

10) FBI & COINTEL-PRO **22**

Metodi COINTEL-PRO dell'FBI

COINTEL-PRO: alcuni episodi

11) Alcuni episodi di Informatori ed Infiltrati **27**

12) Linee Guida per la Sicurezza **28**

" Coloro che esercitano l'autorità temono la maschera perché il loro potere consiste in parte nell'identificare, nello stampare e nel catalogare: nel sapere chi sei... Le nostre maschere non servono per celare la nostra identità ma per rivelarla... "

Testo stampato all'interno di 9000 maschere distribuite durante il Carnevale contro il Capitalismo; Londra, Giugno 1999.

Il Grande Fratello ti osserva, molto più di prima.

Sempre di più la sorveglianza dimostra di essere la rotta verso cui il mondo si sta organizzando.

Si stima che la Gran Bretagna abbia circa 4,2 milioni di telecamere a circuito chiuso (CCTV), la media di una telecamera per ogni 14 cittadini.

Le persone che attraversano il centro di Londra vengono inquadrate dalle telecamere circa 300 volte al giorno.

La sorveglianza è una condizione propria della modernità, integrata nello sviluppo del moderno stato-nazione e del capitalismo...

Molto più di prima, le nostre vite sono monitorate da altri, dalle agenzie governative ai servizi di sicurezza fino ai proprietari dei siti web in cui navighiamo e dei negozi in cui compriamo. Loro ci monitorano in pubblico, sul lavoro e sul web, raccogliendo le nostre informazioni personali in enormi archivi e catalogandoci in base al rischio, valore e attendibilità.

Le telecamere a circuito chiuso CCTV sono solamente uno dei loro tanti strumenti a disposizione. Altri includono i chip RFID (Radio Frequency IDentification), gli apparecchi GPS per la geolocalizzazione, i cookies dei siti web, i software per l'identificazione facciale e le tessere fedeltà dei negozi. I programmi dei computer usati dai servizi segreti possono monitorare ed analizzare miliardi di telefonate ed e-mail in tempo reale. Noi agevoliamo il lavoro a quelli che ci sorvegliano regalando dettagli preziosi della nostra vita privata ai social network come Facebook o ai questionari telematici.

Bene o male la sorveglianza è sempre stata parte delle civiltà. Ciò che c'è di nuovo è la possibilità di integrare diverse fonti di informazione con la tecnologia informatica.

Dopo l'11 settembre la nostra ossessione del prevenire i pericoli ha generato un apparato di sorveglianza di massa in cui ogni individuo viene trattato come un sospetto.

Don Butler, " Il Grande Fratello ti osserva, molto più di prima", Vancouver Sun, 3 Feb. 2009

E per quelli che sono davvero "sospetti" continuate a leggere...

1. Introduzione

La sicurezza è vitale per il successo e la sopravvivenza dei movimenti di resistenza. Ciò è per il semplice motivo che abbiamo un nemico che lavora attivamente per ostacolarci, neutralizzarci e infine distruggerci. Non prestare attenzione riguardo a tutto ciò che concerne la sicurezza può determinare l'esito tra la vittoria e la sconfitta, tra la libertà e l'imprigionamento, tra la vita e la morte. Non solo per te stesso, ma per tutte le persone attorno a te.

L'informazione raccolta da varie fonti e sottoposta a varie analisi e confronti viene chiamata "intelligence". L'azione dell'intelligence è una parte vitale delle operazioni di contro-insurrezione, senza cui il nemico non saprebbe chi, cosa, dove e quando colpire.

Le misure di sicurezza e di contro-sorveglianza sono state designate per limitare ed arginare il flusso di informazioni verso le forze nemiche. Si basano sul principio che la contro-insurrezione sia un aspetto permanente della società e che coloro che sono impegnati nella resistenza sono sempre vulnerabili alla sorveglianza e alla repressione.

2. La Sorveglianza

La sorveglianza è l'osservazione costante e segreta delle persone, dei luoghi, delle cose o degli oggetti, al fine di ottenere informazioni.

Ci sono due tipi di sorveglianza: sorveglianza fisica e tecnologica.

La sorveglianza fisica viene esercitata dal nemico di persona a piedi e/o su veicoli. E' l'unica maniera con cui il target sorvegliato può essere posto sotto continua osservazione in un periodo di tempo esteso. Le squadre addette alla sorveglianza possono essere composte da due persone in un veicolo, o da una dozzina di operatori in sei veicoli (o ancora di più ovviamente). In aggiunta a ciò, possono essere utilizzati motociclette, bici, aerei ed elicotteri.

Dentro questa categoria dobbiamo considerare anche gli informatori, gli infiltrati e i collaboratori. Forse possono essere agenti di polizia, civili reclutati dalla polizia o vecchi compagni.
Questa forma di sorveglianza è la principale fonte di informazioni che l'intelligence dispone per conoscere i pensieri della gente, i loro piani e le loro attività. A volte viene definita "Human intelligence". Per la natura sensibile delle informazioni personali che sono in grado di raccogliere e per la loro abilità di influenzare gli eventi, gli infiltrati e gli informatori sono particolarmente dannosi.

La sorveglianza tecnologica è molto più diffusa. Con un largo utilizzo di telecomunicazioni (telefoni, cellulari, internet, fax, etc.) la sorveglianza tecnologica è la principale fonte dell'intelligence per quanto concerne le attività quotidiane del target sorvegliato, i contatti, le relazioni personali, etc. Più in generale questa consiste in congegni tecnologici per la registrazione, la documentazione o il monitoraggio dei movimenti, le conversazioni e le attività del target sorvegliato. Questa include congegni per l'ascolto dentro le case e le auto, nei telefoni intercettati, nel monitoraggio dell'attività su internet, nei video delle telecamere CCTV, nei dispositivi per la localizzazione, negli strumenti per la visione notturna, etc.

Tanto più grossa è la massa di gente, tanto più l'ambiente urbano agevola la sorveglianza, le comunicazioni e i sistemi elettronici, le strutture e i veicoli in cui gli operatori e i congegni possono essere nascosti. Nella città di solito sono presenti decine di migliaia di telecamere CCTV, nei negozi, nelle banche, nei centri commerciali, in uffici, scuole, transit, strade ed intersezioni.

Nelle zone rurali, la sorveglianza fisica spesso è molto più necessaria per via della mancanza di telecomunicazioni, strade, etc. Le zone di bassa concentrazione demografica rendono facile identificare gli operatori della sorveglianza come "stranieri". Per questo motivo la sorveglianza fisica in queste zone rurali spesso necessita di strumenti di osservazione a lungo raggio (con obbiettivi potenti, veicoli aerei o in situazioni di estrema priorità, di satelliti). In certe situazioni la polizia può esercitare la sorveglianza in un raggio d'azione molto ristretto camuffandosi con abbigliamenti militari-mimetici.

3. La Sicurezza

Sicurezza
definizione n°1: misure adottate per difendersi contro gli attacchi, il furto o la divulgazione.
definizione n°2: tutto ciò che conferisce o garantisce tranquillità e confidenza...

Come notato, l'obbiettivo della sicurezza è proteggere il nostro movimento. Un aspetto vitale di questo obbiettivo è limitare o chiudere del tutto il flusso di informazioni alle forze nemiche. I seguenti 4 principi vanno intesi come linee guida basilari e fondamentali:

1. Non discutere ne mandare informazioni sensibili tramite qualsiasi forma di telecomunicazione (telefono, cellulare, internet, etc.) perché ognuna di queste è vulnerabile alle intercettazioni. I telefoni cellulari possono diventare apparecchi per l'intercettazione dei suoni e perciò bisogna quantomeno rimuovere la batteria prima di discutere di qualsiasi informazione sensibile.

2. Non discutere mai di informazioni sensibili in qualsiasi spazio chiuso vulnerabile ai congegni di ricezione (per esempio le case, i veicoli, i caffè, etc.)

3. Rispetta la regola del "far-sapere-solo-ciò-che-serve-far-sapere": se una persona non è coinvolta nell'informazione, non deve conoscerne i contenuti. Meno gli altri conoscono e minore sarà il rischio che l'informazione fugga e finisca in mani sbagliate.

4. Evita le persone che non sono nelle condizioni di rispettare i principi basilari per la sicurezza. Queste sono un pericolo per te e per tutto il movimento. Tra di loro si includono le persone che parlano troppo, che non prendono seriamente la sicurezza, che eccedono con gli alcoolici, etc.

4. Principi della Sorveglianza

Come già sottolineato, la sorveglianza è l'osservazione costante e segreta di una persona, di un luogo, di un veicolo o di un oggetto al fine di ottenere informazioni. Per risultare efficiente, la sorveglianza non deve essere notata ne scoperta. Appena il target sorvegliato si accorge di essere sotto sorveglianza, trasformerà il suo comportamento e le sue abitudini per nascondere ogni attività "sospetta" ed impedire la fuga di informazioni. Perciò la sorveglianza può risultare difficile da individuare, proprio perché mira ad essere coperta e segreta.

Incrementare l'informazione attraverso la sorveglianza è un processo graduale e lento. L'attività di sorveglianza assomiglia più ad un lavoro di ricongiungimento di tanti brandelli di informazione che ad una presa diretta e frontale della vita del target sorvegliato.

La sorveglianza di solito comincia con informazioni limitate sulle attività del target sorvegliato, la residenza o il luogo del lavoro, etc. Maggiori informazioni saranno raccolte al fine di identificare i tempi, i luoghi, gli orari di lavoro o attività su cui rafforzare la sorveglianza (dicasi "**analisi del comportamento del target**").

Maggiore sarà la sorveglianza esercitata con sforzo e maggiori saranno i risultati dell'intelligence. L'intensità della sorveglianza dipende dalla importanza conferita al target sorvegliato dalla polizia/ intelligence ed anche dalla consapevolezza che il target sorvegliato assume riguardo alle strategie di contro-sorveglianza (target facile / target difficile). Anche solamente leggendo questo opuscolo puoi raggiungere il livello di un target difficile.

Considerate le risorse e le capacità del nostro nemico e la sua volontà di monitorare e reprimere tutte le tendenze ribelli e non-sottomesse (di cui si suppone noi ne facciamo parte), occorre sempre considerare possibile (se non probabile) la sorveglianza contro i nostri movimenti.

5. Sorveglianza fisica

La sorveglianza fisica viene esercitata da persone reali (operatori) a piedi e/o su veicoli. E' l'unico modo con cui un target sorvegliato può essere tenuto sotto osservazione per un periodo di tempo esteso. A piedi o con un veicolo, gli operatori devono tenere il loro target bene in vista. Quando un gruppo di operatori ha l'incarico di mantenere il target sotto costante osservazione si dice che ha il "**comando**" del target (*"command" NdT*). Per non svelare la propria attività di sorveglianza, il gruppo di operatori che detiene il comando viene variato spesso, affinché nessun operatore possa risultare agli occhi del target sorvegliato una presenza fin troppo presente e quindi sospetta (dicasi "**cambio del comando**").

Strategie di sorveglianza particolarmente sofisticate possono coinvolgere diversi operatori e diversi veicoli. In questi casi i gruppi di operatori sono distribuiti attorno al target sorvegliato in una "scatola galleggiante" (*"floating box" in inglese, NdT*) ossia disposti di fronte, di dietro, sui lati e su strade parallele.

Se la sorveglianza fisica esce di scena, può subentrare la sorveglianza tecnologica, e forse può essere già stata messa in funzione molto prima che cominci la stessa sorveglianza fisica. Questo è per via del fatto che la sorveglianza fisica necessita di diverse persone e di diverse risorse. Oltretutto è possibile che gli operatori della sorveglianza abbiano accesso alle intercettazioni sonore delle conversazioni del target sorvegliato da lui pronunciate in casa o in auto proprio nel momento in cui lo stanno tenendo sotto osservazione.

Operatori della sorveglianza e i veicoli

Gli operatori della sorveglianza possono appartenere a qualsiasi gruppo etnico, avere qualsiasi tipo di corporatura, etc. indossare qualsiasi tipologia di

vestiario, rifarsi a qualsiasi tipo di subcultura etc. Non solo i poliziotti e i membri dell'intelligence agiscono come operatori della sorveglianza, ma anche i civili e i membri delle normali famiglie possono essere reclutati per questo obbiettivo. Possono essere uomini, donne, giovani ed anziani (come i vigilanti della RCMP dei primi anni '80). Allo stesso modo i veicoli usati dai gruppi di operatori della sorveglianza possono essere di qualsiasi modello, anno, condizione, colore, etc. La stessa apparenza degli operatori non deve far emergere gli innumerevoli sforzi per mantenere la sorveglianza. Invece, sono proprio le loro attività di sorveglianza che occorre sorvegliare.

Al fine di coordinare gli sforzi di molti operatori del gruppo, questi sono costretti ad indossare apparecchiature per comunicare tra di loro. Di solito queste apparecchiature consistono in oggetti chiaramente funzionali alla comunicazione, come auricolari di plastica piazzati nell'orecchio, microfoni attaccati sulle giacche o sulle magliette all'altezza del collo. Nella tasca può essere riposta l'apparecchiatura più voluminosa con i tasti per le varie funzioni. Varianti di questi strumenti possono includere cellulari con l'attacco per la voce e l'orecchio, lettori MP3 o iPod, etc. Il proliferare di queste apparecchiature per la musica e la telefonia portatile rende molto difficile identificare gli operatori di sorveglianza, poiché queste tecnologie possono inglobare gli strumenti della sorveglianza usati dagli operatori per coordinarsi.

Sorveglianza fissa

La sorveglianza fissa (che non si sposta) viene posizionata attorno alla casa, al luogo del lavoro o attorno ai posti più frequentati del target sorvegliato, al fine di conoscerne le attività, le abitudini, o anche per cominciare la sorveglianza di un target che si suppone debba sopraggiungere in quel luogo stabilito, (dicasi "Stakeout"). Un altro termine usato per definire la sorveglianza fissa è il **punto di osservazione (PO).**

Di solito il punto di osservazione viene scelto in zone panoramiche o di ampia visuale, come le colline, gli edifici, appartamenti o in veicoli parcheggiati nelle aree interessate. La sorveglianza fissa può diventare mobile nel caso gli operatori siano preposizionati e pronti a pedinare il target sorvegliato.

Zone rurali: in una zona rurale, la sorveglianza fissa può consistere in un gruppo di ricognizione armato (polizia o militari) che raggiunge posizioni idonee da cui osservare il target. Per il tipo di sorveglianza richiesta gli operatori spesso fanno uso di strumentazioni specifiche (come può essere l'abbigliamento mimetico), quasi sempre queste operazioni vengono condotte da poliziotti o militari addestrati appositamente. Un altro aspetto importante è il grande arsenale di armi da fuoco in zone rurali (in genere fucili da caccia).

I gruppi di operatori possono scegliere il punto di osservazione su colline o su montagne, usando telecamere o telescopi a lungo raggio, oppure possono piazzarsi all'interno delle foreste adiacenti, in abitazioni abbandonate, campi o cespugli etc. Gli operatori possono indossare abbigliamenti mimetici e costruire postazioni nascoste mimetizzate con l'ambiente (scavando nella terra un solco sufficiente ad inserirsi e coprendo il tutto con la superficie del terreno soprastante).

Sorveglianza mobile

Una volta che il target è stato osservato e si accinge ad andarsene dal punto di osservazione, la sorveglianza diventa mobile. A piedi o su un veicolo il target sorvegliato viene seguito finché non si ferma. Una sorveglianza disposta "a scatola" viene subito installata attorno al target sorvegliato con un operatore incaricato di tenere il contatto visivo diretto sul target (che può essere la persona fisica, il suo veicolo o la sua residenza) avvertendo gli altri operatori sugli spostamenti del target; questa funzione viene definita "**guardia**", (*"trigger" in inglese, NdT*).

Appena il target sorvegliato ricomincia a muoversi, la sorveglianza a scatola diventa mobile per poter seguirlo. In casi di alta priorità la sorveglianza a scatola coprirà tutte le strade principali dentro e fuori la zona interessata e potrà accerchiare completamente il target sorvegliato.

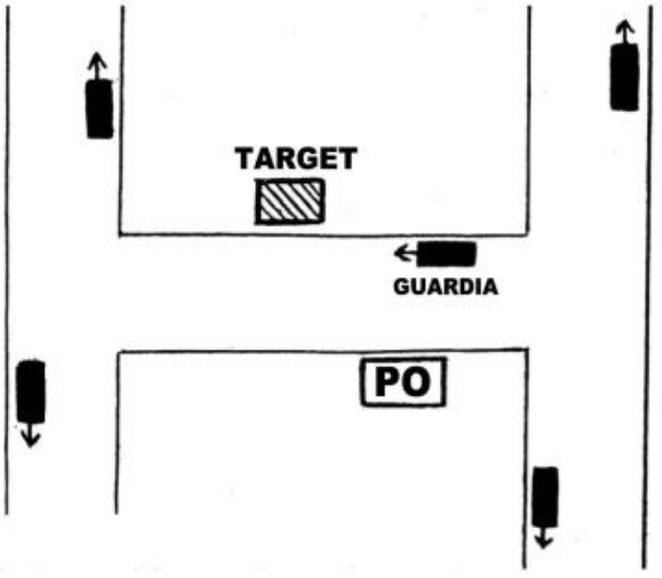
Se il target guida l'automobile, ferma il veicolo e scende a piedi, alcuni operatori scenderanno dai veicoli e seguiranno il target a piedi. Quindi gli operatori si posizioneranno a scatola attorno al veicolo del target oppure seguendo il target con gli operatori a piedi che man mano vengono sostituiti da altri operatori nuovi per non dare nell'occhio.

Per mantenere il loro ruolo, gli operatori possono cambiare abbigliamento al fine di non farsi riconoscere dal target. Se riconosciuti saranno rimossi dall'operazione di sorveglianza e sostituiti con operatori nuovi. Gli operatori possono spostarsi con la bici nel caso il target sorvegliato si sta spostando in bici o a piedi.

Zone rurali: gli operatori che usano i veicoli per la sorveglianza mobile nelle zone rurali sono svantaggiati per la mancanza di coperture sulle strade...

la sorveglianza aerea può compensare questo svantaggio cosi come i congegni GPS per la geo-localizzazione (malgrado senza una sorveglianza diretta queste apparecchiature non garantiscono all'operatore la certezza di chi stia alla guida del veicolo sorvegliato col GPS). In ogni caso anche la sorveglianza mobile in zone rurali rispecchierà queste regole di base, con alcune possibili varianti.

Quattro fasi della sorveglianza mobile (a piedi e/o su veicoli)



Stakeout / Sorveglianza a scatola

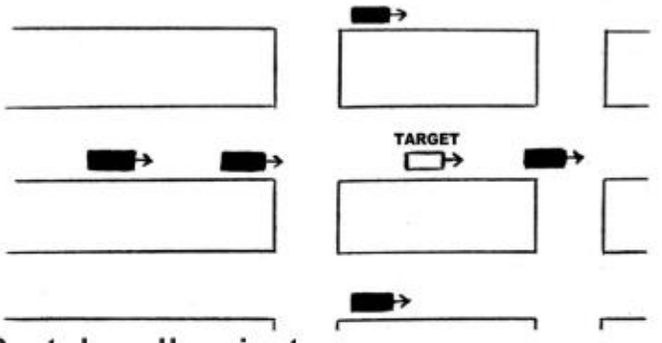
1. Stakeout: i gruppi degli operatori di sorveglianza sono pre-posizionati in un'area specifica, disposti a scatola per coprire tutte le entrate e le uscite della zona sorvegliata. La zona sorvegliata potrebbe essere l'abitazione del target o un luogo in cui si prevede l'arrivo del target.

Uno stakeout può comprendere un punto di osservazione (PO). Nelle aree urbane questo può consistere in appartamenti o abitazioni dalla visuale ampia, veicoli parcheggiati nelle strade etc. Un punto di osservazione valido permette di limitare i rischi di far scoprire al target sorvegliato il gruppo di operatori che lo sta sorvegliando.

2. Pick-up: si dice quando il gruppo di sorveglianza stabilisce il comando del target nel momento in cui questo entra e poi esce dall'area sorvegliata.

3. Inseguimento: comincia immediatamente dopo il pick-up. Questa fase copre tutta l'attività di sorveglianza durante lo spostamento del target da un luogo all'altro.

4. Sorveglianza a scatola: Comincia appena il target si ferma in un'altra locazione. Una tipica sorveglianza a scatola copre tutte le vie d'ingresso e di uscita dalla zona sorvegliata. La principale differenza tra uno stakeout e una sorveglianza a scatola è che per lo stakeout la disposizione degli operatori si compie prima che il target sopraggiunga nell'area sorvegliata; mentre nella sorveglianza a scatola prima si scopre la postazione del target e dopo gli operatori si posizionano secondo la disposizione a scatola.



Scatola galleggiante

Altre forme di sorveglianza fisica

Posta: nonostante oggi la posta cartacea non sia usata quanto le e-mail, la polizia e le agenzie di intelligence hanno una lunga storia di intercettazioni postali, sia di lettere che di pacchi. Gli agenti possono ottenere l'autorizzazione per intercettare la posta, questa viene aperta, viene identificato il contenuto e quindi riconsegnata con un certo ritardo al destinatario. Non è una forma di comunicazione sicura e tanto meno un mezzo sicuro per il trasporto di oggetti.

Spazzatura: frugare tra la spazzatura privata della gente è una pratica molto usata dalla polizia, dall'intelligence e dagli investigatori privati. Tra i reperti pregiati vi sono i vecchi scritti, lettere, pagamenti, fatture, recipienti, flyers, prescrizioni, disegni etc. Tutto ciò che può fornire informazioni personali o sulle attività lavorative. La spazzatura può essere un ricettacolo di reperti e prove di carattere medico-legale (residui, prodotti chimici, fluidi corporei, capelli, etc.)

Vicinato e cittadini sorveglianti: queste persone spesso hanno contatti diretti con la polizia tramite i gruppi di sorveglianza del vicinato o tramite i poliziotti di quartiere. Essi vanno considerati una forma di sorveglianza fisica per il fatto che possono riportare qualsiasi osservazione che si sono fatti su di te, le tue attività, le tue amicizie, etc. Essi possono fornire alla polizia i loro alloggi per facilitare la sorveglianza.

6. Sorveglianza tecnologica

Come notato in precedenza la sorveglianza tecnologica è l'uso di congegni e tecnologie per monitorare e/o registrare le attività del target sorvegliato. Oggi, la sorveglianza tecnologica è assai diffusa nella nostra società per via dello sviluppo crescente delle tecnologie.

Telecomunicazioni

Telefoni, cellulari, internet, fax, e beeper sono particolarmente vulnerabili alla sorveglianza per il fatto che sono controllati dai governi e dalle aziende e sono gestiti attraverso la tecnologia informatica, come tutta la rete di telecomunicazioni. La tecnologia informatica permette l'accesso ad enormi banche dati, al recupero e all'analisi delle comunicazioni senza il bisogno di accedere fisicamente all'abitazione o al luogo di lavoro del target sorvegliato.

Telefoni fissi: i telefoni possono diventare apparecchiature per la ricezione dei suoni anche quando non vengono usati tramite una tecnica conosciuta come "hook switch bypass". Cellulari e telefoni cordless (senza fili) sono i mezzi di comunicazione meno sicuri poiché possono essere facilmente intercettati con apparecchiature accessibili sul mercato.

Cellulari: Poiché i cellulari interagiscono attraverso i satelliti e i ripetitori, possono essere usati per localizzare e tracciare i movimenti di chi ne fa uso. I cellulari possono essere attivati come apparecchiature per la ricezione sonora anche quando sono spenti o inutilizzati. Molti hanno in dotazione telecamere digitali e quindi la possibilità di riprendere video. La proliferazione dei cellulari e delle loro funzioni accessorie ha espanso enormemente il potenziale della sorveglianza, mentre ha ridotto la possibilità di identificare gli operatori che adoperano i congegni per la sorveglianza o per la comunicazione tra gli altri operatori.

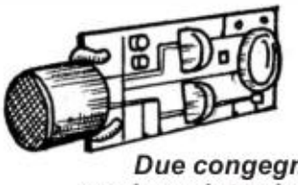
Internet e computer: come i cellulari, internet è un mezzo di comunicazione assai poco sicuro. Le e-mail che spedisci o i siti internet che visiti possono essere intercettati esattamente come una telefonata. Se il tuo computer viene sequestrato o rubato dalla polizia, loro possono avere accesso ad un grosso archivio di informazioni (e-mail, siti web frequentati, documenti, foto, etc.) anche se tu pensi di averle cancellate. In realtà, invece di cancellarle, l'hard disk del tuo computer le rende solamente sovrascrivibili, e quindi facilmente recuperabili. Sul tuo computer possono venir installati software o hardware che registrano tutto ciò che digiti sulla tastiera, permettendo alla sorveglianza di sapere tutto ciò che scrivi. In aggiunta, quando navighi nella rete, particolari software possono venir scaricati e installati di nascosto, questi software permettono ad altri computer di avere accesso al tuo e quindi di attingere informazioni.

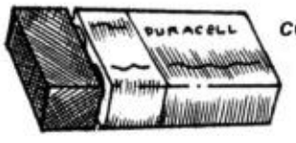
Ogni volta che navighi su internet e apri il tuo account di posta elettronica, puoi venir localizzato e registrato grazie all'indirizzo Internet Protocol (indirizzo IP). L'FBI dispone di speciali software che via mail vengono installati silenziosamente sul tuo computer e che permettono loro di monitorare la tua attività sul web. Questi metodi sono stati utilizzati per arrestare gente che usava internet per diffondere minacce. In alcuni casi la polizia ha prima acquisito l'indirizzo IP del sospetto, e dopo averlo localizzato ha piazzato telecamere vicino alla sua postazione computer per riprenderlo mentre utilizza il web per diffondere altre minacce. La polizia spesso setaccia i profili di Facebook e di altri social network simili per attingere testi, foto e filmati da cui incriminare le persone.

Microfoni

La sorveglianza tramite apparecchiature per la ricezione sonora è uno dei metodi più diffusi per registrare le conversazioni, è diffusa sia per i lavori di intelligence e sia per i comuni arresti. Infatti le investigazioni e i processi multi-milionari quasi sempre si basano esclusivamente su conversazioni registrate (spesso di persone che hanno espresso affermazioni incriminanti in presenza di poliziotti o di informatori infiltrati).

MONETA 20 CENT.





Due congegni wireless per la registrazione sonora disponibili sul mercato; quello in alto può essere collegato ad una batteria al litio o ad un impianto elettrico; quello a sinistra è connesso ad una batteria da 9V.

I congegni per la registrazione vocale, conosciuti anche come cimici, di solito consistono in piccoli microfoni attaccati ad un trasmettitore e ad una fonte di energia elettrica e vengono piazzati nelle abitazioni, nei veicoli, nei luoghi di lavoro, etc. Possono essere piccoli come un bottone (1,5 cm X 1 cm o più ridotti). Le cimici trasmettono ad un

ricevitore, che di solito si trova nei paraggi (molto vicino al punto di osservazione). La vicinanza del ricevitore dipende dal raggio d'azione della cimice. In alcuni casi la polizia ha fatto uso di apparecchiature per ricevere le trasmissioni radio quando non era possibile piazzare un veicolo con un ricevitore nei pressi della cimice (indossata dall'informatore). Gli edifici e il traffico pesante possono disturbare le trasmissioni, dipende dall'apparecchio usato. A volte la polizia si posiziona in edifici abbandonati, sui tetti o in altre zone urbane travestiti da lavoratori per poter ricevere le trasmissioni ad una distanza agevole.

I congegni per la registrazione vocale più diffusi sono wireless (senza fili) e trasmettono ad un ricevitore collocato nei paraggi usando le frequenze radio. Devono essere alimentati da una fonte di energia. Nei congegni più sofisticati sono presenti piccole ma potenti batterie che possono durare per mesi. Nei modelli più economici le batterie per l'alimentazione sono legate assieme al congegno e al microfono e quindi nascoste. Ovviamente più le batterie sono grosse e più sono visibili, e come ogni batteria prima o poi si esauriscono e vanno sostituite con batterie nuove.

Un congegno per la registrazione vocale è il **microfono a filo**, in cui il microfono viene collegato direttamente al ricevitore con un cavo; il ricevitore viene posizionato in una stanza o in un appartamento attiguo. I microfoni a filo non necessitano di una fonte di energia dal momento che la ricevono tramite lo stesso cavo che li collega al ricevitore. Questi microfoni hanno una qualità del suono migliore ma oggi sono poco usati a causa della possibilità elevata che il target sorvegliato li scopra risalendo al cavo.

Di solito i congegni per la registrazione vocale vengono piazzati in luoghi dove si è soliti conversare, come i salotti, le cucine, le camere da letto e i veicoli. Possono venir nascosti nelle cavità dei muri, negli interruttori della luce, nelle lampade, dietro i quadri, sui soffitti, nei ventilatori, etc. Nelle operazioni di alto livello i microfoni sono stati collocati sotto le panchine dei parchi e all'interno dei caffè frequentati dal target sorvegliato.

Nonostante possano essere utilizzati scanner e altre apparecchiature specifiche per scovare questi congegni, non garantiscono che le aree scannerizzate siano sicure. Le nuove tecnologie per la sorveglianza possono aggirare questi apparecchi scanner, e le cimici possono venir temporaneamente spente per annullare qualsiasi frequenza radio. Gli sforzi e i soldi spesi per queste apparecchiature scanner metteranno in allerta il gruppo di operatori della sorveglianza.

Come regola generale, tutti gli spazi chiusi vanno considerati vulnerabili alle apparecchiature della sorveglianza, specialmente quegli spazi frequentati abitualmente dai membri/attivisti del movimento: gli spazi occupati, i circoli, etc.

Un altro tipo di congegno per la ricezione vocale è quello indossato sul corpo dell'informatore o dell'infiltrato. Come altri tipi di congegni questo avrà un piccolo microfono collegato ad una batteria e ad un trasmettitore. Apparecchiature più sofisticate possono essere inserite in diversi oggetti di uso quotidiano (macchine fotografiche, penne, orologi, borse, tazze, etc.). Apparecchiature per la ricezione vocale sono state usate dall'FBI e dall'ATF durante operazioni segrete contro bande di motociclisti, nascoste nei beeper e nelle batterie dei cellulari. Queste apparecchiature hanno interruttori di accensione/spegnimento apposta per poter essere disattivate nel momento in cui venga tentato di scovarle tramite tecnologie scanner.

Un congegno per la ricezione sonora è contenuto in questo orologio

Apparecchiature laser sono usate per raccogliere le vibrazioni dell'aria e convertirle in segnali audio, per poi registrare le conversazioni negli uffici, negli appartamenti, etc.

Microfoni parabolici

Questi potenti microfoni sono designati per origliare le conversazioni a distanze estese. Soprannominati anche "orecchie bioniche" i microfoni parabolici sono apparecchi da impugnare in mano composti da un microfono orizzontale attaccato ad un disco concavo. L'operatore indossa delle cuffie. Alcuni microfoni parabolici hanno un raggio d'azione effettivo di 300 metri. Altre versioni commerciali sono usate per la caccia, ed alcune di queste hanno un binocolo integrato (da cui emerge un piccolo microfono disposto orizzontalmente).

Videocamere

Le telecamere a circuito chiuso (CCTV; Closed-Circuit TeleVision) sono uno degli esempi più famosi della sorveglianza tecnologica nel mondo occidentale. In ogni città ci sono decine di migliaia di telecamere CCTV, nei negozi, nelle banche, nei parchi, negli uffici, nelle scuole, nelle strade e negli incroci.

Mini-telecamera CCTV

Per le operazioni di sorveglianza sono frequenti le telecamere CCTV in miniatura. Queste hanno permesso di filmare persone che vendevano e compravano la droga, armi e bombe, cosi come persone che commettevano azioni incriminanti. Telecamere CCTV in miniatura possono essere piccole fino ad avere un centimetro di diametro (con un piccolo foro su una facciata). Come i congegni per la ricezione sonora, questi possono essere nascosti in qualsiasi oggetto, come un beeper, un peluche, un VCR, un orologio, una radio, un rivelatore del fumo, etc. (queste apparecchiature video si possono comprare liberamente sul mercato). Negli appartamenti o nelle stanze d'albergo, o in qualsiasi struttura adiacente, i gruppi di sorveglianza possono ottenere l'accesso al luogo e fare un foro nei muri o nei soffitti ed inserire la microcamera (come succede durante situazioni sospette in luoghi chiusi).

Le microcamere CCTV devono disporre di una fonte di energia e di un trasmettitore che permetta loro di mandare le immagini riprese al registratore degli operatori di sorveglianza. Come le apparecchiature per la registrazione vocale, l'energia può venire da una batteria come può venir presa dall'impianto elettrico dell'abitazione o del veicolo. Alcune telecamere sofisticate hanno anche la funzione per la visione notturna.

Nei casi in cui la sorveglianza fisica di un sospetto risulta troppo difficile, o in cui le attività illegali da sorvegliare succedono troppo frequentemente, microcamere CCTV vengono nascoste appena fuori l'abitazione del sospetto. Queste sono sensibili ai movimenti e riprendono solo quando nell'area ripresa compare qualcuno. Nel 2007 in Germania questa tecnologia venne usata per sorvegliare le case di alcune persone sospettate di aver commesso attacchi sporadici nell'arco di alcuni mesi (in questo caso una sorveglianza fisica sarebbe stata assai dispendiosa e improduttiva).

Videocamere potenti sono state montate su elicotteri, aeroplani e veicoli aerei senza pilota (UAV, Unmanned Aerial Vehicles). Questi veicoli possono aleggiare o spostarsi su una zona ad altitudini molto alte e risultare virtualmente impercettibili alla vista o all'udito di chi sta sotto, e ciò nonostante possono identificarne il volto.

Molti cellulari e fotocamere dispongono di funzioni video. Tante forze di polizia montano videocamere sulle loro automobili. Nel 2007 la polizia britannica ha adottato una microtelecamera montata sulla visiera del cappello che può essere indossata da agenti in divisa per registrare gli incidenti e i volti dei sospettati. Questa microtelecamera assomiglia ad una piccola lampadina elettrica. Ci sono pure nuove radio da spalla usate da alcune forze di polizia che hanno integrate all'interno piccole fotocamere e videocamere.

Acquisire fotografie

L'uso di videocamere e macchine fotografiche da 35mm resta un'importante attrezzatura per il lavoro di sorveglianza. Particolarmente utili per documentarsi e identificare individui, luoghi, veicoli, etc. Notevoli sono le pellicole a 35mm e le macchine fotografiche digitali che forniscono immagini nitide ed ad alta risoluzione, a differenza delle immagini delle videocamere. Le fotografie devono essere prese da un operatore che abbia la visuale sul target. Con gli zoom ad alta potenza, si possono ottenere anche primi piani fotografando da grandi distanze.

Molti cellulari hanno in dotazione fotocamere digitali installate e possono essere usate per fotografare persone, documenti, targhe, etc.

Apparecchi per il rintracciamento

Di solito vengono attaccati sotto i veicoli nella zona posteriore, questi apparecchi emettono un segnale che può venir captato dal satellite e dalla tecnologia cellulare (i GPS, Global Positioning System). Qualsiasi veicolo equipaggiato con la tecnologia GPS è già nella condizione di poter essere rintracciato (come la rete OnStar). Come già notato in precedenza, anche i telefoni cellulari sono apparecchi per il rintracciamento.

Un tipico apparecchio per il rintracciamento usato dall'FBI si compone di un trasmettitore GPS, un'antenna satellitare, una batteria e una scatola con vari chip elettronici. Tutti questi componenti vengono collegati con un cavo e racchiusi in una scatola di metallo nera fissata sotto i veicoli con dei magneti

Apparecchio per la localizzazione ProScout (formato libro)

estremamente potenti. Il pacchetto con le batterie contiene 4 batterie al litio modello D, un tubo metallico cilindrico lungo 12cm. La scatola coi chip elettronici ha le dimensioni di un libro tascabile. Con questo apparecchio, il rintracciamento del veicolo sorvegliato viene determinato secondo un margine di errore di pochi isolati.

Apparecchi per il rintracciamento disponibili sul mercato come il Quicktrack GPS Tracker, consistono in una scatoletta nera in metallo con potenti magneti. E' grossa circa 4,6 cm X 2,5 cm e la sua batteria ha una durata di 40 ore in modalità rintracciamento, mentre ha una durata di un mese in modalità standby.

Recenti apparecchiature GPS disponibili sul mercato sono piccole quasi come orologi da polso. Avendo tempo a sufficienza si possono installare in ogni parte del veicolo apparecchiature per il rintracciamento particolarmente sofisticate (specie se si lascia il proprio veicolo fermo ed incustodito per lungo tempo).

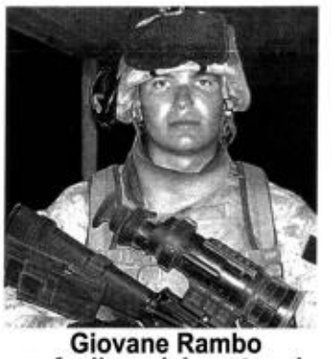
Una variante degli apparecchi per il rintracciamento è il chip RFID (Radio Frequency IDentification), un piccolo congegno (grosso come un chicco di riso) che emette un segnale radio. Viene usato dalle aziende per monitorare la spedizione dei pacchi e per prevenire i furti nei negozi. Chip RFID vengono impiantati chirurgicamente sotto la pelle di persone per ragioni mediche (il chip contiene la loro cartella clinica) o anche per ragioni di sicurezza (potenziali vittime di sequestri di persona). L'FBI ha utilizzato i chip RFID e i congegni GPS per rintracciare i traffici di droga.

OK for medical chip

The U.S. Food and Drug Administration has given approval to Applied Digital Solutions of Delray Beach, Fla., to market the VeriChip, an implantable computer chip about the size of a grain of rice, for medical purposes. The chip could hold a person's entire medical history.

Visione notturna e visione termica

Le apparecchiature per la visione notturna (NVD, Night Vision Device) permettono di amplificare la debole luce naturale della Luna e delle stelle, permettendo all'osservatore di vedere ciò che altrimenti sarebbe nel buio più totale. La visuale degli apparecchi NVD risulta come un immagine sgranata e verde. La visione notturna può essere limitata dall'assenza totale di fonti di luce, dalla nebbia, dalla pioggia pesante, etc. Se le apparecchiature NVD permettono di vedere di notte o in condizioni di luce minima, le apparecchiature per la visione termica individuano le alterazioni della temperatura. Le telecamere a visione termica possono vedere attraverso il fumo e la nebbia e vengono attualmente utilizzate dai pompieri per individuare l'origine delle fiamme in mezzo al fumo degli incendi. Sia i veicoli recentemente usati, sia i corpi umani, sia i terreni scavati di recente possono essere individuati per via del calore presente. Equipaggiamenti speciali per la visione termica possono essere impiegati per monitorare gli spostamenti delle persone all'interno di una struttura. Per queste ragioni sia le tecnologie per la visione notturna sia quelle per la visione termica sono abitualmente utilizzate per le operazioni in elicottero della polizia e dell'esercito. Delle due tecnologie, quelle per la visione notturna è la più diffusa, specialmente tra i militari semplici e i gruppi specializzati della polizia. Sia gli NVD che gli apparecchi a visione termica possono presentarsi sotto forma di occhiali, binocoli o fucili telescopici. Vengono tipicamente usati per la sorveglianza in zone rurali dove manca l'illuminazione artificiale. Sia gli elicotteri che gli aeroplani e gli UAV (veicoli aerei senza pilota) possono essere equipaggiati con le tecnologie a visione notturna o termica.



Giovane Rambo con fucile a visione termica

Tecnologia biometrica

E' lo studio dei tratti fisiologici personali a scopi di sorveglianza, come il riconoscimento facciale, lo scanner dell'iride, il riconoscimento vocale, le impronte digitali, lo studio della postura e della camminata, lo scanner integrale del corpo, etc. Assieme alle tecnologie informatiche del computer, lo studio della biometria si è diffuso a macchia d'olio in questi ultimi decenni.

Apparecchio per la scansione dell'iride

In termini di sorveglianza, le tecnologie biometriche possono essere utilizzate per identificare singole persone mescolate in una folla basandosi sul riconoscimento facciale o sullo scanner corporeo. Le telefonate possono essere analizzate per identificare gli interlocutori. Le impronte digitali possono essere scannerizzate digitalmente con specifici apparecchi al fine di confermare o stabilire istantaneamente le identità. Molte nazioni stanno adottando parametri biometrici per le nuove carte d'identità (anche per patenti e passaporti), incluse la scansione dell'iride e il riconoscimento facciale. Per poter ottenere agevolazioni in varie istituzioni burocratiche, governative ed economiche viene richiesto sempre più spesso di farsi sottoporre allo scanner biometrico.

Veicoli aerei senza pilota (UAV)

Gli UAV sono tipicamente usati dall'esercito per la sorveglianza e la ricognizione. Sebbene ci siano diversi tipi di UAV, tutti servono per la sorveglianza aerea e tutti dispongono di potenti videocamere con funzioni per la visione notturna e la visione termica. Vengono pilotati a distanza da un operatore su terra, il quale osserva la superficie o la zona sorvegliata tramite la videocamera presente sull'UAV. Versioni ridotte degli UAV, come il Raven, lo Skylark o la EagleScan sono aeroplani in miniatura e possono essere lanciati a mano per decollare. Questi hanno un volo di breve durata e servono ai militari che combattono in prima linea per avere una ricognizione della zona adiacente. Versioni più grosse come Henron e Predator hanno le dimensioni di un piccolo aereo e possono rimanere in volo per quasi 24 ore, spostandosi anche per distanze estese. Possono anche rimanere sospesi ad altitudini elevate. Possono essere equipaggiati di missili e sono stati impiegati dall'esercito americano e israeliano per assassinare target specifici.

Skylark UAV usato dall'esercito canadese in Afghanistan

Satelliti

I satelliti vengono usati dall'esercito, dalla intelligence e dalle agenzie commerciali per tutta una serie di obbiettivi, tra cui le foto satellitari, le comunicazioni, la navigazione, etc. Vengono lanciati in orbite specifiche che mantengono in tutto l'arco della loro vita (a volte durano più di 10 anni). Ci sono centinaia di satelliti che orbitano attorno alla Terra.

I Satelliti spia più sviluppati sono quelli lanciati dagli USA, tra cui il gruppo di satelliti chiamati "Key Hole" (KH). I satelliti-spia KH-12 e il KH-13 possono identificare oggetti appoggiati a terra piccoli anche 5 cm (fotografandoli da centinaia di miglia di distanza). Questi fanno uso di radar, laser, infrarossi e sensori elettromagnetici per vedere attraverso la coltre di nubi, la boscaglia e pure attraverso le strutture in cemento, al fine di ottenere immagini e informazioni.

Satelliti specifici per lo scatto di immagini vengono usati principalmente per l'intelligence militare al fine di monitorare i movimenti degli eserciti, le postazioni di armi, basi, porti, navi merci, etc. Raramente vengono utilizzati per sorvegliare singoli individui poiché sono corpi in orbita e non possono rimanere sospesi stabilmente sopra una zona specifica e quindi non possono fornire riprese in diretta di una singola locazione. Inoltre, nelle immagini aeree che forniscono appare solo la parte superiore della testa delle persone, il che non è molto utile per la sorveglianza.

Altri satelliti-spia sono quelli utilizzati per l'azienda SIGINT ("Signals Intelligence") che monitorano il traffico delle onde radio e dei cellulari. Si stima che nello spazio ci siano 100 satelliti americani per la sicurezza nazionale, di cui 6-7 di questi sono lanciati con lo scopo di catturare immagini, e 9-11 sono per la SIGINT. Il Canada e altri stati alleati mettono in condivisione i dati della loro intelligence con il governo americano tramite reti telematiche come la Echelon; tra i dati condivisi vi sono quelli raccolti coi satelliti-spia americani.

7. Scovare la Sorveglianza

A volte scovare la sorveglianza può essere difficile. Di solito si cerca di scovarne la presenza al fine di eluderla. Per questa ragione quando si cercano tracce della sorveglianza non bisogna farlo vistosamente. Se gli operatori ritengono che il target sorvegliato stia praticando forme di contro-sorveglianza, potrebbero intensificare le loro tattiche di sorveglianza ed anche sospettare che il target si dedichi alla contro-sorveglianza perché in procinto di compiere "attività illegali."

Nella maggior parte dei casi, gli operatori addetti alla sorveglianza si tireranno indietro se si accorgono di essere stati scoperti. La sorveglianza stessa potrebbe cessare. In altre situazioni i team di sorveglianza continueranno a mantenere il comando sul target anche se questo è consapevole di essere sorvegliato. Ovviamente la sorveglianza della polizia può essere esercitata al fine di intimidire il target, una pratica del genere rientra in una guerra psicologica più ampia il cui fine è neutralizzare il target con paure e paranoie indotte.

Scovare la sorveglianza fisica

La chiave per scovare la sorveglianza è la **consapevolezza** e l'**osservazione** di ciò che ti circonda, incluse le persone e i veicoli. Nell'identificare possibili operatori, comincia con l'osservare il loro abbigliamento, la statura, gli atteggiamenti e i tratti facciali (inclusi il taglio e il colore dei capelli, la forma della testa e del volto, baffi, segni particolari, etc.) In particolare, qualsiasi tratto o lineamento distintivo può aiutarti molto a ricordare e riconoscere in un secondo momento gli stessi individui e veicoli.

La maggior parte degli operatori tenteranno di integrarsi nell'ambiente e di minimizzare qualsiasi fattore che possa attirare l'attenzione su di loro. Vestiti, capigliature o altri connotati strani o particolarmente colorati verranno evitati per via dell'attenzione che attirano su di sé. Perciò la maggior parte degli operatori si distinguerà per il suo aspetto semplice e normale.

Nell'identificare possibili operatori, parti dal presupposto che tutti sono potenzialmente degli operatori. Comincia eliminando quelli che non ti sembrano arruolabili nella sorveglianza, al fine di focalizzarti su quelli che invece lo sembrano. Tieni in mente che alcuni team di sorveglianza sono composti da persone che risulterebbero incapaci di superare semplici test di ginnastica di base e che possono comprendere vecchie signore, uomini bassi e di grossa corporatura, etc. Poliziotti infiltrati si sono introdotti nelle bande di motociclisti grazie al fatto di essere appassionati di tatuaggi, di portare i capelli lunghi e la barba. E' molto importante valutare le persone in base al loro comportamento e in base a ciò che fanno, e non in base al loro aspetto o al loro modo di apparire.

I veicoli possono essere osservati in base al loro colore, forma, modello, graffi/ammaccature particolari e ovviamente alle targhe. Di notte puoi identificare i veicoli di possibili operatori dalla silhouette del veicolo e dalla posizione dei fari.

Un traguardo notevole nello scovare la sorveglianza è osservare un particolare individuo e/o un particolare veicolo in una zona specifica e successivamente rivedere gli stessi in altre zone diverse.

Caratteristiche generali degli operatori di sicurezza (a piedi o su veicoli):

- Possono appartenere a qualsiasi etnia, sesso, corporatura, età, etc.
- Di solito evitano lo sguardo diretto e quando tentano di farlo possono addirittura apparire goffi o imbarazzati.
- Possono apparire fuori luogo, nervosi o in tensione (perché lo sono).
- Possono venir visti o ascoltati nell'atto di parlare in microfoni posizionati sul collo, aggiustarsi gli auricolari o impugnare apparecchi per poter aggiustare il volume o mandare segnali al team di sorveglianza, nascondendoli a volte nella tasca.
- Possono venir osservati mentre mandano segnali (con le mani, muovendo il capo, etc.) o parlando direttamente ad altri membri del team di sorveglianza.

Tecniche di riconoscimento della sorveglianza

Uno dei momenti migliori per scovare la sorveglianza è quando la sorveglianza a scatola si è posizionata attorno ad una zona. I team di sorveglianza sono più vulnerabili a farsi scoprire durante questa fase dell'operazione. In alcuni casi potrebbero starsene seduti per ore ad aspettare che il target compaia o si muova.

I **punti di osservazione** nei piani alti degli appartamenti o degli edifici a volte si possono identificare dalla loro apparente assenza di attività, tendine calate, tapparelle abbassate o altri modi per oscurare le finestre. Sebbene loro vogliano vedere fuori, non vogliono che tu li veda dentro. Tutto ciò che occorre loro al fine di osservare l'esterno, è una piccola apertura per le lenti della telecamera o del telescopio.

Possibili punti di osservazione possono essere rilevati nelle primissime vicinanze dell'abitazione del target (usando il criterio descritto qui sopra) cosi come entrando o uscendo dalla zona che si suppone sotto sorveglianza. Per il team di sorveglianza, il punto di osservazione ideale deve permettere un'ampia visuale sul veicolo del target o sull'ingresso della sua abitazione.

Più si è familiari al vicinato, e più è facile identificare nuovi veicoli e nuovi vicini, entrambi i quali

potrebbero essere dei potenziali operatori di sorveglianza. A volte alla polizia risulta irrealistico sfrattare i vicini o posizionarsi nelle loro case per la sorveglianza. Quindi viene usato un veicolo come punto di osservazione.

Nel caso di un **veicolo come punto di osservazione**, viene scelto un furgone, un minifurgone, un camper, un camion da trasporti; dei veicoli larghi abbastanza da contenere gli operatori e l'equipaggiamento per la sorveglianza. Come nel caso degli edifici adibiti a punti di sorveglianza, anche i veicoli utilizzati a tale scopo si distingueranno dall'assenza di attività e dall'impossibilità di osservarne l'interno. Tende o altre coperture possono venire applicate alle finestre. Un possibile indicatore della sorveglianza è la presenza di altri veicoli con scompartimento posteriore nelle primissime vicinanze.

Se un veicolo parcheggiato rispecchia queste caratteristiche e l'autista se ne esce e successivamente entra in un veicolo diverso, il primo veicolo parcheggiato potrebbe essere un potenziale punto di osservazione. In alcuni episodi la polizia ha parcheggiato una normale automobile con un operatore nascosto nel baule. L'operatore può monitorare e trasmettere e/o registrare le attività esterne osservando da uno spioncino.

Una variante del veicolo adibito a punto di osservazione è il parcheggio di un veicolo contenente un apparecchio ricevitore per captare i segnali di un trasmettitore piazzato nelle vicinanze (in un edificio o addosso ad una persona) o contenente una mini-telecamera CCTV installata. In questo caso l'operatore lascia la macchina per la durata dell'operazione di sorveglianza, per poi riprendersela successivamente.

****

Quando si abbandona un luogo, sia a piedi o con un veicolo, il target sorvegliato dovrebbe guardarsi attorno discretamente ed osservare per trovare tracce di una guardia (*"a trigger" in inglese, ossia l'operatore che deve mantenere il contatto visivo sul target, NdT*) cosi come il pedinatore (*"the follow" in inglese, NdT*), la persona o il veicolo che deve abbandonare il luogo assieme al target per seguirlo.

Si può anche camminare attorno al vicinato e scrutare per scovare possibile sorveglianza. Andarsene e ritornare sul posto (Double-back) come se si avesse dimenticato qualcosa, può costringere gli operatori a ristabilire una scatola di sorveglianza, correndo il rischio di esporsi agli occhi del target.

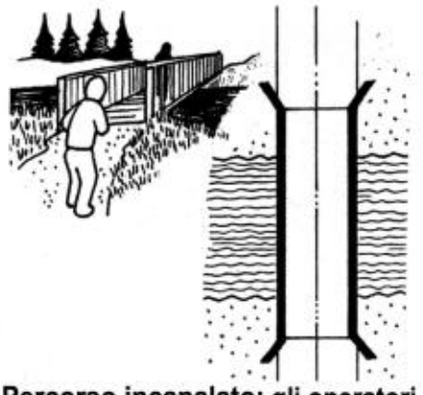
Un altro momento in cui gli operatori di sorveglianza sono identificabili è durante il cambio del mezzo di trasporto, dal veicolo a piedi o viceversa. Tieni d'occhio le persone che piombano inaspettatamente in un veicolo, o che ne escono allo stesso modo, etc.

Durante la sorveglianza mobile, sono le reazioni degli operatori che rivelano la loro attività. Alcune di queste reazioni sono automatiche poiché sono parte della routine delle operazioni di sorveglianza.

Per esempio, si dice **rispecchiamento** (*"mirroring" in inglese, NdT*) quando un operatore di sorveglianza duplica le tue azioni come se seguisse i tuoi passi, specialmente nella sorveglianza mobile su veicoli. Si dice tenere il passo (*"pacing" in inglese, NdT*) quando loro mantengono la stessa distanza tra loro e il target, rallentando e accellerando per mantenere la stessa distanza.

Ricalcando certi comportamenti prestabiliti, gli operatori possono venir colti di sorpresa.

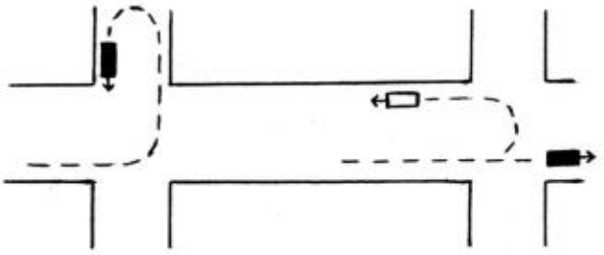
Muovendosi lungo un **percorso incanalato** (*"channelized terrain" in inglese, NdT*) si può costringere gli operatori ad esporsi all'osservazione del target. I percorsi incanalati sono quei luoghi dove tutto il traffico (a piedi o su veicoli) deve passare attraverso un passaggio o un'apertura ristretta. Un ponte o un tunnel sono un esempio di questi passaggi. Al fine di tenere il comando, il team di sorveglianza deve necessariamente entrare ed attraversare il percorso incanalato. Il target sorvegliato può attraversare a piedi fino alla metà del ponte, quindi fermarsi fingendo di ammirare la vista per poi girarsi e tornare indietro (inversione ad U) per osservare come reagisce il flusso di persone e di veicoli.



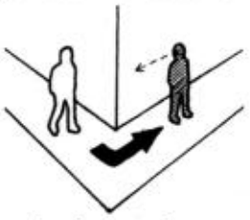
Percorso incanalato: gli operatori sono costretti ad attraversarlo per tenere il comando del target

Quando si guida o si cammina, fare bruscamente una **inversione ad U** può costringere gli operatori di sorveglianza a reagire di modo da far rilevare la loro attività. Gli operatori poco addestrati e gli operatori scoperti eseguiranno a loro volta l'inversione ad U e continueranno a seguire il target. Un operatore ben addestrato invece continuerà la rotta uscendo di scena, lasciando il suo incarico ad un altro operatore.

Reazione standard ad una inversione ad U:
il veicolo dell'operatore al comando continuerà dritto, i veicoli degli operatori che stavano dietro cambieranno postazione e direzione al fine di seguire il target sulla sua nuova traiettoria.



Quando si cammina o si guida, si può mettere in pratica una deviazione cieca (*"blind turn" in inglese, NdT*) per costringere gli operatori di sorveglianza a reagire inaspettatamente. La deviazione cieca è una strategia in cui il target risvolta dietro un angolo e qui si ferma, aspettando e osservando le reazioni dei potenziali operatori di sorveglianza. Una reazione standard di un operatore sarà di continuare a camminare lungo l'angolo gettando uno sguardo per individuare la posizione del target. Quindi comunicherà la posizione del target ad altri operatori e lascerà il comando ad altri membri del team di sorveglianza. Operatori meno addestrati potrebbero semplicemente girare l'angolo e trovarsi faccia a faccia col target, probabilmente reagendo in maniera inaspettata o scomposta.



Deviazione cieca

A piedi, l'unica opportunità per osservare discretamente chi ti sta dietro è il momento in cui attraversi un'intersezione. Attraversare velocemente una strada (**jaywalk** *in inglese, NdT*) ti dà il pretesto di guardarti attorno per poter individuare potenziali operatori. Entrare in **locali pubblici**, come i centri commerciali, uffici, etc. può costringere gli operatori ad entrare assieme a te e ad esporsi alla tua osservazione. Prendere gli ascensori ti concede di girarti di 180° per osservare chi hai alle spalle. Prendere gli ascensori può costringere gli operatori ad un'esposizione ancora più ravvicinata. Inoltre farti più piani sugli ascensori a vetro ti permette di osservare larghe zone da una posizione altolocata.

Il **trasporto pubblico** può servire ad individuare potenziali operatori. Salire sui bus o sul metrò può costringere gli operatori ad esporsi maggiormente alla tua osservazione o a rischiare di perdere il controllo su di te. Se gli operatori sono costretti a salire su un veicolo pubblico assieme a te, hai la possibilità di osservare i tratti facciali particolari e di incrociare gli sguardi dei potenziali operatori spingendoli a reagire in maniera scomposta. Osserva quelli che salgono alla fermata dopo quella su cui tu sei salito cosi come quelli già presenti ed esposti alla tua visuale e allo stesso modo quelli che salgono alle fermate successive. Una volta che il target scende alla fermata, nuovi operatori a piedi potrebbero fare la loro comparsa, perciò se lo stesso veicolo appare in prossimità di più fermate del bus o della metro, costituisce un possibile indicatore della presenza di sorveglianza.

Sulle **strade**, fermarsi in un'area di sosta potrebbe costringere i veicoli della sorveglianza a parcheggiare ed aspettare. Guidare attraverso le aree di sosta in cui ci si è fermati permette di osservare quali veicoli si sono fermati per poterli identificare qualora si ripresentassero alle fermate successive. Come le metropolitane, le autostrade si caratterizzano per l'alta velocità che può rendere gli operatori impreparati alle circostanze. Rampe d'uscita, sbocchi stradali, aree di sosta, inversioni ad U, inversioni cieche, etc. possono essere tutte sfruttate sulle strade. Le strade inoltre offrono ampie zone di osservazione per lunghi tempi.

Sia che si tratti di sorveglianza a piedi o sui veicoli, gli operatori addetti al comando possono essere cambiati frequentemente per minimizzare il rischio di esporsi agli occhi del target. Spesso, gesti imprevisti o improvvisi possono costringere i team di sorveglianza a reagire. In ogni caso, se il tuo comportamento si è dimostrato ciclico e prevedibile, un cambiamento brusco potrebbe rendere gli operatori sospetti. Per scovare la sorveglianza al meglio bisogna agire il più segretamente e discretamente possibile. Se sei in un veicolo usa gli specchietti retrovisori. Occhiali da sole con le lenti a tutto tondo possono tornare utili coprendo gli occhi quando bisogna guardarsi attorno senza farsi notare.

Zone rurali: potenziali Punti di Osservazione (PO) possono essere rilevati dall'abitazione del target. Questi PO devono necessariamente avere la visuale sull'abitazione del target. L'unico modo per scovare possibili PO è attraversare fisicamente la zona adiacente l'abitazione del target. Zone adibite a PO possono essere identificate dalla presenza di terreni alterati, appiattiti per permettere agli operatori di potersi sedere o di dormire, dalle tracce varie lasciate dalle attrezzature degli operatori, dai loro rifiuti, etc. Riconoscere le tracce sul terreno può aiutare enormemente nell'identificare potenziali zone addette a PO. Punti di Osservazione a lungo termine possono consistere in un nascondiglio abbandonato. Per scovare la sorveglianza nelle zone

rurali si può fare ricorso ai cani, cosi come si possono osservare le reazioni degli animali e in particolare degli uccelli (in molte retate della polizia, i cani sono stati i primi ad accorgersi delle anomalie circostanti).

Scovare la sorveglianza tecnologica

La sorveglianza tecnologica è difficile da scovare, specialmente quella che coinvolge le telecomunicazioni. Una regola generale da tenere per fronteggiare la sorveglianza tecnologica è che qualsiasi informazione deve essere protetta in quanto potenzialmente intercettabile dalla sorveglianza tecnologica. Utilizzare tecnologie di contro-sorveglianza per scovare le tecnologie della sorveglianza non garantisce alcuna sicurezza assoluta. Il nostro nemico dispone di un arsenale tecnologico molto più esteso, incluso l'accesso alle attrezzature delle telecomunicazioni, delle aziende, etc. Tutto ciò ovviamente determina le nostre misure di sicurezza contro la sorveglianza tecnologica.

Uno degli obbiettivi della sorveglianza fisica è permettere agli agenti della intelligence o della polizia di intrufolarsi al fine di piazzare nell'abitazione le apparecchiature per la sorveglianza tecnologica. Speciali team addetti all'intrusione potrebbero come prima cosa introdursi nella residenza, o nella zona lavoro, o nel veicolo, e quindi fotografare i muri interni, i lampadari, le cartine, oggetti, etc. A questo punto stabiliscono quali siano i migliori apparecchi e i migliori punti in cui installarli. Quindi se ne vanno, preparano gli apparecchi e ritornano.

In molti casi, non c'è alcun segno evidente di intrusioni e nulla viene prelevato. Se i cani sono dentro la casa, possono manifestare comportamenti strani a causa di apparecchiature ad ultra-suoni usate per tenerli sotto controllo durante le intrusioni della polizia. In altri casi, si può ricorrere ai comuni allarmi. Per infiltrarsi nell'abitazione possono venir utilizzati agenti camuffati da tecnici addetti alla riparazione delle linee telefoniche, della TV o della linea elettrica. Il proprietario dello stabile, se disponibile, può fornire le chiavi. I raid e le perquisizioni della polizia sono ottimi momenti per installare congegni per la sorveglianza.

Gli oggetti sequestrati dalla polizia durante i raid, come i computer, i videoregistatori, etc. successivamente restituiti, possono contenere congegni impiantati all'interno. Ciò vale anche per i veicoli sequestrati o lasciati in custodia per giorni interi o per certi regali inaspettati come stereo o TV (i cosiddetti "cavalli di troia").

Un possibile indicatore della presenza di sorveglianza elettronica (cimici o microtelecamere) sono le interferenze nelle apparecchiature radio, nella TV o nelle connessioni dei cellulari.

Prima della tecnologia digitale, intercettare i telefoni era un operazione grezza e spesso si riconosceva per via di rumori di sottofondo anomali, come tasti premuti, volumi bassi, etc. Oggi intercettare i telefoni può essere fatto molto più efficientemente senza rumori di sottofondo.

Ricercare i congegni tecnologici dovrebbe essere un'attività da svolgere il più discretamente possibile, mentre si finge di pulire la casa, etc. In alcuni casi i raid della polizia sono stati fatti appena dopo che i sospetti trovarono congegni per la ricezione all'interno della propria abitazione o del proprio veicolo. La ricerca di questi congegni dovrebbe essere sistematica e pianificata per ogni stanza, dal soffitto fino al pavimento, includendo tutti gli oggetti, apparecchi elettronici, interruttori della luce, prese della corrente, lampadari, condotti di areazione, rilevatori del fumo, etc. Sulle superfici dei muri le piccole zone dove il colore è sbiadito, dove la texture subisce delle variazioni anomale, dove sono presenti piccoli fori, andrebbero ispezionate. Per migliorare l'ispezione delle zone ridotte si possono utilizzare piccole torce. Tutti i congegni elettrici dovrebbero essere aperti e ispezionati, tutti i quadri e gli specchi rimossi. Drappi e tende ispezionati, cosi come i vasi delle piante, mobilio, banchi, etc.

Congegni per la ricezione o microcamere possono finire all'interno di un'abitazione come "cavalli di troia", camuffati all'interno di regali come nuovi orologi, radio, lettori CD, piccole TV, etc.

La **ricerca nei veicoli** dovrebbe venir svolta dopo il lavaggio dell'auto. Parcheggia il veicolo in un luogo riservato (come un garage) e ispeziona il telaio per possibili apparecchi per il rintracciamento attaccati coi magneti. Ispeziona l'interno del bagagliaio e il foro di ventilazione del motore. Ispeziona l'interno del tetto e delle portiere, i cruscotti, gli specchi e i sedili.

Congegni per la ricezione che funzionano tramite le frequenze radio possono essere scovati con apparecchi scanner. Se la radio, la TV o il telefono cominciano a ricevere frequenze diverse, se presentano disturbi o manifestano anomalie, ciò è un possibile indicatore della presenza di tecnologie per la sorveglianza.

Se dei congegni tecnologici vengono scovati, evidentemente dimostrano che la sorveglianza è

in vigore. In questi casi si può reagire in modi diversi a seconda della situazione. I congegni si possono anche lasciare intoccati, nel caso la loro rimozione potrebbe indurre la polizia ad infiltrarsi nel veicolo ulteriormente per riprenderseli e/o sostituirli con congegni più sofisticati. Una volta scovati i congegni per la sorveglianza, ci si può sbizzarrire creando disinformazione. Gli apparecchi per il rintracciamento scovati nel proprio veicolo si possono riattaccare all'ultimo momento sotto altri veicoli, etc.

sicurezza contro la sorveglianza tecnologica

E' quasi impossibile garantire l'immunità dalla sorveglianza tecnologica; sia che si tratti degli ambienti chiusi, come le stanze o i veicoli ben conosciuti dagli agenti di polizia, o che si tratti di qualsiasi forma di telecomunicazione. Quando bisogna discutere di informazioni o di attività sensibili **evita qualsiasi ambiente chiuso,** specialmente quelli legati alla propria persona o ad altri membri del movimento, inoltre ricordati di **evitare l'uso delle telecomunicazioni**. La migliore forma di comunicazione è quella faccia-a-faccia.

La regola generale è: **contro un nemico che dispone di un apparato tecnologico esteso, riduci la tecnologia (o escludila del tutto).** Non cercare di sopraffare la sorveglianza tecnologica con mezzi tecnologici.

Telecomunicazioni

Prendi consapevolezza che tutte le telecomunicazioni sono vulnerabili alla sorveglianza ed evita di discutere di informazioni o attività sensibili al telefono, su internet, etc. incluse le dicerie, i gossip e i dettagli della vita privata dei singoli individui. Se proprio necessario comunicare informazioni sensibili attraverso i mezzi di telecomunicazione, ricorri ad un codice prestabilito di parole e nomi.

Telefoni cellulari

I cellulari possono essere utilizzati sia come apparecchi per la ricezione sonora che per il rintracciamento, non dovrebbero venir portati con sé durante qualsiasi attività segreta o quando si discute di informazioni sensibili. Come minimo si dovrebbe rimuovere la batteria.

Computer ed internet

I consigli di base presentati di seguito sono tratti da *"A Pratical Security Handbook for Activists & Campaign,"* un testo pubblicato dai movimenti di resistenza del Regno Unito (reperibile sul sito www.activistsecurity.org). A prescindere da ciò, tutte le telecomunicazioni vanno sempre e comunque considerate mezzi di comunicazione insicuri e potenzialmente intercettabili.

Sicurezza del computer

1. Installa ed aggiorna regolarmente i firewall e gli anti-virus. Esistono programmi gratuiti come AVG (www.grisoft.com) ed anche Zone Alarm (www.zonealarm.com) che sono compatibili per i sistemi operativi Windows. Molto importante è attivare l'aggiornamento automatico di modo da tenere i programmi sempre aggiornati.

2. Installa un programma per rilevare gli spyware, come Ad-Aware, programma scaricabile liberamente da www.lavasoft.de.

3. Cancellare i file non li rimuove realmente dal tuo hard disk, li rende soltanto sovrascrivibili. Per renderli davvero irreperibili occorre sovrascriverli adeguatamente con programmi specifici per questa funzione *(la cancellazione definitiva ed irreversibile di un file si dice "Wipe" in inglese, NdT)*. Alcuni programmi raccomandati sono Clean Disk Security ed anche PGP *(o anche File Shredder, NdT)*.

4. Tutti i file sensibili presenti sul tuo computer, sui tuoi CD o sui tuoi floppy andrebbero criptati usando un programma come PGP *(o Truecrypt, NdT)*. Puoi raggruppare tutti i singoli file sensibili in un unico grande archivio (usando programmi come Winzip o anche Stuffit) e quindi decriptare quest'ultimo. In questo modo anche i nomi dei file sensibili sono nascosti. Dopo aver fatto il copia-incolla dei file sensibili, cancella i file originali con la funzione "Wipe"; questa operazione dovresti svolgerla ogni sera dopo aver utilizzato il tuo computer. In alternativa puoi criptare l'intero hard disk.

5. Scegli password che siano efficienti, lunghe almeno 16 caratteri e che includano se possibile, caratteri con maiuscole e minuscole, numeri e simboli. Password deboli sono facili da infrangere. Per gli infiltrati esperti non è impossibile violare un computer protetto da password, perciò è necessario criptare tutto ciò che c'é di sensibile sul tuo computer.

- E' buona cosa cambiare le password ad intervalli regolari.
- Non lasciare bigliettini con le password incollati sotto il tuo tavolo o sotto la tua sedia; sono i primi posti in cui si andrà a cercare.
- Non inventare le password basandoti sui nomi di familiari, di amici, di animali e nemmeno sulle date di nascita.
- Nell'inventare le password, non limitarti ad utilizzare parole esistenti sul dizionario.

6. Nel caso il tuo computer possa venir rubato, fai un back-up dei dati e tienilo nascosto da qualche altra parte in un luogo segreto e sicuro *("fare il back-up" significa copiare i dati presenti sul proprio computer su un supporto di memoria esterno, come una chiavetta USB, un hard disk esterno, un CD o un DVD, etc. NdT).*
7. Considera i vantaggi nel passare ad altri sistemi operativi più sicuri di Windows, come i sistemi operativi Mac o ancora meglio i sistemi operativi Linux.
8. Evita l'utilizzo di tastiere wireless *(senza fili, NdT)* perché l'informazione che viaggia dalla tastiera wireless al tuo computer può essere facilmente intercettata.
9. Tieni i file importanti e/o sensibili cosi come le chiavi di crittografia di PGP su dispositivi di memoria esterna, come le chiavette USB, gli hard disk esterni, i CD o i DVD, etc.

Privacy su Internet

1. Le e-mail non sono sicure e sono facilmente intercettabili. Per incrementare la privacy, usa i sistemi di criptazione PGP *(tra le varie versioni di PGP la meno rischiosa è la versione open source, ossia il software GnuPG; scaricabile dal sito web:* www.gnupg.com *oppure il client di posta Thunderbird con il plug-in Enigmail, NdT)*. Quando componi le tue e-mail non scrivere niente di cui tu non sia in grado di giustificare davanti ad un tribunale.

Se vuoi lasciare dei messaggi ad un'altra persona senza che i tuoi sorveglianti sappiano chi è il destinatario di questi messaggi, crea dei falsi account... e utilizzali lo stesso. Considera la possibilità di utilizzare questi account come cassette-deposito per i messaggi (non li salvi come e-mail da spedire, ma ti limiti a salvarli nelle "bozze" senza indicare il destinatario; in questo modo la persona a cui lasci il messaggio può leggerlo entrando nel tuo falso account da un altro computer anonimo).
2. Proteggiti dallo spam, specialmente dalle e-mail non richieste, anche se possono sembrare genuine, come quelle inviate da una banca. Non comprare mai nulla e non cliccare sui link di siti web presenti su queste e-mail...
3. Ogni volta che accedi ad internet lasci tracce della tua navigazione che permettono di risalire a te. Se vuoi visitare un sito web senza farlo sapere ad altri, ricorri ad un sito web anonymizer *(o ad un software anonymizer come Tor, NdT)* o ad un internet café. Se sospetti di essere sorvegliato, non fare nulla di sensibile col tuo computer di casa. Quando entri in un Internet café, guardati intorno per scovare possibili telecamere CCTV, quindi disattiva quelle piccole od oscurale (altrimenti ricorri ad un camuffamento).

***NdT I°**: alcuni file digitali, come le immagini JPEG, i pdf, i file di testo, i video, etc. hanno in allegato dei dati nascosti (i "**metadata**") che registrano informazioni aggiuntive che possono far risalire all'autore di quel file. Per esempio, ogni fotografia digitale scattata contiene un metadata chiamato "**Exif**" che tiene registrato il modello e il numero di serie della fotocamera digitale utilizzata, il software utilizzato, l'orario in cui è stata scattata e (per le fotocamere dotate di GPS) le coordinate geografiche in cui è stata scattata, etc... Per diffondere file digitali tutelando la propria privacy e il proprio anonimato conviene rimuovere i metadata dai file con i software specifici per questa funzione. Per i sistemi operativi Linux c'é la funzione ExifTool.*

***NdT II°**: quando si naviga sul web, oltre all'indirizzo IP esiste un altro codice digitale che può far risalire all'identità del navigatore: si tratta dell'**indirizzo MAC**; una sorta di "targa digitale" che identifica le schede di rete ethernet del PC. Anche l'indirizzo MAC si può modificare con i software specifici.*

***NdT III°:** per cancellare completamente ed irreversibilmente tutta la memoria del proprio hard disk (o del proprio supporto di memoria esterno) si può usare il software **DBAN (Darik's Boot and Nuke)**; è un software open source designato per sovrascrivere un certo numero di volte un intero supporto di memoria (a seconda del metodo usato si avrà un livello maggiore o minore di efficacia). DBAN si installa su un supporto di memoria esterno (un CD, una chiavetta USB, etc.) e si attiva in fase di boot dal PC su cui vanno cancellati i dati. DBAN è liberamente accessibile dal sito: https://*www.dban.org

***NdT IV°:** i **keylogger** sono dei software/hardware che vengono installati sui PC per intercettare tutto ciò che viene digitato sulla tastiera. Per ridurre i rischi di intercettazioni dei dati digitati si possono usare **tastiere virtuali** come il software **Onboard** (per Linux) in alternativa alla tastiera fisica.*

***NdT V°:** una risorsa informatica interessante è il sistema operativo **Linux Tails**: è un sistema operativo "Live" (che si attiva dal PC senza dover essere installato sull'hard disk) ed open source che contiene molti software specifici per la sicurezza. Si installa su un supporto di memoria esterno e si attiva in fase di boot da un qualsiasi PC. I dati elaborati vengono salvati sulla memoria RAM del PC; prima dello spegnimento questa viene sovrascritta cancellando dal PC le traccie delle attività svolte con Tails. Tails è liberamente accessibile dal sito web del progetto Tor: https://*www.torproject.org*

Congegni per la ricezione sonora e mini-telecamere

Per proteggersi contro le intrusioni segrete della polizia nelle abitazioni o nei veicoli fatte per piazzare congegni per la sorveglianza, si può fare ricorso alle più comuni apparecchiature antifurto. Queste includono i classici lucchetti robusti alle porte e finestre, allarmi, telecamere di sorveglianza e cani da guardia. I veicoli possono venir parcheggiati in garage e resi più sicuri con sistemi ad allarme. In ogni caso, nessuna di queste misure garantisce la sicurezza assoluta contro le intrusioni segrete.

Alcune gang di motociclisti hanno cominciato da poco ad utilizzare apparecchi scanner nelle loro residenze e nei loro club per scovare trasmettitori nascosti sui corpi degli informatori o degli infiltrati. Come reazione la polizia ha inserito nei congegni per la ricezione un interruttore on/off per poterli spegnere.

In certi casi le bande di motociclisti hanno installato telecamere CCTV attorno alle loro residenze, fuori dai laboratori per la droga o all'interno dei loro club, il tutto per monitorare i loro spazi dalle intrusioni segrete della polizia. Inoltre hanno nascosto apparecchi per la registrazione vocale che si attivano in presenza di suono al fine di identificare meglio gli intrusi.

Per ostacolare la sorveglianza della polizia, le bande di motociclisti hanno piazzato sentinelle ed hanno organizzato pattuglie disposte sui quattro angoli dell'edificio che ospitava i loro raduni. Questa situazione costringe gli operatori infiltrati ad indietreggiare per trovare aree sicure da cui ricevere tranquillamente le trasmissioni. Un'altra pratica è incontrarsi in un primo luogo d'appuntamento per poi spostarsi successivamente in un altro luogo conosciuto solo da pochi che offra buone condizioni per la contro-sorveglianza. In certi casi, le bande di motociclisti si radunano in una zona rurale in prossimità di un aeroporto, al fine di scoraggiare l'uso di apparecchi aerei telecomandati, utilizzati dalla repressione per ricevere le frequenze radio delle cimici.

Per fronteggiare le apparecchiature per la registrazione vocale, le bande di motociclisti cominciano ad usare lavagnette per scriverci sopra le informazioni segrete e poi cancellarle. Un'altra variante di questo metodo consiste nello scrivere le informazioni su un singolo foglietto di carta appoggiato ad una superficie solida (per non lasciare alcuna impressione) e quindi distruggerlo subito dopo. Per ostacolare le apparecchiature per la ricezione sonora (inclusi i microfoni parabolici) si possono condurre le discussioni segrete in aree isolate o in luoghi improvvisati.

Si possono usare nomi e parole in codici prestabiliti per evitare di riferirsi direttamente alle informazioni sensibili.

Codice: chiave di lettere/numeri. Scegli una parola di dieci lettere in cui nessuna si ripeta, ed assegna un numero ad ogni lettera:

J A M E S B R O W N
1 2 3 4 5 6 7 8 9 0
Esempio: WRE-WBNA = 974-9602
Codice al telefono: il cantante di colore

Curiosità itagliane (NdT):
La repressione made in italy è affetta da spiccate paranoie complottiste ed ha l'abitudine di "scovare" nei discorsi intercettati degli attivisti mefistofeliche "parole in codice" anche quando queste di fatto non ci sono; queste fantomatiche "parole in codice" vengono poi interpretate arbitrariamente dal P.M. al fine di attribuire agli attivisti incriminati attività o propositi criminosi che porterebbero ad arresti o ad incrementi delle pene...

Apparecchi per la localizzazione

Per contrastare l'uso degli apparecchi per la localizzazione, non si devono utilizzare veicoli personali per attività segrete. Gli ultimi modelli di automobili molto spesso hanno pre-installati dispositivi GPS, come quelli della rete On-Star. Molte compagnie per il noleggio di automobili installano dispositivi GPS per monitorare i loro veicoli. E' possibile che la polizia piazzi un dispositivo GPS su una bicicletta. Qualsiasi veicolo usato come contro-sorveglianza deve essere "immacolato"; non deve fornire dati o caratteristiche che facciano risalire a te o ad alcun attivista.

WorldTracker GPS tracker, disponibile sul mercato

Sorveglianza aerea e visione notturna

Per aggirare la sorveglianza notturna vai in mezzo ai centri commerciali, negli appartamenti, nelle stazioni dei pullman o in qualsiasi edificio che abbia più uscite e piazze spaziose. Se possibile cambia giacca e cappello.

Per aggirare la sorveglianza aerea notturna (cosi come la visione termica e/o notturna) in un'area urbana o suburbana, piazzati dentro edifici grossi, sotto i ponti di cemento, sotto i veicoli, nei tunnel o nei sistemi fognari, etc.

Per aggirare la sorveglianza aerea nelle zone rurali, piazzati sotto i ponti, sotto i tubi di drenaggio,

sott'acqua, dentro boscaglie, dentro i tunnel, ect.

Cercare di nasconderti in una certa zona mentre sei già stato rintracciato dalla sorveglianza aerea può spingere la repressione a mandare delle pattuglie nella zona dove ti sei nascosto. Nel caso la sorveglianza aerea fosse esercitata da un'altitudine che sfugge alla tua percezione uditiva, potresti non accorgerti di essere sorvegliato.

Alcune misure utilizzate per contrastare la visione termica e ad infrarossi includono l'utilizzo di speciali "coperte termiche": un panno di consistenza metallica che intrappola il calore corporeo e che quindi riduce le tracce termiche, così come si possono ridurre immergendosi nell'acqua.

8. Aggirare la Sorveglianza

Le misure di contro-sorveglianza solitamente vengono prese per aggirare la polizia/intelligence mentre si praticano attività segrete. Quando ci si prepara per la contro-sorveglianza, un individuo potenzialmente sotto sorveglianza dovrebbe tenere in considerazione i suoi movimenti e le sue attività abitudinarie del lungo periodo di tempo precedente. Ciò gli permette di individuare possibili orari, luoghi e metodi per aggirare la sorveglianza. Dopo aver sorvegliato per lungo tempo il target, gli stessi operatori possono cadere vittima della sua routine e diventare vulnerabili alle misure di contro-sorveglianza.

Il principale obbiettivo della contro-sorveglianza è aggirare gli agenti della polizia/intelligence. Per esempio, se è possibile fuggire dallo stakeout iniziale o dalla sorveglianza a scatola, il target può mandare in tilt la sorveglianza e muoversi senza il pericolo di venire osservato. Le tecniche per scovare la sorveglianza, come le inversioni ad U, le double-back, deviazioni cieche, etc. possono essere utilizzate anche per aggirare la sorveglianza.

Aggirare gli stakeout o le scatole di sorveglianza può essere fatto in ogni punto del tragitto e non necessariamente appena si esce dalla propria residenza. Edifici pubblici con uscite multiple o segrete possono essere utilizzati a tale fine. I trasporti pubblici possono essere altrettanto utili per disperdere il team di sorveglianza, etc.

I camuffamenti possono intensificare notevolmente le misure di contro-sorveglianza. Gli operatori devono riconoscere il target per poterlo seguire. Sebbene i tratti facciali siano il modo migliore per identificare individui specifici, gli operatori fanno affidamento alla statura, all'abbigliamento e al comportamento.

L'apparenza fisica si può alterare in molti modi:

- L'abbigliamento gonfio o attillato può alterare la forma. Imbottire gli indumenti può far apparire più largo o corposo.
- Cambiare lo stile o i colori del proprio abbigliamento.
- Cambiare la postura o l'andatura.
- Utilizzare parrucche e anche make-up da teatro.

Se l'uso dei camuffamenti viene riconosciuto dagli operatori, questi comprenderanno l'intenzione del target di aggirare la loro sorveglianza per prepararsi ad una possibile attività segreta. Per ogni azione di contro-sorveglianza occorre metterci grande cura e pianificazione, e i camuffamenti dovrebbero essere efficaci. E' buona cosa tenere in considerazione la possibilità di cambiarsi le scarpe.

In un ambiente urbano, le azioni di contro-sorveglianza praticate a piedi hanno molte più possibilità di successo rispetto a quelle fatte con i veicoli. C'è un numero limitato di zone in cui un veicolo può transitare (strade, autostrade, garage, vicoli, etc.). In aggiunta i veicoli possono aver attaccati i congegni per la localizzazione; quindi non importa quante inversioni ad U o quante deviazioni cieche si facciano, gli operatori sapranno sempre dove si trova il veicolo.

D'altro canto spostarsi a piedi garantisce un'agibilità quasi illimitata. I target che si muovono a piedi possono sfruttare i terreni e i percorsi del tragitto per eludere i team di sorveglianza. I trasporti pubblici, specialmente le metropolitane sono difficili da pedinare per gli operatori, sia per l'alta velocità , per la facilità nel cambiare le direzioni, per le uscite multiple dalle stazioni, etc. Luoghi pubblici come i centri commerciali, i complessi di uffici, etc. sono ostili per gli operatori, sia per le uscite multiple, i diversi piani, gli ascensori, etc. In situazioni di emergenza (come quando suona l'allarme antiincendio) gli operatori avranno molta più difficoltà nel seguire il target.

La sorveglianza si può aggirare molto più facilmente di notte o quando ci sono cattive condizioni climatiche (come in condizioni di pioggia) al fine di limitare la visibilità.

Spesso, compiendo azioni illogiche o scomposte in contesti urbani o in locali pubblici permette di identificare gli operatori di sorveglianza e di limitare la loro capacità di seguirti (anche se ciò potrebbe mettere in allerta gli operatori riguardo ai tuoi tentativi di contro-sorveglianza). Prendere l'ascensore per fare un piano per poi scendere a piedi è illogico,

e chiunque facesse in questo modo sarebbe altamente sospetto. Aspettare alla fermata del pullman o della metro senza salirci sopra può costringere gli operatori a salire ad almeno una fermata o a correre il rischio di esporsi. Prendere i pullman o i treni entrando dal fondo per poi spostarsi davanti permette di identificare potenziali operatori. Salire e scendere ripetutamente da un mezzo pubblico può mandare ulteriormente in tilt il team di sorveglianza.

9. Informatori ed Infiltrati

Gli informatori e gli infiltrati sono spie che attingono informazioni all'interno dei gruppi di resistenza per fornirle alla repressione. Possono anche svolgere ruoli molto più attivi. Il loro operato può sfociare nella cattura, gli arresti, l'imprigionamento e perfino la morte dei target sorvegliati. Il termine "collaboratore" viene utilizzato per ogni membro o cittadino che aiuta o assiste la repressione.

Gli informatori e gli infiltrati forniscono alla repressione informazioni uniche e speciali riguardo la vita privata dei target (tratti caratteriali, progetti, intenzioni, etc.) che non possono essere attinte in nessun altro modo. In aggiunta, gli infiltrati e collaboratori possono distruggere fisicamente o sabotare le attività dei movimenti di resistenza. Possono spargere disinformazione e dicerie distruttive, creare divisioni e paranoie. Possono anche registrare azioni e dichiarazioni incriminanti. Soprattutto, loro sono una componente essenziale ed attiva per le operazioni di contro-insurrezione cosi come per le investigazioni.

Gli informatori sono persone reclutate dalla intelligence per raccogliere informazioni. Di solito sono semplici cittadini, a volte amici o conoscenti del gruppo sotto sorveglianza. Possono essere perfino attivisti amareggiati che si sentono isolati o traditi dal gruppo. Oppure potrebbero essere membri del gruppo genuini, arrestati e sottoposti a pressioni. La polizia di solito si riferisce a loro chiamandoli "informatori confidenziali" o anche "fonti confidenziali".

Un metodo standard con cui la repressione recluta i suoi informatori è trovare persone (dentro o attorno al gruppo sotto sorveglianza) con problemi. Le persone più vulnerabili a questo reclutamento sono quelle che cercano protezione o che cercano vendetta, persone affette da tossicodipendenze o da alcoolismo, persone che soffrono di traumi o di disturbi mentali, persone che rischiano di scontare lunghissime sentenze di prigione o anche quelle che sono finite in situazioni compromettenti (dicasi "estorsioni"). L'intimidazione e la coercizione possono essere utilizzate per costringere una persona a diventare un informatore. Il denaro può essere un altro fattore che spinge le persone a diventare informatori e a farle svolgere questo ruolo anche per periodi di tempo molto lunghi.

La repressione impiega la stessa sorveglianza per identificare i potenziali informatori. Relazioni personali, problemi di droga o di denaro, attività sessuali, conflitti personali, conflitti di potere interni al gruppo, etc. vengono tutti analizzati dalla repressione al fine di trovare una fessura attraverso cui fare pressione per conquistarsi potenziali informatori.

Alcuni attivisti arrestati e sottoposti a pressioni possono crollare e collaborare con la polizia. In certi casi questo crollo può essere dovuto ad una mancanza di convinzione nella lotta. E' importante che all'interno di un movimento di resistenza i suoi membri non vengano spinti ad agire sotto alcuna forma di pressione, coercizione e tanto meno intimidazione; ma che pratichino queste azioni in base ad una forte convinzione sull'importanza dell'agire per il movimento. Gli studi hanno dimostrato che le persone più resistenti alle torture e alle pressioni sono quelle spinte da un ideale forte, e non da interessi economici personali ne da questioni di prestigio sociale.

Un individuo che diventa un informatore, avendo tradito la fiducia dei suoi amici e dei compagni, si ritrova sempre più succube della protezione fornitagli dagli agenti della polizia e dell'intelligence per cui lavora. Gli informatori possono essere membri marginali o semplici simpatizzanti che osservano e raccolgono informazione tranquillamente, mentre altri potrebbero venire incoraggiati dai loro protettori a diventare più attivi, fungendo da agenti provocatori (informatori o agenti infiltrati che provocano azioni solitamente illegali per far arrestare gli attivisti).

Gli infiltrati di solito sono civili arruolati dalle forze di sicurezza dello stato (o delle aziende private) o anche agenti di polizia/intelligence. Questi si inseriscono all'interno del gruppo fingendo di essere attivisti genuini dediti alla causa del movimento, nel senso stretto e in senso largo del termine. Possono appartenere a qualsiasi etnia, corporatura, etc. (ovviamente dipende dal gruppo sotto osservazione). Gli infiltrati della polizia hanno dimostrato in più occasioni di immedesimarsi fedelmente al loro ruolo nel gruppo, apparendo e atteggiandosi secondo la loro parte (un esempio sono le investigazioni segrete sulle bande di motociclisti).

Gli infiltrati possono permanere per lunghi tempi ed essere coinvolti profondamente nel gruppo, possono instaurare amicizie intime, possono fornire un peso determinante all'interno delle funzioni dell'intelligence cosi come all'interno delle investigazioni. Oppure possono essere temporaneamente operativi svolgendo obbiettivi specifici (per esempio neutralizzare i leader di un gruppo). Alcuni infiltrati vengono detti "agenti provocatori" quando il loro obbiettivo primario è istigare gli attivisti a compiere attività di vario tipo (spesso illegali).

Gli infiltrati consolidano il loro ruolo in un lungo periodo di tempo, durante il quale si incontrano con i membri del gruppo ed instaurano con loro rapporti di amicizia. Ciò può cominciare con incontri occasionali, interessi comuni, eventi, raduni, etc. Dietro le attività di infiltrazione c'è sempre uno studio minuzioso dei profili psicologici dei membri del gruppo (perché gli infiltrati devono sapere quando e dove essere e in che modo agire).

Spesso è un informatore ad introdurre l'infiltrato nel gruppo, Gli infiltrati possono farsi amici di un membro del gruppo al fine di entrare in contatto col gruppo intero.

Gli infiltrati possono entrare anche in un gruppo spacciandosi per membri genuini di un altra zona o regione in cui hanno preso parte al movimento. Loro possono dichiarare di conoscere certe persone o di esser stati in certe iniziative ed eventi al fine di ottenere credibilità presso il gruppo. Una tipica copertura di chi si infiltra nei gruppi radicali è spacciarsi per uno studente; difatti le università stanno reclutando personale per le agenzie di intelligence.

In certi casi gli infiltrati possono rifornire al gruppo diverse risorse, tra cui il denaro, i veicoli, armi o informazione; tutte cose che possono essere molto utili e che innalzano il prestigio e l'influenza dell'agente infiltrato all'interno del gruppo stesso. A volte possono anche raggiungere ruoli chiave all'interno del gruppo o assumere la leadership o la gestione delle misure di sicurezza al fine di estendere la loro influenza e il loro accesso all'informazione (al riguardo si può leggere il capitolo decimo di questo opuscolo intitolato "tecniche COINTEL-PRO dell'FBI").

bew are the infiltration

Note dal "Security Culture: A Handbook for Activists", edizione Novembre 2001:

Tipologie di informatori

- *L'informatore "bazzicante" ("the hang around type" in inglese, NdT):* sono persone che partecipano agli incontri e alle attività regolarmente, ma che di solito non vengono coinvolte. Queste raccolgono documenti, ascoltano le conversazioni e osservano chi e che cosa. Questo modo di osservare è relativamente passivo.

- *L'informatore "dormiente" ("the sleeper type", NdT):* il loro modus operandi è simile a quello dell'informatore "bazzicante", eccetto per il fatto che il loro assorbire informazioni viene usato per attivare il loro ruolo in un secondo momento.

- *L'informatore "neofita" ("the novice type", NdT)* presenta un atteggiamento in qualche maniera più attivo, ma si limita a partecipare ad attività meno eclatanti. Non prendono l'iniziativa ma il loro operato viene comunque apprezzato dal gruppo. Il loro atteggiamento aiuta a conquistarsi la fiducia e la credibilità del gruppo.

- *Il "super attivista" ("the super activist type" NdT)*: compaiono dal nulla e d'improvviso sono ovunque. Che si tratti di un incontro, di una protesta o di un'azione loro sono sempre al centro della scena. Tieni in considerazione che atteggiamenti del genere possono presentarsi anche da parte di nuovi attivisti genuini, la cui dedizione ed entusiasmo sono cosi forti da spingerli a voler combattere il potere in ogni momento della giornata.

Occorre sottolineare che con tutti questi modus operandi è difficile distinguere l'atteggiamento di un infiltrato da una persona sinceramente dedita al movimento. Allora, come si possono distinguere? Un infiltrato potrebbe fare un sacco di domande sui gruppi di azione diretta, su individui e su attività illegali. Potrebbe suggerire possibili obbiettivi e proporsi volontario per fare ricognizioni così come per prendere parte all'azione. Gli infiltrati potrebbero anche tentare di costruire profili sui membri del gruppo; conoscerne a fondo le loro convinzioni, le loro abitudini, le loro amicizie e le loro debolezze. Tutto ciò mentre celano agli altri attivisti la loro vera identità.

Chiunque faccia un sacco di domande sull'azione diretta non deve essere necessariamente considerato un infiltrato, ma sicuramente DEVE ESSERE qualcuno a cui prestare attenzione. Quantomeno è una persona che ha bisogno di essere informata riguardo le problematiche della sicurezza. I nuovi attivisti dovrebbero comprendere che le tattiche di azione diretta sono rischiose e che fare troppe domande mette a rischio la gente. Se quella persona persiste nel fare domande, costituisce un problema e quindi andrebbero prese delle misure appropriate. Gli attivisti che non comprendono l'importanza della sicurezza dovrebbero essere tenuti lontano da situazioni in cui potrebbero finire per incriminare altri.

L'infiltrato speciale

("the undercover Infiltrator", NdT).

"Un infiltrato speciale, altamente addestrato, è fornito di documenti di identità falsi (in cui di solito viene preservato solo il suo vero nome di battesimo affinché non si scordi di rispondere quando viene chiamato) e un'ossatura base della sua storia personale, tra cui un qualche datore di lavoro che attesti di averlo assunto nella sua attività (e che poi vada a notificare alla polizia che qualcuno sta indagando sulla vita dell'infiltrato). Il vissuto dell'infiltrato speciale potrebbe venir celato per prevenire che egli, parlandone, si contraddica o cada in errore. Alla fine, un vero infiltrato speciale potrà arrivare a praticare un vero lavoro, affittare una casa o un appartamento e vivere dentro il suo ruolo 24 ore al giorno.

"Un infiltrato speciale che lavora sotto copertura potrà avere anche i documenti falsi, ma prima o poi vorrà anche tornare a casa dalla sua famiglia e alla sua "*vera*" vita (di solito in un'altra città). A volte gli agenti della narcotici o di altre speciali unità dovranno togliersi la maschera."

(Ecodifense: A Field Guide to Monkeywrenching, Foreman and Haywood, Abzzug Press, Chico CA 1996, pag. 296).

Incontri tra informatori e i loro superiori

("informant-handler meetings", NdT).

Come parte di un'operazione segreta, gli infiltrati/informatori devono scambiarsi informazioni, equipaggiamenti o denaro con i loro "superiori". Il modo più sicuro è l'incontro faccia-a-faccia. Per esempio l'FBI ha preso in affitto appartamenti per permettere questi incontri diretti, o per disporre di depositi anonimi in cui lasciare messaggi, registrazioni, etc. e anche per avere rifugi sicuri in cui riposare. In altre circostanze l'informatore ed il suo superiore si possono incontrare in un parcheggio, in tal caso uno dei due sale sull'automobile dell'altro.

"Per mantenere la sicurezza, Tait [un informatore all'interno degli Hells Angels] e gli agenti si ritrovavano in posti segreti... Un agente si piazzava in un parcheggio interno e Tait si introduceva nella sua automobile. Quindi loro guidavano fino ad arrivare ad un motel o ad un locale pubblico di un'altra città, luoghi presidiati esternamente da altri due agenti". (*Hells Angels: into the Abyss, di Yves Lavigne, Harper Collins Publishers Ltd., Toronto* 1996, pag. 237-238).

Quando devono comunicare via telefono, di solito uno contatta l'altro sul suo beeper/pager, lasciandogli un recapito telefonico a cui potergli telefonare in tutta sicurezza. Raggiunto questo livello di precauzione, i loro dialoghi sono comunque limitati ed in codice:

"Tait chiamò McKinley [l'agente dell'FBI suo superiore] ad Oakland per riferirgli le novità. Non chiamò mai alla residenza di McKinley perché gli Hells Angels avevano accesso alle registrazioni delle compagnie telefoniche... Alla stessa maniera, McKinley contattò sempre Tait." *(Hells Angels: Into the Abyss, pag. 147).*

Come comportarsi con gli informatori e gli infiltrati

Come per la sorveglianza, scovare gli informatori e gli infiltrati può essere difficile. Alcuni lavorano molto duramente per nascondere la loro attività e per recitare il loro ruolo di membri genuini del movimento. Intuito, osservazione e analisi delle attività e della condotta di una persona possono essere di aiuto nell'identificare possibili informatori ed infiltrati. Si dovrebbero svolgere ricerche sul passato di quelle persone sospette al fine di confermarne l'identità (malgrado un'operazione di sorveglianza ben organizzata avrà provveduto a costruire per bene l'identità falsa dell'agente infiltrato). Gli stessi gruppi di attivisti possono organizzare le loro operazioni di sorveglianza per conoscere di più sulla gente sospetta.

Almeno finché non risulta molto evidente, denunciare e accusare pubblicamente i sospetti spesso può fare più male che bene al movimento. Un atteggiamento del genere potrebbe generare eccessive paranoie, rivalità personali o faide interne, etc. specialmente quando non c'è una forte evidenza. A volte si può impedire alla persona sospettata di partecipare ad attività sensibili (come possono essere le comunicazioni, la gestione dei fondi, il trasporto,

le discussioni sulle tattiche o sulle strategie, etc.) con modi discreti.

Quando si affrontano gli infiltrati e gli informatori, la loro reazione più comune sarà di rigettare l'accusa rivoltagli contro. Spesso andranno ad enfatizzare tutti i rischi, i sacrifici, e la lealtà che hanno dimostrato. Useranno le reazioni emotive altrui per conquistarsi la simpatia degli altri membri del gruppo (specie quelli che potrebbero essere meno convinti che la persona accusata sia davvero un infiltrato o un informatore).

Se una persona viene effettivamente riconosciuta come un infiltrato/informatore (come potrebbe risultare da possibili rivelazioni di un tribunale, dall'aver scovato appunti o apparecchi per la registrazione, o per sua stessa ammissione) occorre fotografare questa persona al fine di informare gli altri membri del movimento. Se possibile andrebbe registrata la sua ammissione. Ogni gruppo, ogni spazio chiuso e ogni materiale di cui l'infiltrato/informatore confermato abbia avuto accesso andrebbe accertato dai possibili rischi, dalle password manipolate, etc.

Raccogliere informazioni e dati
("Background Checks" in inglese, NdT).

Quali sono i possibili criteri in base a cui individuare potenziali informatori? Prima di tutto, finché non hai delle ragioni concrete o delle prove concrete che il sospetto sia un infiltrato è meglio non diffondere dicerie che danneggerebbero solo il movimento. I sospetti che spargi andrebbero varati e messi a confronto con qualche dato concreto. Il passato di una persona sospetta si può verificare, specialmente quando questa dichiara di aver partecipato a forme di attivismo in altri ambienti. Consulta i tuoi contatti di questi ambienti; le affermazioni della persona sospetta risultano coerenti, o emergono aspetti ambigui e confusi? Sono mai emersi problemi tra la persona sospetta e quell'ambiente? Avere conoscenti e amicizie in ambienti lontani è un vantaggio assai importante perché rende molto più difficile per un informatore inventarsi il suo passato basandosi su frequentazioni e attività varie.

"Quali sono i mezzi di sussistenza di quella persona? Chi sono i suoi amici? Che tipo di contraddizioni esistono fra i suoi ideali professati e il modo in cui vive? (da "*Security Culture: A Handbook for Activists*").

In una delle operazioni segrete della ATF contro gli Hells Angels (l'operazione Black Biscuit), gli agenti ebbero a disposizione tutta un'ossatura di informazioni false sul loro passato assieme a tanti documenti di identità altrettanto falsi da riuscire ad ingannare la contro-sorveglianza degli Hells Angels, che annovera tutta una vasta rete di investigatori. Gli investigatori privati assunti da questa enorme banda di motociclisti, assieme ad altre fonti dell'intelligence, hanno dato per attendibile la falsa identità degli agenti infiltrati, incrementando pericolosamente il senso di sicurezza nella banda.

10. FBI & COINTEL-PRO

Il famigerato programma di contro-intelligence dell'FBI (COINTEL-PRO) dovrebbe ricordarci a che punto può arrivare il nostro nemico per smantellare la resistenza. Era vero negli anni 60'-70' così come è vero oggi, sicché molti dei militanti di quel periodo sono ancora tra noi e molti di loro sono rimasti in prigione per via di quella strategia repressiva (tra cui Leonard Peltier, Mumia Abu-Jamal, etc.). Alcuni di loro sono morti, uccisi dall'FBI, dalla polizia e da organizzazioni paramilitari durante gli anni 1960-1970. Se non avremo imparato da quegli anni sarà non solo un fallimento per il nostro movimento che rimarrà vulnerabile a quelle tattiche, ma anche un disonore per i sacrifici fatti dalla generazione precedente.

Il programma COINTEL-PRO ebbe le sue radici nella campagna anti-comunista del 1950 (agli albori della Guerra Fredda). I suoi primi target furono i gruppi di comunisti e socialisti, cosi come il movimento per i diritti dei neri. Negli anni 1960 nuovi movimenti di liberazione emersero attorno al mondo. L'attacco degli USA al Vietnam e la resistenza fiera dei vietnamiti generò un clima di ribellione ed insurrezione che si diffuse nella stessa America.

A quei tempi, il programma COINTEL-PRO si estendeva in tutto il paese e coinvolgeva un apparato di sorveglianza molto esteso, informatori, collaboratori, aggressioni, false accuse, imprigionamenti, comunicazioni fabbricate e campagne di disinformazione e di diffamazione, furti, vandalismi, incendi venivano impiegati come strategie repressive letali. Molti organizzatori chiave vennero assassinati, e molti altri di quelli sono ancora in prigione. Tra i più colpiti vi furono le Pantere Nere e il Movimento degli Indiani Americani, cosi anche per i movimenti messicani e portoricani, e in parte anche per il movimento contro la guerra.

L'obbiettivo ultimo di questa campagna controinsurrezionale era di distruggere le organizzazioni dei movimenti di resistenza usando ogni mezzo necessario. Uno dei mezzi privilegiati consisteva nell'instillare un clima di paranoia e paura all'interno dei movimenti al fine di neutralizzarli. Coloro che rifiutarono di piegarsi vennero colpiti con metodi

ancora più violenti, ed alcuni perfino uccisi. Assalti e omicidi violenti contribuirono ad incrementare le paranoie e le insicurezze. Sfruttando le divisioni interne durante un periodo di intensa repressione, la polizia/FBI ebbe successo nel neutralizzare questa prima fase dei movimenti di resistenza negli USA (ma non riuscirono ad ucciderne lo spirito).

Il programma COINTEL-PRO venne alla luce dopo che nel 1971 ignoti scovarono alcune comunicazioni dell'FBI all'interno degli uffici della Pennsylvania. Le indagini del governo dettero l'impressione che il programma COINTEL-PRO venne chiuso; in ogni caso la repressione domestica continuò attraverso gli anni 70', gli anni 80' e 90'. Oggi, nuove leggi anti-terrorismo come il PATRIOT ACT hanno legittimato tante di quelle pratiche repressive del programma COINTEL-PRO, ed hanno pure esteso i poteri dell'FBI, della polizia e delle agenzie di intelligence. In Canada, la RCMP (*la polizia canadese, NdT*) si è dimostrata la migliore allieva dell'FBI; svolgendo contemporaneamente il ruolo di forza di polizia nazionale e la funzione di "polizia politica". Negli anni 70' scoppiò uno scandalo in cui la RCMP dimostrò di aver commesso attività illegali contro gruppi dissidenti, attività come scassinamenti, vandalismi, furti ed incendi. Nel 1995, durante l'assedio al Ts'Peten (Lago di Gustafsen, BC) la RCMP costruì falsi scontri armati e fece uso di armi in zone in cui venne stipulato il divieto di utilizzarle. Un ufficiale delle relazioni pubbliche della RCMP, venne registrato da una telecamera mentre pronunciò questa frase: *" le campagne diffamatorie sono la nostra specialità".*

Metodi COINTEL-PRO dell'FBI

1. Sorveglianza

La sorveglianza estensiva e a largo raggio venne usata per racimolare informazioni sui gruppi e sugli individui, sia sorveglianza tecnologica (cimici, intercettazioni, telefoni, posta, foto e video) che fisica (veicoli e agenti). L'informazione raccolta in questo modo spesso costituì la base per ulteriori azioni COINTEL-PRO. Per queste misure di sorveglianza venne coinvolta l'FBI con le polizie locali assieme ad altre forze repressive. La sorveglianza stessa venne spesso utilizzata come mezzo per instillare paranoie e paure (con strategie di sorveglianza intense e fin troppo evidenti).

2. Infiltrati, informatori e collaboratori

Una delle strategie chiave del programma COINTEL-PRO dell'FBI fu il largo uso di infiltrati ed informatori. Gli informatori, di solito membri disaffezionati o associati al gruppo, vennero reclutati con l'intimidazione e/o col denaro. Questi raccolsero importanti dati sui profili personali dei membri. Nel caso degli infiltrati ed informatori, questi smembrarono attivamente le organizzazioni e permisero alla polizia/FBI di svolgere attacchi mortali senza troppi ostacoli, di creare montature per incriminare gli attivisti, etc.

Tra gli infiltrati si includono gli agenti dell'FBI, i poliziotti in borghese ed anche i civili. In alcuni dipartimenti della polizia, "squadre rosse" lavorarono assieme alle unità anti-bande per prevenire le possibili unioni tra bande e i movimenti di resistenza. Reclutarono perfino infiltrati tra i membri di bande, facendo pressioni col denaro o con la minaccia della galera.

Gli infiltrati molto spesso passarono informazioni e risorse al gruppo (fornite dai loro superiori della polizia/FBI). Spesso, per via della loro esperienza nell'uso delle armi e della violenza, gli infiltrati vennero promossi a posizioni di alto rango nell'organizzazione, tra cui i ruoli di responsabilità per la sicurezza di alcune branchie dell'organizzazione o degli stessi leader.

Ma come fu possibile che i movimenti di resistenza furono così labili alle infiltrazioni? Perché furono organizzazioni completamente pubbliche ed aperte, che reclutavano i loro membri dalla massa di gente. In una situazione simile, gli infiltrati erano facili da piazzare. L'unica area in cui le misure di sicurezza venivano prese in considerazione era il livello della leadership, ed è proprio qui che vennero commessi alcuni dei peggiori sbagli per un movimento di resistenza.

In entrambe le vicende delle Pantere Nere e del Movimento degli Indiani Americani, gli infiltrati riuscirono a raggiungere il cuore dell'organizzazione, spesso con ruoli connessi alla sicurezza del movimento stesso. Alcuni infiltrati recitarono il ruolo dell'attivista "ultra-militante," promuovendo la violenza e cercando di coinvolgere il gruppo in attività illegali. Criminali e prostitute vennero costrette ad infiltrarsi, e una volta all'interno del gruppo, a diffondere droghe, armi e a stimolare atteggiamenti antisociali o violenti tra i membri del gruppo. Altre loro attività consistettero nel costruire prove di colpevolezza, rubare i fondi, sabotare l'equipaggiamento o il lavoro organizzativo, fornire informazioni che portarono agli arresti o agli omicidi di attivisti, cosi come spargere disinformazione, paranoie e divisioni.

3. Diffamare la reputazione degli attivisti
("Bad-jacket, or snitch-jacket" in inglese, NdT).

A volte la repressione può far sì che un membro genuino del movimento venga dipinto come un informatore (o come un ladro, uno stupratore, etc). Spesso, altri informatori vengono usati per spargere dicerie, per costruire prove di colpevolezza, etc. Al fine di diffamare la reputazione di un attivista, la polizia può arrestare frequentemente un gruppo durante i raid, e rilasciare subito l'attivista-target della loro diffamazione (mentre gli altri vengono tenuti in prigione). La stessa polizia può spargere gossip o lasciare indizi che portino a far credere che l'attivista-target sia un infiltrato.
L'obbiettivo ultimo di questa strategia di diffamazione è neutralizzare l'attivista-target togliendogli credibilità agli occhi del gruppo e quindi annullando il suo potenziale organizzativo. Questa strategia ha generato all'interno dei gruppi tutta una serie di interrogatori, assalti e perfino alle esecuzioni di membri genuini sospettati di essere informatori (come successe tra le Pantere Nere).

4. False comunicazioni

Gli agenti della repressione spedirono false lettere agli attivisti e ai vari gruppi al fine di creare disinformazione (lettere con asserzioni di relazioni sessuali tra membri, minacce di morte, etc.). Spesso vennero sfruttate le ostilità esistenti tra i gruppi per aizzarli tra di loro, incrementando l'attrito al punto da spingerli ad assaltarsi ed uccidersi a vicenda.

Un altro esempio di false comunicazioni fu la produzione di falsi notiziari, falsi poster, etc. da parte dell'FBI/polizia, distribuendoli come pubblicazioni genuine del movimento. Questa strategia riuscì a far crollare l'afflusso di finanziamenti per un'iniziativa delle Pantere Nere; in questo caso l'FBI spedì alcuni fumetti offensivi ai finanziatori del movimento spacciandoli per pubblicazioni genuine delle Pantere Nere.

5. Disinformazione mediatica

In collaborazione con i media istituzionali, l'FBI e la polizia condussero campagne di diffamazione e di disinformazione contro i movimenti, le organizzazioni e contro i singoli individui, dipingendoli come dei violenti, dei criminali, dei terroristi o dei malati mentali.

6. Arresti / false prove di colpevolezza / macchinazioni

Accuse insignificanti e macchinazioni spudorate vennero utilizzate per trascinare persone e gruppi nei tribunali ed imprigionarne molti con sentenze molto severe. Ondate di arresti e di accuse prosciugano i movimenti delle loro risorse e del loro tempo, deviando le loro energie dalla resistenza alla difesa legale. L'imprigionamento servì a neutralizzare gli organizzatori ed a spaventare i potenziali attivisti. Molte decine di prigionieri politici e prigionieri di guerra rimangono tutt'oggi nelle prigioni degli USA, imprigionati nel 1970 a causa delle strategie del COINTEL-PRO. Gli arresti e gli imprigionamenti sono serviti per criminalizzare i gruppi e i movimenti.

7. Altre forme di molestie

Altre forme di molestie praticate dall'FBI e dalla polizia consistono nel fermare gli attivisti fuori dalle loro case e dai loro luoghi di lavoro per interrogarli, nel far visite ai loro datori di lavoro, ai loro padroni di casa o ai loro familiari per fare pressioni su di loro (costringendo gli attivisti a perdere il lavoro, a traslocare o a fare i conti con l'ostracismo dei parenti). Gli agenti potrebbero anche fare pressioni per cancellare le prenotazioni dei bus organizzati dai gruppi, o annunciando che certi incontri, raduni etc. sono stati cancellati.

8. Furti, Vandalismo e incendi

L'FBI e la polizia locale si introdussero periodicamente negli uffici e nelle abitazioni degli attivisti al fine di rubare documenti e file, copiarli e/o distruggere le attrezzature presenti. Gli uffici vennero anche incendiati, distruggendo così risorse costose come le presse, i file, gli archivi, etc.

9. Pseudo-gruppi

Falsi gruppi vennero costruiti dagli agenti della polizia/intelligence per screditare il movimento e intrappolare i membri genuini dei movimenti. Negli anni 60' e 70' l'FBI costruì molti pseudo-gruppi per distruggere le campagne politiche (come successe agli Independistas portoricani, ai gruppi contro la guerra, etc.).

10. Violenza omicida (*"Lethal force", NdT*).

Alcuni organizzatori chiave dei movimenti vennero uccisi dalla polizia durante i raid e gli assalti, dai vigilantes (tra cui campeggiavano razzisti di estrema destra), dagli infiltrati dell'FBI o come risultato della diffamazione della loro reputazione pianificata dall'intelligence. Decine di attivisti vennero uccisi durante gli anni 50', 60' e 70', tra cui:

- Fred Hampton e Mark Clark (Pantere Nere) furono uccisi entrambi durante un raid della polizia nella loro casa di Chicago, nel 1969.
- Alprentice Carter e John Huggins (delle Pantere Nere) furono uccisi nel 1969 dai membri di un gruppo rivale, in una faida istigata dal programma COINTEL-PRO.
- George Jackson, un prigioniero e un membro di spicco delle Pantere Nere, venne ucciso nel 1971 durante quello che i media dichiararono come "un tentativo di evasione."
- Fred Bennett, un membro genuino delle Pantere Nere di San Francisco venne ucciso dai suoi compagni nel 1969, dopo che venne abilmente spacciato per un infiltrato da parte di un vero infiltrato dell'FBI. Uno delle Pantere Nere coinvolto nell'omicidio di Bennet subì la stessa diffamazione architettata dall'FBI e venne ucciso a sua volta dalle Pantere Nere nel 1972 (!)

11. Appoggio di squadroni della morte

Nella riserva di Pine Ridge nel South Dakota, almeno 67 membri ed associati del Movimento degli Indiani Americani furono uccisi tra il 1973 e il 1976 dalla polizia della BIA (*"Bureau of Indian Affairs Police": un corpo speciale del governo federale USA che svolge funzioni di polizia all'interno delle riserve indiane; NdT*) e da organizzazioni paramilitari (i Guardiani della Nazione di Oglala, conosciuti anche con il nome di GOONs). I GOONs furono arruolati da un presidente corrotto delle tribù indiane, erano armati, equipaggiati e appoggiati dall'FBI in quanto costituivano una risorsa per le strategie contro-insurrezionali contro la resistenza indigena. I GOONs instaurarono un regime di terrore contro il Movimento degli Indiani Americani e gli indigeni tradizionalisti della riserva, praticando assalti, attacchi incendiari, spari dai veicoli ed omicidi.

Altri esempi di come la repressione ha appoggiato gruppi di vigilantes e gruppi paramilitari sono l'assistenza che l'FBI offrì a gruppi di estrema destra come i Minutemen, la Secret Army Organization e il Ku Klux Klan. Questi ed altri gruppi ricevettero informazioni, equipaggiamenti ed armi per perpetuare i loro assalti ed omicidi. Alcuni ebbero pure contatti con membri dell'intelligence dell'esercito USA. Gli squadroni della morte ed i gruppi paramilitari sono diffusi in molti paesi del terzo mondo.

COINTEL-PRO: alcuni episodi

Assassinio di Fred Hampton & Mark Clark, 1969

Fred Hampton e Mark Clark furono membri della sezione di Chicago delle Pantere Nere, Hampton fu un leader giovane e promettente, un organizzatore altamente efficiente che cominciò a stringere alleanze con altri movimenti ed anche con bande di strada di Chicago, compresi i Blackstone Rangers.

Nel 1968, l'infiltrato dell'FBI William O'Neal si unì alla sezione di Chicago. O'Neal era un criminale meschino, accusato di aver rubato un'automobile e di essersi spacciato per un agente dell'FBI con documenti falsi. In cambio dell'assoluzione da queste imputazioni, O'Neal accettò di infiltrarsi nella sezione di Chicago. Divenne molto rapidamente capo della sicurezza e guardia del corpo di Fred Hampton. Ciò fu dovuto alla sua esperienza con le armi e con la violenza. Al fine di fermare l'alleanza tra le Pantere Nere e i Blackstone Rangers vennero mandate delle lettere contraffatte ad entrambi i gruppi con avvertimenti e minacce rivolti ad uno o l'altro dei gruppi. Tutto ciò portò a violenti scontri tra i due gruppi, istigati da O'Neal.

O'Neal fece pressioni costanti per spingere ad azioni armate e rapine, offrendo armi e addestramento (l'attivista "ultra-militante"). Egli consigliò di munirsi di un aereo per bombardare il municipio, di munire ogni membro delle Pantere Nere di armi e di installare sedie elettriche per interrogare e torturare coloro che fossero sospetti di essere informatori (tutti rifiutarono). Nel giugno del 1969 seminò diverse armi da fuoco negli uffici delle Pantere Nere per fornire alla polizia il preteso per un raid. Questi raid vennero ripetuti nel luglio e nell'ottobre dello stesso anno.

William O'Neal, gangsta infiltrato dell'FBI

Assieme ad altri infiltrati, William O'Neal sottrasse dalle

Pantere Nere i loro assegni, documenti, libri, registrazioni, film, etc. al fine di sabotare i loro sforzi. L'FBI realizzò dei fumetti contraffatti che furono spediti ai finanziatori di un'iniziativa delle Pantere Nere. Questi fumetti furono così offensivi che molti finanziatori ritirarono il loro appoggio economico.

Nel novembre del 1969, l'FBI e la polizia locale cominciarono a pianificare l'assassinio di Hampton. O'Neal fornì una pianta dettagliata dell'appartamento di Hampton, inclusa la locazione del suo letto e della sua testa quando questi dorme.

Il 4 dicembre 1969, quattordici poliziotti armati fino ai denti fecero irruzione nell'appartamento con un mandato per la ricerca di "armi illegali." Poco prima di quella notte O'Neal preparò la cena per i presenti nell'appartamento, inclusi dei drink alcolici contenenti un sonnifero. Alle 4:30 del mattino, la polizia sfondò la porta e sparò immediatamente a Mark Clark che se ne stava seduto nella stanza di fronte e che teneva un fucile. Sfortunatamente Clark si addormentò per il drink passatogli da O'Neal.

Dopo di che, la polizia diresse i suoi fucili contro il muro dove stava il letto di Hampton, nell'area della sua testa. Sia Hampton che Clark vennero uccisi, mentre altri vennero feriti. La polizia di Chicago dichiarò che si trattò di una "violenta sparatoria" in cui le Pantere Nere risultarono pesantemente armate, sebbene l'unico colpo sparato dalle Pantere Nere fu quello partito dal fucile di Clark come riflesso ai colpi infertigli dalla polizia. (Secondo la versione dei media, O'Neal si suicidò negli anni 80').

Douglas Durham, 1973-75

Douglas Durham fu un non-nativo infiltrato all'interno del Movimento degli Indiani Americani per conto dell'FBI. Prima di fare l'infiltrato fece l'ufficiale di polizia nello Iowa e lavorò anche per la CIA, facendo anche alcune esperienze nelle Forze Speciali dell'esercito. Ebbe un addestramento speciale per le demolizioni, i sabotaggi, gli scassi, etc.

Nei primi anni 60' finì dentro la criminalità organizzata, compresi alcuni giri di prostituzione. Questa attività generò conflitti con sua moglie, che morì per una violenta aggressione di Durham nel luglio del 1964. Venne licenziato dalla polizia ed etichettato come un violento schizoide "inadatto per il servizio pubblico."

Durham ricominciò un'altra volta a lavorare come poliziotto dell'intelligence nel 1971. Fu presente durante l'assedio al Wounded Knee nel 1973, fingendo di essere un reporter. Dopo tale evento entrò nel Movimento degli Indiani Americani (AIM) nella sezione dello Iowa, tingendosi i capelli di nero e portando lenti a contatto castane. Qui dichiarò di discendere per un quarto dagli indiani Chippewa.

Per via delle sue esperienze ed abilità, Durham divenne capo della sicurezza per tutto l'AIM ed anche una guardia del corpo di Dennis Banks, uno dei leaders nazionali dell'AIM. Durante i processi per il Wounded Knee del 1974-75, Durham supervisionò tutte le discussioni legali e le strategie, cosi come prese il controllo di buona parte dell'amministrazione dell'AIM tramite il suo ufficio nazionale a Minneapolis (finanziamenti compresi).

Come fecero altri informatori, Durham fece pressioni per spingere il movimento verso attività violente, come sequestri di politici, scontri armati, etc. E' sospettato dell'omicidio di almeno una persona, Janita Eagle Deer, che venne uccisa nell'aprile del 1975. Durham fu l'ultima persona avvistata con lei dopo che venne da lui stesso prelevata dalla casa di un parente. Janita Eagle Deer accusò William Janklow, ai tempi procuratore generale del South Dakota (poi governatore) di aver subito uno stupro da lui.

Nel marzo del 1975, gli avvocati che lavoravano per la commissione di difesa del Wounded Knee ottennero dall'FBI alcuni documenti svelati dal tribunale, uno di questi conteneva un'indagine firmata da Durham. Quando venne messo davanti a questo documento, Durham ammise il suo ruolo di infiltrato per la polizia. La sua ammissione demoralizzò ulteriormente l'AIM, che in quel periodo venne colpita da un'intensa repressione che comprese diversi omicidi, aggressioni, ed imprigionamenti dei suoi membri.

Per maggiori informazioni su questi episodi: "*Agents of Repression: the FBI's Secret War Against the Black Panther Party and the American Indian Movement*", di Ward Churchill e Jim Vander Wall. South End Press, edizione 1990.

11. Alcuni episodi di Informatori ed Infiltrati

Quebec, infiltrato nel FLQ

Negli anni 60' e nei primi anni 70' il Fronte di Liberazione del Quebec (FLQ) diede vita ad alcuni conflitti di guerriglia urbana. Carole de Vault fu una giovane attivista del Partito del Quebec, un gruppo politico egemone che condivise obbiettivi simili alla lotta per l'indipendenza portata avanti dal FLQ. Essa venne coinvolta nella lotta del FLQ, ma presto divenne un'informatrice ben pagata. La sua vera dedizione politica fu per il Partito del Quebec che propugnava un approccio riformista, difatti lei si tenne lontano dall'ambiente militante del FLQ finché questo non minacciò le attività legalizzate del Partito del Quebec. Questo è un esempio di come un informatore possa infiltrarsi in un gruppo e allo stesso tempo fare attivismo per il proprio movimento svolgendo il ruolo di informatore.

Arresti del gruppo "Germinal", 2001

Gli arresti del gruppo militante "Germinal" attivo nell'area *anti-free trade* delle proteste americane del 2001 nella città di Quebec, furono l'esito di operazioni segrete durate per mesi. Il gruppo, avente sede a Montreal fu il bersaglio di un'operazione di polizia che aveva come fulcro della loro sorveglianza il fatto che uno dei membri di quel gruppo era in cerca di lavoro.

La polizia mise in piedi una falsa agenzia di consegna mobili a domicilio, completa di uffici e di camion, gestita da agenti di polizia sotto copertura, i quali affittarono case nei pressi delle abitazioni dei membri del gruppo sorvegliato. Il membro del gruppo fece domanda di lavoro e quindi lavorò per molti mesi a fianco di un agente di polizia che riuscì ad infiltrarsi nel gruppo.

I loro arresti vennero fatti alla vigilia di una protesta di massa del 20-22 aprile, e furono al centro di una campagna mass-mediatica diffamatrice usata dalla polizia per giustificare le loro misure estremamente repressive adottate durante la protesta di massa. Quelli arrestati furono scovati in possesso di maschere antigas, lacrimogeni e di Thunderflashes (dei petardi molto potenti usati dall'esercito per simulare le granate durante le esercitazioni). Nonostante questo, la polizia e i media li dipinsero come un "gruppo armato".

Questo esempio mostra come la polizia che dispone di alti budget per le attività di repressione può investire decine di migliaia di dollari in operazioni ad alto livello per arrestare militanti di basso livello.

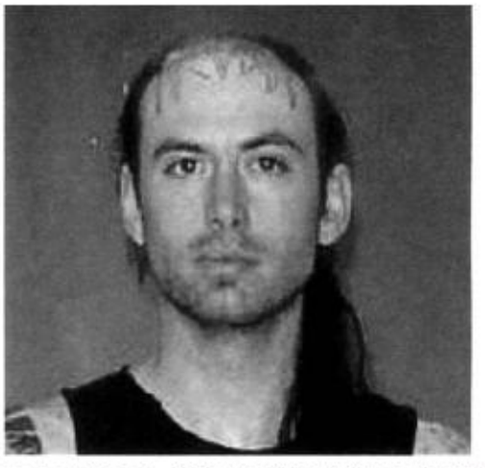
Operazione Backfire: l'FBI arresta membri dell'ELF, 2004-2006

Nel 2004 l'FBI lanciò l'operazione Backfire, riunendo sette operazioni investigative diverse sotto il suo ufficio di Portland, nell'Oregon. Queste operazioni investigative si concentrarono su 16 differenti attacchi compiuti dall'Earth Liberation Front (ELF) tra il 1996 e il 2002 nella parte ovest degli USA, che causarono danni per più di 80 milioni di dollari.

Nel dicembre 2005 e nel gennaio del 2006 l'FBI accusò cinque donne e sei uomini di 65 capi d'accusa, tra cui incendio, utilizzo di apparecchiature distruttive, cospirazione e distruzione di infrastrutture per l'energia. Un prigioniero sotto custodia si suicidò. Questi arresti furono dovuti fondamentalmente all'attività di un singolo informatore:
Jacob Ferguson.

Ferguson prese parte come infiltrato ad lacune azioni dell'ELF e fornì all'FBI i nomi degli altri che parteciparono. Indossò apparecchiature per la ricezione sonora per registrarli in affermazioni incriminanti sulle azioni dirette. Basandosi su queste registrazioni, furono emessi diversi mandati di perquisizione per le case e i luoghi di lavoro degli attivisti, in cui l'FBI sequestrò computer, manuali, documenti di identità contraffatti, abbigliamento, strumenti ed equipaggiamenti vari che vennero sottoposti alle analisi della scientifica ai fini dell'investigazione.

Secondo le ricostruzioni, Ferguson fu per lungo tempo dipendente dall'eroina e cominciò a collaborare con l'FBI nel 2004. Nonostante la sua tossicodipendenza, pare che riuscì a conquistarsi la fiducia e la confidenza del gruppo, che parlò apertamente con lui delle proprie attività illegali mentre questi li registrava di nascosto.



Jacob Ferguson, informatore hippy dell'FBI

12. Linee Guida per la Sicurezza

1). Stabilisci le linee guida per la sicurezza appropriate per il livello delle attività praticate dal tuo gruppo. Un buon punto di partenza è la non-collaborazione con alcun tipo di polizia o agenzia di intelligence. Nessuna discussione su azioni illegali in qualsiasi spazio o incontro pubblico. Tieni sotto controllo l'accesso alle chiavi, password, file, fondi, equipaggiamenti, etc. concedendoli solo a membri fidati. Fai una copia dei file, delle informazioni e dei documenti importanti e depositali in un posto sicuro e segreto. Metti in piedi un gruppo di membri fidati che possano trattare tutto ciò che riguarda la sicurezza, le infiltrazioni della polizia, gli informatori, etc.

2). Interagisci apertamente ai contenuti e alle forme pronunciate o praticate da chicchessia, sia che si tratti di un sospetto infiltrato, di una persona con problemi emotivi o semplicemente di una persona ingenua.

3). Sii consapevole dei potenziali agenti provocatori e degli elementi criminali che incitano continuamente il gruppo ad attività illegali rischiose e che potrebbero anche avere accesso ad armi o ad altre risorse da condividere col gruppo. Molti gruppi negli anni 60'-70' compromisero i principi base della sicurezza per agevolare questo tipo di infiltrati.

4). Non prendere per vero tutto ciò che leggi o che hai sentito dire. Assicurati della genuinità delle tue fonti di informazione prima di agire. Maggiori comunicazioni personali tra membri estranei avrebbero potuto prevenire o limitare molte operazioni dell'FBI durante gli anni 60'-70'.

5). Non spargere dicerie maligne sugli altri; parla con amici fidati (o coi membri di quei gruppi addetti a gestire le situazioni di infiltramenti dell'intelligence). Evita di fare gossip sugli altri, specialmente quando fai uso delle telecomunicazioni.

6). Verifica e ricontrolla tutte le disposizioni per gli alloggi, i trasporti, le stanze per gli incontri, etc. per assicurarti che non siano state cancellate o cambiate da altri.

7). Prendi nota e documenta ogni forma di molestia, furto, aggressione, raid, arresto, sorveglianza, tentativi di reclutare informatori, etc. al fine di identificare le strategie e gli obbiettivi della repressione. Queste documentazioni possono essere usate per fare rapporti e per la difesa legale.

8). NON parlare mai con nessun agente di polizia o dell'intelligence. Non permettere loro di entrare in casa tua se non con un mandato. Cerca di prendere fotografie degli agenti coinvolti. Se i membri ingenui del movimento si lasciano andare a conversazioni con agenti della polizia o dell'intelligence, spiega loro il danno che ne potrebbe conseguire.

9). Metti in allerta gli altri se le molestie dell'intelligence o della polizia si intensificano, (tieni degli incontri, fai conferenze stampa, etc.). Queste misure rendono gli altri gruppi consapevoli delle molestie della repressione e denunciandole pubblicamente, possono limitarle.

10). Prepara i membri del gruppo a continuare l'organizzazione nel caso i leader vengano arrestati, etc. Ciò comporta la condivisione di conoscenze ed abilità, dei contatti pubblici, etc.

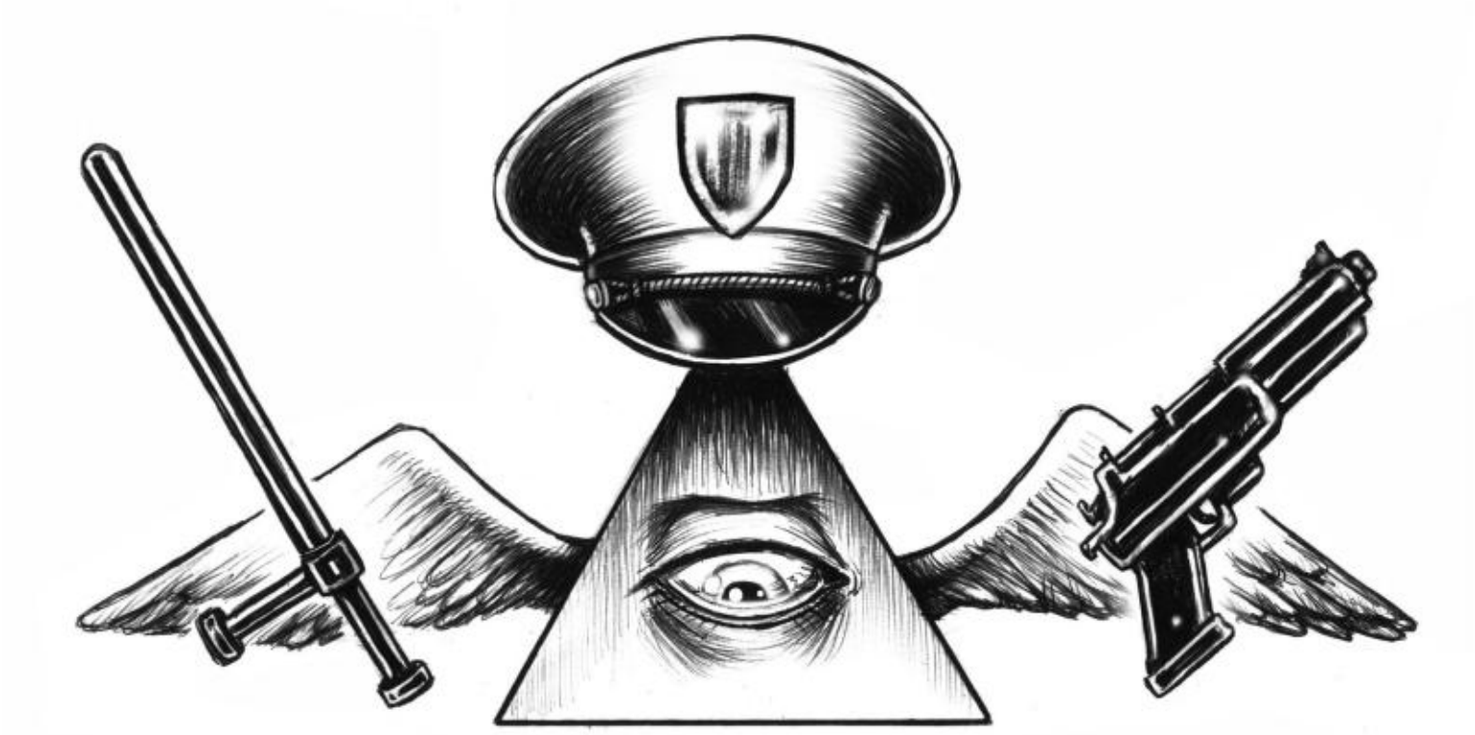
Considerazioni finali (NdT)

Quanto è miserabile una vita trascorsa davanti al buco della serratura?

Una vita a sbirciare quel che fanno altri, ad origliare quel che dicono altri. Una vita da guardoni, che si crogiolano nello strappare brandelli delle esistenze altrui, di persone che nemmeno sono in grado di conoscere nella loro complessità, ma di cui violano senza alcuno scrupolo l'intimità. C'è chi lo fa da dietro un cespuglio, chi lo fa con l'ausilio di una microspia, chi lo fa al riparo di uno schermo. E non è detto affatto che i primi siano i peggiori. Almeno la loro passione non è esente da rischi. Per soddisfarla, mettono pur sempre a repentaglio le loro ossa. Ma che dire degli altri, di chi deve solo premere un bottone e piazzare un'antenna per invadere in tutta sicurezza le emozioni e le sensazioni dei propri bersagli?

citazione estratta da: *"Il buco della serratura"*
articolo apparso su: *www.finimondo.org*

RESISTI AL CONTROLLO SOCIALE
RESISTI ALLO STATO DI POLIZIA



Traduzione in lingua itagliana dell'opuscolo pubblicato negli USA:
"Security & Counter-Surveillance, Information against Police State"

scaricabile liberamente nella versione originale in lingua inglese dal link:
http://anti-politics.net/distro/2009/warriorsecurity-read.pdf

FIP fotocopiato in proprio

GRAFICA NERA

NO-PROFIT
NO-COPYRIGHT
ristampa e diffondi liberamente