Seguridad y Contra-Vigilancia

Información contra el estado policial

Traducción a la edición del año 2009, Vancouver, Canadá/Territorio Coast Salish

Contenido:

"Aquellos en la autoridad le temen a las mascara ya que su poder reside en parte en identificar, clasificar y catalogar: para saber quién eres... nuestras mascaras no son para esconder nuestra identidad sino para revelarla..."

Fragmento del texto "Las 9,000 mascaras" ("9.000 Mask") distribuido en el Carnaval Contra El Capital, Londres, Junio de 1999

"EL gran hermano te vigila, más que nunca antes."

En incontables maneras, la vigilancia emerge como la forma dominante en cómo el mundo se organiza a sí mismo.

El reino unido tiene en estimado 4.2 millones de cámaras de circuito cerrado (CCTV)- una cada 14 ciudadanos. Personas en el centro de Londres son captadas en cámara unas 300 veces al día.

La vigilancia es una condición de la modernidad, integralmente dispuesta al estado-nación y el capitalismo...

Más que nunca antes, nuestras vidas son visibles para otros, desde agencias de gobierno a servicios de seguridad pasando por los dueños de las páginas web que transitamos a las tiendas en las que compramos. Nos siguen en público, en nuestros lugares de trabajo y en el internet, compilando nuestra información personal en masivos almacenes de datos, sorteándonos en categorías de riesgo, valor y confianza.

Cámaras CCTV son solo una de sus herramientas.

Otras incluyen chip de identificación por frecuencias de radio (RFID), localizadores GPS, Cookies de las páginas web, programas de reconocimiento facial y ¿tarjetas de lealtad de tiendas?. Programas computacionales usados por servicios de seguridad pueden monitorear y analizar billones de llamadas telefónicas y correos electrónicos en tiempo real. Incluso se los hemos hecho más fácil para los vigilantes, voluntariamente destapando piezas de nuestra vida en redes sociales como Facebook o en cuestionarios y concursos de internet.

De una manera u otra, la vigilancia siempre ah sido parte de la sociedad humana. Lo nuevo son la tecnologías computarizada que ah hecho posible la integración de vastos y diversos bits de información. También, nuestra obsesión pos 11/9 de eliminar riesgos ah producido una arquitectura de vigilancia de masas en donde todos son tratados como sospechosos.

Don Butler, "Big brother is watching, more than ever before", Vancouver Sun, Feb 3, 2009.

Y para los que realmente son "sospechosos", sigan leyendo...

1. Introducción

La seguridad es vital para el triunfo y sobrevivencia del movimiento de resistencia. Esto es porque tenemos un enemigo que activamente trabaja en sabotearnos, neutralizarnos y finalmente destruirnos. Fallar en lo que a seguridad concierne puede ser la diferencia entre la victoria y la derrota, libertad o aprisionamiento, vida o muerte. No solo para ti mismo, sino también para los que te rodean.

Información conseguida desde varias fuentes, y que está sujeta a análisis y comparación, es llamada **INTELIGENCIA**. La búsqueda de inteligencia es una parte vital de las operaciones de contra-insurgencia, sin ella el enemigo no sabe ni quien, ni cuando, ni como, ni donde atacar.

Las medidas de seguridad y contra-vigilancia están diseñadas para limitar y negar el flujo de información hacia las fuerzas enemigas. Está basada en el principio de que la contra-insurgencia es una parte permanente de la sociedad y los que están involucrados en la resistencia siempre están vulnerables a la vigilancia y la represión.

2. Vigilancia

Vigilancia es la continua y secreta observación de personas, lugares, cosas u objetos, en orden de obtener información.

Hay dos tipos de vigilancia: física y técnica.

Vigilancia física es realizada por el personal del enemigo a pie y/o en vehículo. Es la única manera que la persona objetivo pueda ser observada en un extendido periodo de tiempo. Los equipos de vigilancia pueden ser de dos personas en un vehículo o una docena de operadores en 6 vehículos (o incluso más, obviamente). Adicionalmente, motos, bicicletas, aviones o helicópteros también pueden ser usados.

En esta categoría también debemos considerar a los informantes, infiltrados y colaboradores. Pueden ser agentes de la policía, civiles reclutados por la policía, o "compañeros". Esta forma de vigilancia física es la fuente principal de inteligencia de los pensamientos, planes o actividades de las personas. Es a veces referida como "Inteligencia humana". Debido a la sensible naturaleza de la información personal estos están habilitados para buscarla, y su habilidad para influenciar eventos hace que los infiltrados e informantes sean especialmente peligrosos.

La Vigilancia Técnica es lejos la más común. Con la proliferación del uso de las telecomunicaciones (teléfono, celulares, bíper, internet, fax), la vigilancia técnica en la principal fuente de inteligencia de las actividades del día a día de una persona, sus contactos y sus relaciones personales, etc. En general, esta consiste en aparatos técnicos para grabar, documentar o monitorear los movimientos, conversaciones o actividades de un objetivo individual. Esto incluye aparatos de escucha en casas y autos, teléfonos pinchados, monitoreo de la actividad en internet, Videos CCTV, aparatos de localización, aparatos de visión nocturna, etc.

El ambiente urbano es lejos el más propicio para la vigilancia, dado la gran masa de personas, comunicaciones y sistemas eléctricos, estructuras, y vehículos en donde agentes o aparatos pueden ser implementados. En la ciudad también hay cientos de cámaras CCTV, en tiendas, bancos, malls, oficinas, escuelas, calles e intersecciones.

En áreas rurales, la vigilancia física es más a menudo necesaria debido a la falta de telecomunicaciones, caminos, etc. La baja densidad de población sirve para identificar a los agentes como "afuerinos". Por estas razones la vigilancia física en áreas rurales requiere observaciones a gran distancia (por equipos en tierra, aviones espía o satélites en operaciones de alta prioridad). En algunos casos, policías con camuflaje militar pueden minimizar la distancia de vigilancia.

3. Seguridad

Seguridad n 1. Medidas adoptadas para resguardarse de ataques, robos o ¿desconciertos?. 2. Algo que proporciona o asegura seguridad y confianza...

Como hemos dicho, el propósito de la seguridad es proteger nuestro movimiento. Una parte vital de esto es limitar o negar el flujo de información a las fuerzas enemigas. Los siguientes 4 principios deberían ser líneas básicas y fundamentales de la seguridad.

1. **No mandes o discutas información sensible por ningún medio de telecomunicación** (teléfono, celular, internet, etc.), todas están vulnerables a ser interceptadas. **Los celulares** pueden ser utilizados como micrófonos activos y se deben remover sus baterías antes de discutir cualquier tipo de información secreta.

2. **Nunca discutas información sensible en lugares cerrados** vulnerables a aparatos de escucha (casas, vehículos, cafés, bares, etc.)

3. **Sigue la regla de solo saber lo necesario**: Si una persona no está involucrada en la información, no necesita saber su contenido. Mientras menos personas sepan, menos riesgo hay de que se filtre información.

4. **Evita aquellos que son incapaces de seguir los códigos básicos de seguridad.** Son peligrosos para ti y para el movimiento. Esto incluye personas que hablan de mas, que no se toman enserio la seguridad, drogadictos, etc.

4. Principios de la vigilancia.

Como hemos dicho, la vigilancia es la secreta y continua observación de una persona, lugar, vehículo, u objeto en orden de ganar información. Para que sea efectiva, la vigilancia debe ser pasar desapercibida e indetectable. En cuento el/la objetivo esté al tanto de estar bajo vigilancia, alterara su comportamiento y cancelara cualquier tipo de actividad "sospechosa", como también detendrá el flujo de información. Por estas razones, la vigilancia puede ser difícil de detectar ya que se esfuerza en estar cubierta y escondida.

La entrega de información a través de la vigilancia es progresiva y a menudo un largo y lento proceso. Es desde la recolección de una variedad de piezas de información del objetivo en pos de entregar un patrón.

La vigilancia normalmente parte con limitada información de las actividades, residencia o lugar de trabajo del objetivo. Más información será entregada en orden de identificar tiempos, locaciones, rutas de viaje, o actividades para focalizar los esfuerzos de la vigilancia (esto se conoce como **análisis del patrón del objetivo**)

Mientras más extenso sea el esfuerzo de la vigilancia, mayor será la cantidad de información producida. La extensión de la vigilancia depende de la importancia que la inteligencia policial le dé al objetivo, y las habilidades de estar atento y conocimientos en contra-vigilancia del mismo. (Objetivo suave vs. Objetivo duro)

Solo leyendo este manual puede hacerte un objetivo duro.

Dado los recursos y las capacidades de nuestro enemigo y su intento de monitorear y reprimir tendencias rebeldes (en las que debemos asumir que somos parte), la vigilancia en contra de nuestros movimientos debe ser siempre considerada como posible (si es que no probable).

5. Vigilancia Física

La vigilancia física es realizada por el personal del enemigo (operadores) a pie o en vehículo. Es la única forma en que una persona objetivo

pueda ser continuamente observada por un extendido periodo de tiempo. A pie o en vehículo, los operadores deben mantener el objetivo a la vista. Un equipo asignado para mantener la línea de visión se dice que tiene el **"comando"** del objetivo. En orden de no ser detectados, el comando es frecuentemente cambiado, para que ningún operador o equipo este en la línea de visión del objetivo por mucho tiempo (**cambio de comando**).

Sofisticados esfuerzos de vigilancia pueden involucrar diferentes operadores y vehículos. En esos casos, el equipo se dispone alrededor del objetivo en una **"caja flotante"** (enfrente, detrás, a los lados, y en rutas paralelas).

Si la vigilancia física está siendo implementada, se puede asumir que también la vigilancia técnica está ocurriendo, y puede haberlo estado haciendo un tiempo antes que la vigilancia física empezara. Esto es porque la vigilancia física requiere múltiples operadores para que sea efectiva, y derrocha personal y recursos. Es por esto que es posible que los operadores tengan acceso a grabaciones de audio de las conversaciones del objetivo en su residencia o vehículo, mientras lo observan.

Operadores y Vehículos de Vigilancia

Los operadores pueden ser de cualquier raza, etnia, tamaño, forma, etc. No solo son usados policías o agentes de inteligencia, también pueden haber civiles y miembros de la familia. Pueden ser hombres o mujeres, jóvenes o viejos. Así mismo, vehículos usados por los equipos de vigilancia pueden ser de cualquier modelo, año, condición, color, etc. La apariencia por si sola raramente revelara un sofisticado esfuerzo de vigilancia. En cambio, son sus actividades las que debemos observar.

En orden de coordinar los esfuerzos de varios miembros de un equipo, equipos de comunicación serán usados por los operadores. Estos usualmente consisten en audífonos puestos en la oreja y micrófonos enganchados en chaquetas o poleras al nivel del pecho o en collares. Un volumen, botones de on/off o aparatos que quepan en algún bolsillo. Variantes de estos incluyen celulares con audífonos y micrófonos, reproductores MP3 o iPods, etc. La proliferación de estos aparatos pueden hacer realmente difícil la identificación de operadores basados simplemente en el hecho de que estén conectados a alguno de estos aparatos.

Vigilancia Estática

La vigilancia estática (ósea que no se mueve) es puesta en los alrededores de las casas o negocios por los que se mueve el objetivo, para observar actividades, patrones de movimiento, asociaciones, o para empezar la vigilancia de un objetivo esperado en la locación (stakeout). Otra forma de vigilancia estática es la de **Punto de Observación (PO)**.

Es usualmente conducida por posiciones elevadas tales como cerros, edificios, apartamentos, o vehículos aparcados en el área. La vigilancia estática puede cambiar a vigilancia móvil con operadores pre-posicionados y listos para seguir.

****

Rural: En áreas rurales, la vigilancia estática puede consistir en equipos armados de reconocimientos (policía o militares) posicionados donde se pueda observar al objetivo. Ya que este tipo de vigilancia requiere técnicas especiales en el terreno (camuflaje), es usualmente desplegado por unidades especialmente entrenadas de la policía o los militares. Otro factor es la variedad de armas de fuego en las áreas rurales (rifles de caza).

Los equipos pueden preparar operaciones en cerros altos o laderas de montañas, usando poderosas cámaras de larga distancia y telescopios o en un tupido bosque, edificios abandonados, campos, arbustos, etc. Los operadores pueden usar ropa camuflada, incluyendo ¿"trajes ghillie"?, y estructuras camufladas en posiciones escondidas (cavando en un área lo suficientemente grande para acostarse en ella, estableciendo un soporte arriba de la cabeza, y cubriéndolo con una capa de tierra).

Vigilancia Móvil

Una vez que la persona objetivo está siendo observada y abandona la locación, la vigilancia se transforma en móvil. A pie o en vehículo, el/la objetivo es seguido hasta que se detiene. Una caja de vigilancia es nuevamente puesta en funcionamiento liderada por un operador que tiene contacto directo con la línea de visión del vehículo o locación (este es el **gatillo**, que alerta a los demás operadores de las acciones del objetivo)

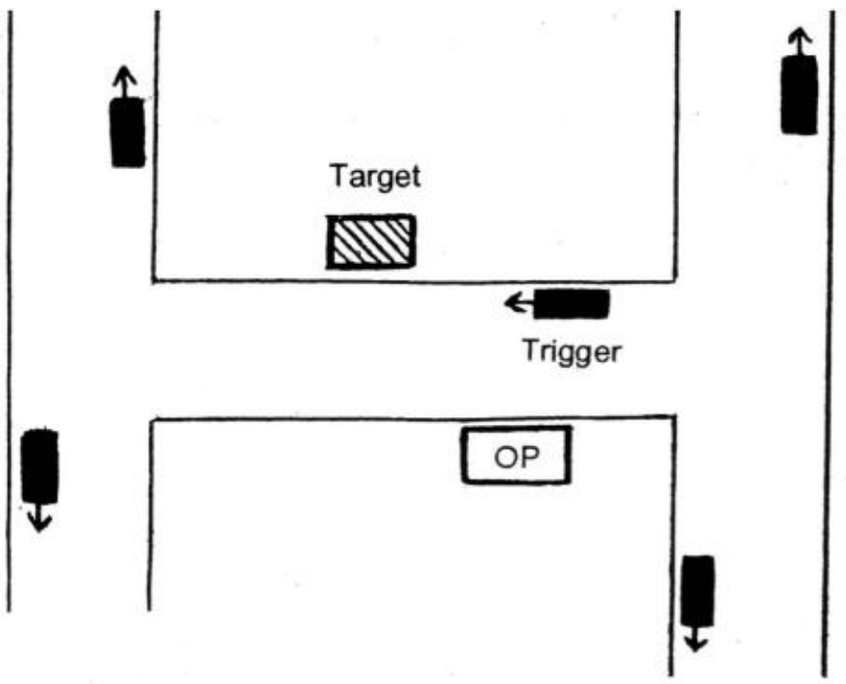
Una vez que el objetivo reaparece en movimiento, la caja de vigilancia estática se transforma en una de vigilancia móvil. En los casos de alta prioridad, la caja de vigilancia cubre todas las rutas conocidas de entrada y salida del objetivo literalmente rodeándolo.

Si una persona maneja, se detiene y camina alrededor, los vehículos de vigilancia sueltan operadores a pie. Estos se posicionaran en una caja alrededor del vehículo del objetivo, o asisten la vigilancia a pie recogiendo y cambiando operadores.
Por su parte, los operadores a pie pueden cambiarse de chaquetas, gorros y otros tipos de ropa para prevenir ser detectados. Una vez detectados, serán removidos del operativo y cambiados por otros operadores. Los operadores pueden también usar bicicletas si es que el objetivo se mueve en ellas o a pie.

******

Rural: la vigilancia en vehículos en áreas rurales presenta algunos problemas por la falta de cobertura en los caminos. La vigilancia aérea puede asistir de una manera espectacular, también los aparatos de GPS (aunque estos no pueden decir con certeza quién maneja el vehículo sin algún tipo de vigilancia de la línea de visión del objetivo). Aun así, la vigilancia móvil en áreas rurales seguirá estos patrones básicos, con algunas modificaciones.

Cuatro fases de la vigilancia móvil (a pie o en vehículo)



Stakeout/Caja de vigilancia

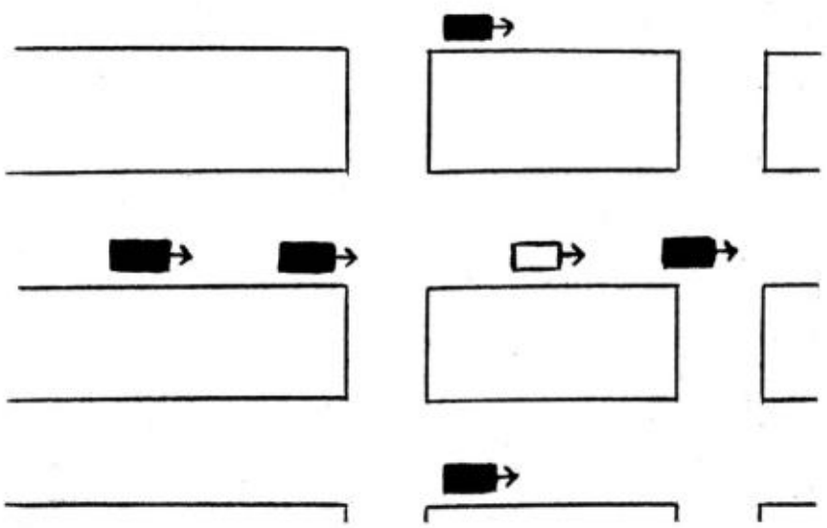
1.Stakeout: miembros del equipo de vigilancia son pre-posicionados en un área específica, usualmente en caja para cubrir todas las rutas de entrada y salida. Puede ser en la residencia del objetivo como también en algún lugar que se espere que visite.

Un Stakeout puede incluir Puestos de Observación (PO). En áreas urbanas pueden usarse apartamentos o casas, vehículos estacionados en la calle, etc. Un PO limita las posibilidades de ser detectada por un largo periodo de tiempo.

2. Levantamiento: ocurre cuando el equipo de vigilancia establece el comando del objetivo entrando y luego saliendo de una determinada área.

3. Seguimiento: empieza inmediatamente después del levantamiento. Esta fase cubre todos los aspectos de la vigilancia mientras el objetivo se mueve de una locación a otra.

4. Caja de vigilancia: comienza los más pronto posible luego de que el objetivo se detiene en otra locación. Una caja de vigilancia estándar cubre todas las rutas de entrada y salida de un área especifica. La diferencia más importante entre el stakeout y la caja de vigilancia es que en un stakeout, es realizada antes de que el objetivo aparezca. En una caja de vigilancia es conocido que el objetivo está en un área o locación especifica.



Caja Flotante

Otras formas de vigilancia física

Correo: aunque no es tan usado como el email, la policía y las agencias de inteligencia tiene un largo historial de interceptar entregas postales, incluidas cartas y paquetes. Los agentes pueden obtener autorización de interceptar el correo, las que se atrasan en la entrega mientras ellos las abren, inspeccionan el contenido, y luego las vuelven a sellar. Esta no es una forma segura de comunicarse ni trasportar elementos.

Basura: inspeccionar la basura personal de las personas es una

práctica común usada por la policía, la inteligencia, y los investigadores privados. Esto incluye notas viejas, cartas, cuentas, recipientes, flyers, prescripciones, dibujos, etc. Todas las cuales pueden aportar información personal o de negocios. La basura también puede ser una fuente de evidencia forense (residuos, químicos, fluidos corporales, pelo, etc.)

Vigilancia vecinal/ Ciudadanos vigilantes: estas entidades usualmente tienen contacto directo con la policía a través de grupos de vigilancia vecinal o centros comunitarios de la policía. Deberán ser considerados como una forma de vigilancia física en cuanto estos puedan reportar cualquier observación que hagan de ti, tus actividades, amigos, etc. También pueden proveer a la policía de lugares de vigilancia en sus casas o negocios.

6. Vigilancia Técnica

Como hemos dicho, la vigilancia técnica consiste en la utilización de aparatos o tecnologías para monitorear y/o grabar las actividades del objetivo. Hoy en día, la vigilancia técnica esta propagada por la sociedad, dada la entrega de nuevas tecnologías y equipamientos.

Telecomunicaciones

Teléfonos, celulares, Internet, fax, y bipers son especialmente vulnerables a la vigilancia dado el control del gobierno y las corporaciones, y su uso de tecnologías digitales computarizadas en los sistemas de telecomunicaciones. Estas permiten un gran acceso, almacenamiento, retribución y análisis de las comunicaciones, sin la necesidad de accesos físicos a las residencias o lugares de trabajo.

Teléfonos: Los teléfonos pueden ser transformados en aparatos activos de escucha a través de una técnica conocida por a hook switch bypass, incluso cuando no están en uso. Los celulares y teléfonos inalámbricos están entre las formas menos seguras de comunicación ya que pueden ser interceptadas por rastreadores que podemos encontrar en el comercio.

Celulares: Los celulares, ya que operan a través de satélites y redes de torres trasmisoras, pueden ser usados para rastrear los movimientos de una persona y su locación. Los celulares también pueden ser trasformados en aparatos activos de escucha, incluso cuando no están en uso. Muchos de estos también tienen adosados cámaras digitales y capacidades de video. La proliferación de los

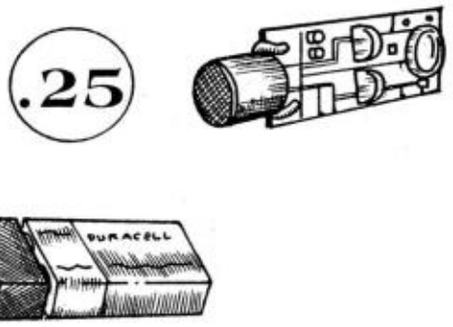
celulares y sus capacidades expanden de gran manera el potencial de la vigilancia, mientras reducen la visibilidad del operador con cámara (o sistema de comunicación)

Computadores e Internet: Como los celulares, la Internet es una muy insegura forma de comunicación. Los emails que mandas, o las paginas que visitas en tu computador personal, pueden ser interceptas al igual que una llamada telefónica. Si tu computador es reducido o robado por la policía, ellos pueden tener acceso a una gran cantidad de información (como mails, vistas a paginas, documentos, fotos) incluso si las has borrado. Esto es porque en vez de realmente borrar la información, el disco duro de tu computador solo reescribe la información si es que lo necesita. Encriptadores pueden ser instalados en la computadora como una forma de deshabilitar la vigilancia, impidiendo leer lo que escribes. Además, cuando estés conectado desde tu computador puedes bajar programas que deshabilitan a otros computadores de tener acceso para recopilar información.

Cada vez que te conectas para revisar tu mail, esa locación puede ser rastreada a través de la dirección del Protocolo de Internet (IP). El FBI tiene un programa que pueden bajar a tu computadora a través del mail el cual les proporciona acceso a tu actividad en Internet. Estos métodos han sido utilizados para arrestar personas haciendo amenazas por internet. En algunos casos, la policía identifica la dirección IP la cual adquiere vigilancia en video del sospechoso aumentando las amenazas. También la policía comúnmente revisa las cuentas de Facebook de las personas o sitios similares en busca de textos, fotos o videos incriminatorios.

Aparatos de Escucha

La vigilancia por audio es uno de los principales métodos de grabar conversaciones para buscar información o crear cargos criminales. De hecho, investigaciones multi-millonarias y juicios están comúnmente basados casi en su totalidad en conversaciones grabadas (personas pueden hacer declaraciones incriminatorias para los policías encubiertos o los informantes)



Dos aparatos de escucha inalambricos disponibles en el mercado; el de arriba puede ser enchufado a una fuente de energia en la habitacion/vehiculo. La de abajo se conecta a una bateria de 9V.

Los aparatos de escucha, también conocidos como **bichos**, son usualmente pequeños micrófonos atados a trasmisores y fuentes de poder y son colocados en residencias, lugares de trabajo, vehículos, etc. Pueden ser tan pequeños como 3 x 2.5 cm. Estos trasmiten a un recibidor, que usualmente se encuentra en el área (puestos cercanos de vigilancia y/o vehículos). La proximidad del recibidor dependerá en el rango efectivo del aparato. A veces, la policía tiende a usar edificios abandonados, azoteas, u otras áreas posando de trabajadores en orden de recibir las trasmisiones del aparato.

Los aparatos más comunes de escucha son **inalámbricos** y trasmiten al recibidor cercano usando frecuencias de radio. Tienen que tener una fuente de energía. En aparatos sofisticados, pequeñas pero poderosas baterías son usadas y pueden durar meses. En modelos más baratos paquetes de baterías son enganchados y escondidos junto al micrófono. Por supuesto, mientras mas largo los paquetes de batería sean, más fácil de detectar son y tendrán que tarde o temprano ser remplazados por baterías frescas. Los aparatos también pueden ser enganchados al sistema eléctrico de la casa o las fuentes de energía de un auto.

Otras formas de dispositivos de escucha pueden ser **micrófonos cableados**, en donde un cable va desde el micrófono directamente al recibidor, usualmente en una habitación o departamento continuo. Los micrófonos cableados no necesitan una fuente de energía ya que son alimentados por el monitor atreves del cable. Los micrófonos cableados tienen mejor calidad de sonido pero nos son tan comúnmente usados hoy por su gran potencial de ser descubiertos (a través del cable).

Los aparatos de escucha son puestos en lugares donde usualmente ocurren las conversaciones, como el living, la cocina, piezas, y vehículos. Pueden ser escondidos en los interruptores de la luz, tapas de la pared, lámparas, detrás de cuadros, en el entretecho, paredes, conductos de aire, etc. En operaciones de alto nivel, los aparatos también son colocados en bancas del parque y cafés que son frecuentados por el objetivo.

También scanners y otras formas especializadas de equipos pueden ser usados para localizar aparatos, estos no aseguran que un área sea segura. Las nuevas tecnologías pueden superar la localización de los aparatos, y los “bichos” pueden ser apagados a control remoto, cortando temporalmente las trasmisiones de radio frecuencia. El dinero y esfuerzo gastados en adquirir ese tipo de equipos solo alertara al equipo de vigilancia.

Como regla general, todos los espacios cerrados deben ser considerados vulnerables a la vigilancia a través de aparatos de escucha, especialmente los que son frecuentados por miembros del movimiento/asociados, etc.

Otros tipos de aparatos de escucha son aquellos que están en el cuerpo de informantes o infiltrados. Al igual que otros tipos de aparatos, estos tienen un micrófono unido a un trasmisor y una batería. Aparatos de escucha más sofisticados pueden ser encontrados en una enorme cantidad de objetos (cámaras, lapiceras, relojes, mochilas, tazones, etc.). Los aparatos de escucha son usados por el FBI y la ATF en operaciones encubiertas en contra de pandillas de motoqueros escondiéndolos en bipers o baterías de celulares. Tienen botones de on/off con los que pueden ser apagados si es que un scanner está siendo usado para detectar trasmisores escondidos.

Un aparato de escucha estaba contenido en este reloj.

Aparatos laser pueden ser usados para recopilar las vibraciones de los vidrios y convertirlas en señales de audio, por lo tanto graban conversaciones en oficinas, departamentos, etc.

Micrófonos Parabólicos

Poderosos micrófonos direccionales son diseñados para escuchar conversaciones a una gran distancia. También llamados "oídos biónicas", los micrófonos parabólicos son aparatos sujetados a mano con un micrófono direccional y un disco adosado a él. Los operadores usan audífonos. Algunos micrófonos parabólicos tienen un rango efectivo de 300 metros. Las versiones civiles son vendidas para la caza, y algunos son adosados a binoculares (los que tendrán un pequeño micrófono direccional saliendo de su cuerpo).

Cámaras de Video

Los sistemas cerrados de televisión (CCTV) son uno de los más comunes y prolíferos ejemplos de la vigilancia técnica en la sociedad. En cada

ciudad hay cientos de miles de cámaras CCTV, en tiendas, bancos, malls, oficinas, escuelas, calles e intersecciones.


Mini-Camara CCTV

Para operaciones de vigilancia, cámaras CCTV en miniatura son rutinariamente usadas. Han grabado personas haciendo y vendiendo drogas, armas, y bombas, también haciendo declaraciones incriminatorias. Las mini cámaras CCTV pueden ser tan pequeñas como una moneda de diámetro (con una pequeña apertura). Al igual que los aparatos de escucha, las mini-cámaras pueden ser escondidas en casi todo, como un bíper, un oso de peluche, un reproductor de VCR, un reloj, una radio, un detector de humo, etc. (tales aparatos están disponibles en el comercio). En un departamento o habitaciones de un motel o estructuras similares, los equipos de vigilancia pueden tener acceso a través de un pequeño hoyo taladrado en la pared, el entretecho o el piso, insertando la cámara (como se ah hecho en escondites de sospechosos).

Los mini aparatos CCTV tienen que tener una fuente de energía y un trasmisor para entregar la información a un monitor cercano-al equipo de vigilancia (o grabadoras). Como los aparatos de escucha, la fuente de energía puede ser una batería adosada o un cable directamente conectado al cableado de una residencia o la batería de un auto. Cámaras sofisticadas también incluyen visión nocturna.

En casos donde la vigilancia física de un sospechoso es demasiado difícil, o en actividades ilegales que ocurren por grandes intervalos de tiempo, las mini cámaras CCTV son encubiertas fuera de la residencia. Hay detectores de movimiento que solo graban cuando existe algún movimiento. En Alemania el 2007 esta técnica fue usada para monitorear las residencias de sospechosos de realizar ataques esporádicos en el curso de varios meses. (cuando la vigilancia física fue poco productiva)

Poderosas cámaras de video han sido montadas en helicópteros, planeadores o vehículos aéreos no tripulados (UAV). Estos vehículos pueden estar o circular algún área a grandes altitudes, virtualmente fuera de vista o rango de escucha, y aun así individualizar rostros de personas.

Muchos celulares o cámaras digitales tienen capacidad de video. Cada vez mas fuerzas policiales instalan cámaras en sus autos. En el 2007, la policía británica instalo mini cámaras que pueden ser utilizadas desde

el uniforme de un oficial para grabar incidentes y sospechosos. Con pequeños flashes adosados. También hay nuevos radios de hombro utilizados por algunas fuerzas policiacas que tienen mini cámaras de video o de fotos.

Fotografía Fija

El uso de cámaras de 35mm o cámaras digitales son una importante herramienta para el trabajo de vigilancia. Son especialmente útiles para documentar o identificar individuos, locaciones vehículos, etc. En particular los rollos de 35mm y las cámaras digitales de alta definición proveen una clara y concisa imagen en comparación a las de video. Las fotografías deben ser tomadas por un operador con una línea de visión del objetivo. Con lentes zoom de alto poder, acercamientos pueden ser realizados a grandes distancias.

Muchos celulares ahora tienen cámaras digitales instaladas que pueden ser usadas para tomar fotos de personas, patentes, documentos, etc.

Aparatos Rastreadores

Usualmente adosados en el interior de los vehículos, estos aparatos emiten una señal que puede ser rastreada por satélites y tecnologías de celulares (el sistema de posicionamiento global: GPS). Cualquier vehículo equipado con tecnología GPS es capaz de ser rastreado (ej. La red OnStar). Como hemos dicho, los celulares también son dispositivos rastreables.

Una versión documentada de dispositivos de rastreo usados por el FBI consiste en un trasmisor GPS, una antena de celular, un paquete de batería, y su caja correspondiente. Están son puestas en cajas negras de metal, conectada a través de cables, y adosadas a la parte inferior de los vehículos por imanes extremadamente fuertes. El paquete de batería contiene 4 pilas de litio tamaño D, pequeños cilindros de metal. La caja correspondiente es del tamaño de un libro pequeño. Con esto, la locación del dispositivo puede ser determinada en algunos metros.

Aparato de rastreo ProScout (Tamaño Biblia)

Los dispositivos de rastreo disponibles en el comercio, tales como los Quicktrack GPS Tracker, consisten en una caja

de metal negra con potentes imanes. Son de 11 x 5,5 cm de tamaño y las baterías tienen una vida útil de 40 horas en modo de rastreo, y de un mes en standby.

Recientes dispositivos comerciales de GPS son casi tan pequeños como un reloj de muñeca. Dispositivos sofisticados de rastreo pueden ser instalados en cualquier parte del vehículo (no solo en la parte inferior, esto es especialmente cierto si es que el vehículo es dejado sin atención por un largo periodo de tiempo)


— AP

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.

Una variante de los dispositivos de rastreo es la Identificación De Radio Frecuencia (RFID), un pequeño dispositivo (pequeño como un grano de arroz), el cual emite una señal. Es usado por corporaciones para rastrear cargamentos o bienes y para prevenir robos. Los RFID miniaturas son implantados quirúrgicamente en la piel por razones medicas (estos contienen todo el historial médico) al igual que por seguridad (para potenciales víctimas de secuestro). El FBI también ah usado el RFID o dispositivos GPS para rastrear cargamentos de drogas.

Visión Nocturna e Imágenes Termales

Los dispositivos de visión nocturna (NVD) amplifican la luz existente de la luna o las estrellas, pudiendo así ver lo que de otra manera seria completa oscuridad. Usualmente son imágenes verdosas y arenosas.


LCPL GREG MATHESS

GI JOE con Mira de Vision Nocturna

La visión nocturna puede ser limitada por la falta de alguna fuente de luz, fuertes lluvias, niebla, etc. Mientras que la visión nocturna permite ver en la noche o en situaciones con poca luminosidad, las imágenes termales detectan alteraciones en la temperatura. Las cámaras de imagen termal pueden ver a través de la niebla o el humo y es rutinariamente usada por los bomberos para descubrir los puntos de fuego tapados por el denso humo. Motores de vehículos recientemente usados, figuras humanas, tierra recién removida, etc. pueden también ser detectadas. Equipos especializados de imagen termal son también usados para monitorear el movimiento de personas dentro de una

estructura. Por estas razones, ambas visiones termales y nocturnas son usadas con frecuencia por los helicópteros militares o policiacos. De las dos, la NVD es la más comúnmente usada para ayudar en el combate a soldados y equipos especializados de la policía. Ambos dispositivos tanto termales como de visión nocturna pueden venir en formas de lentes, binoculares o miras de rifle. Son comúnmente usados en vigilancia rural cuando hay poca luz artificial. Helicópteros, planeadores o vehículos aéreos no tripulados (UAV) pueden ser equipados con dispositivos de visión termal o nocturna.

Biométrica

Es el uso de características fisiológicas individuales, tales como el reconocimiento facial, scanner de iris, huellas digitales, postura y forma de caminar, imagen total del cuerpo, etc. Dado el avance en las computadoras y la tecnología el uso de la biométrica como forma de identificar y rastrear personas prolifera cada vez más.

Aparato para escanear Iris (izquerda)

En términos de vigilancia, las tecnologías biométricas pueden ser usadas para identificar o rastrear personas en una multitud, basadas en el reconocimiento fácil y/o la imagen corporal. Llamadas telefónicas pueden ser analizadas para identificar las voces. Las huellas digitales pueden ser manualmente digitalizadas para confirmar o establecer identidades (en el lugar). Muchos países están ahora adoptando características biométricas para las nuevas tarjetas de identidad (licencias de conducir y pasaportes), incluyendo scanner de iris y reconocimiento facial. Con el aumento de facilidades para la industria, los gobiernos y oficinas complejas, etc. cada vez más de estas requieren scanner biométricos.

Vehículos Aéreos No Tripulados (UAV)

Los UAV son comúnmente utilizados por fuerzas militares para la

vigilancia y el reconocimiento. Hay muchos tipos de UAV, pero todos sirven como una plataforma aérea de vigilancia que traen poderosas equipos de cámara equipados con visión nocturna y visión termal. Son controlados a control remoto por un operador en tierra que observa el patrón de vuelo del UAV a través de la cámara abordo. Versiones pequeñas, tales como el Raven, Skylark o el EagleScan, son del tamaño de aeroplanos miniatura que pueden ser lanzados a mano. Tienen pequeños tiempos de vuelo y son hechos para ser usados en la línea de fuego de las tropas de combate que requieren el reconocimiento de áreas cercanas. Los UAV más grandes pueden ser equipados con misiles y han sido usados en objetivos de asesinato por el ejército israelí y estadounidense.

UAV Skylark usado por las Fuerzas Canadienses en Afganistan

Satélites

Los satélites son usados por los militares, la inteligencia y las agencias comerciales para una variedad de propósitos, incluyendo imagines digitales, comunicaciones, navegación, etc. Estos son lanzados en orbitas especificas, en las cuales se mantienen en el curso de su vida (más de 10 años en algunos casos). Hay cientos de satélites en órbita alrededor de la tierra.

Los satélites espía mas avanzados son dispuestos por el gobierno estadounidense, incluyendo la serie "Key Hole" (KH) de imágenes satelitales. Las versiones KH-12 y KH-13 pueden identificar objetos pequeños desde 12cm en la tierra (desde cientos de miles de metros en el espacio). También usan radares, laser, infrarrojos, y sensores electromagnéticos para ver a través de nubes, bosques, e incluso estructuras de concreto, creando imágenes y recopilando información.

Las imágenes satelitales son primariamente usadas por la inteligencia militar para monitorear movimientos de tropas, posición de armas, bases, puertos, cargamento de barcos, etc. Son limitados en su uso de vigilancia individual ya que están en órbita y no pueden cubrir estáticamente un área, y por lo tanto no pueden producir imágenes a tiempo real de una locación específica. Además las imágenes aéreas

en cenital no son muy útiles.

Otros satélites de vigilancia son los usados por SIGINT (señales de inteligencia) las que monitorean el trafico de frecuencias de radio y celulares. Hay alrededor de 100 satélites de seguridad nacional de los estados unidos en órbita, los cuales de 6-7 trabajan con imágenes, y de 9-11 trabajan con SIGINT. Canadá y otros estados aliados comparten información a través de redes estadounidenses como Echelon, incluyendo información de los satélites espías.

7. Detectando la Vigilancia

Confirmar la vigilancia puede a menudo ser difícil. Es usualmente hecho para determinar si es que la vigilancia existe (en orden de evadirla). Por estas razones, la detección de la vigilancia obvia debe ser evadida. Si es que los operadores piensan que el objetivo está familiarizado con la contra-vigilancia, estos pueden volverse más sofisticados en su aproximación, y pueden pensar que el objetivo está dispuesto a realizar algunas actividades "ilegales".

En la mayoría de los casos, los operadores de la vigilancia retrocederán si es que creen que han sido detectados. La vigilancia en si puede ser detenida. En otras situaciones, los equipos de vigilancia pueden mantener el comando del objetivo incluso si son detectados (vigilancia descubierta). La vigilancia obvia de la policía es a veces para intimidar al objetivo siendo parte de una operación de guerra sicológica mucho más larga, usualmente diseñada para neutralizar al objetivo a través del miedo y la paranoia.

Detectando la Vigilancia Física

La clave para la detección exitosa de la vigilancia es **estar atentos y observar los que nos rodea**, incluyendo personas y vehículos. En orden de identificar potenciales operadores, has nota de su ropa, tamaño, formas de moverse, características faciales (incluyendo el estilo y el color de pelo, forma de la cabeza y cara, bigotes, marcas, etc.). En particular, cualquiera marca o característica puede ayudar a la retención y la habilidad de luego identificar a los mismos individuos o vehículos.

La mayoría de los operadores tratara de minimizar o neutralizar su reconocimiento. La ropa o el cabello colorido o extraño, etc. serán desechadas por la involuntaria atención que reciben. Por lo tanto, la mayoría de los operadores serán reconocidos por su apariencia casual

y desapercibida.
En orden de identificar posibles operadores, empieza por observar a los de tu alrededor. Asume que todos pueden ser potenciales operadores. Comienza eliminando a los que tiene menos posibilidades de estar conectados con la vigilancia, en orden de enfocar a los que si están. Ten en cuenta que algunos equipos de vigilancia consisten en personas que se ven como si no hubieran pasado los exámenes físicos, y pueden incluir pequeñas ancianas asiáticas, pequeños hombres gordos, etc. La policía encubierta que ah infiltrado pandillas de motoqueros, son facilitados por su propio interés en tatuajes, dejando crecer sus cabellos y no afeitándose. Es más importante evaluar lo que las personas hacen y su comportamiento en vez de su apariencia física.
Los vehículos pueden ser observados por su color, forma, modelo, marcas notables, y patentes. De noche las siluetas del vehículo y la posición de sus luces delanteras pueden asistir a identificar posibles operadores.
Un punto importante en la detección de la vigilancia es observar a un individuo y/o vehículo en una locación, y luego en las locaciones siguientes.

Características Generales de los Operadores de la Vigilancia (A Pie y Vehículos)

- Pueden ser de cualquier raza o etnia, tamaño o forma, viejos o jóvenes.
- Usualmente evitaran el contacto directo de ojos y pueden parecer extraños en su esfuerzo por lograrlo.
- Pueden parecer fuera de lugar, nerviosos y tensos (porque lo están).
- Pueden ser vistos o escuchados hablándole al micrófono de su pecho, ajustándose los audífonos, o usando apartados de mano para ajustar el volumen o la señal (contenidos en sus bolsillos).
- Pueden ser observados haciendo señas (con la mano, la cabeza, etc.) o directamente hablando con otro miembro del equipo de vigilancia.

Técnicas para Detectar

Uno de los mejores momentos para detectar la vigilancia es cuando una ***caja de vigilancia*** ah sido establecida en una locación. Los equipos de vigilancia son más vulnerables de ser detectados durante esta fase

de las operaciones. En algunos casos, pueden estar quietos por horas esperando que el objetivo se mueva o aparezca.

Los Puestos de Observación en departamentos o casas pueden ser a veces identificados por la falta de actividad, luces apagadas, o cortinas, u otras formas de cubrir las ventanas. Ya que están hechas para mirara hacia fuera, y no para que los vean hacia dentro. En orden de ver hacia fuera, pueden tener una pequeña apertura donde colocar el lente de una cámara o el telescopio.

Posibles locaciones para PO pueden ser observadas desde la locación del objetivo (usando el método descrito arriba) como también cuando entra o sale del área. Para los equipos de vigilancia, la locación ideal es un buen punto en la línea de visión de la puerta principal del objetivo y su vehículo.

Mientras más familiarizado se está con el vecindario, mas fácil será identificar vehículos nuevos o incluso vecinos, ambos pueden ser potenciales vigilantes. A veces es poco práctico para la policía arrendar o usar los departamentos o casas de civiles. Cuando esto sucede ocupan un vehículo como Puesto de Observación.

Si es que un **vehículo es usado como Puesto de Observación**, es usualmente una van, mini van, furgón, o camioneta cubierta – lo suficientemente grande para almacenar operadores y equipos de vigilancia. Al igual que el escenario del departamento, un PO de vehículo será reconocible por su falta de actividad y por la nula capacidad de ver dentro de la parte del compartimiento. Cortinas u otras formas de cubrir serán puestas en las ventanas. PO de vehículos pueden estar estacionados por días o ser movidos y remplazados. Un posible indicador de la vigilancia es la presencia constante de vehículos con compartimiento trasero.

Si es que un vehículo coincide con estas características y es estacionado y luego el conductor se aleja caminando y se sube a otro vehículo, puede ser un potencial puesto de observación. En algunos casos la policía puede estacionar un auto normal de pasajeros con un operador escondido en la cajuela. El operador puede monitorear un trasmisor y/o una video grabadora de las actividades a través de un hoyo en la cerradura.

Una variación del PO de vehículo es estacionar un auto con algún tipo de dispositivo para recibir o grabar las trasmisiones de algún emisor cercano (en un edificio, o una persona) o tener instalado una cámara CCTV. El operador deja el auto el tiempo necesario para la operación de vigilancia y lo recoge luego.

******

Cuando se deja una locación, sea en vehículo o a pie, el objetivo individual discretamente observara por signos de un **gatillo** (un operador en la línea de visión) como también al seguidor- una persona o vehículo que también se retira y empieza a seguirlo.

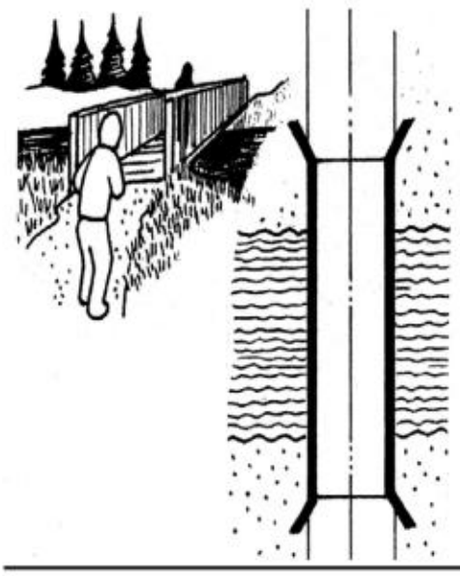
Una persona también puede caminar por el vecindario y observar por posible vigilancia. Llendo y luego volviendo (**doble vuelta**)- como si algo se olvidara – esto puede forzar a los operadores a restablecer la caja de vigilancia, potencialmente exponiéndose.

Otra ocasión en la que los operadores de la vigilancia son vulnerables a ser descubiertos es durante las transiciones de pie a vehículo o viceversa. Observar a personas que se apuran demasiado en entrar a un vehículo, o salir de ellos abruptamente, etc.

Durante la vigilancia móvil, es a menudo las reacciones de los operadores las que revelaran su actividad. Algunos de estos son subconscientes y se convierten en parte de la rutina de la operación de la vigilancia.

Por ejemplo, **reflejando** es cuando el operador de vigilancia duplica tus acciones para seguirte el paso, especialmente en vigilancia con vehículos. **Marcando el paso** es cuando se mantiene la misma distancia constante entre ellos y el objetivo, acelerando o alentándose para seguir el paso.

Tomando ciertas rutas o acciones, los operadores de vigilancia también pueden ser expuestos con la guardia baja.



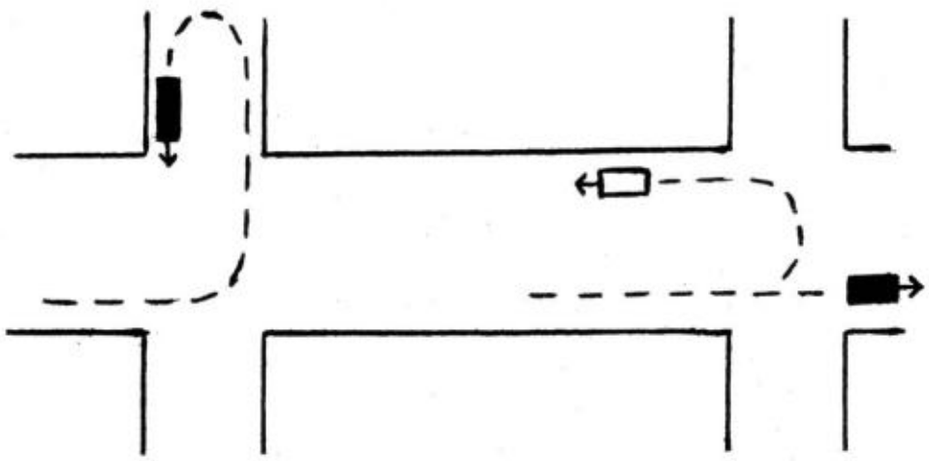
Terreno Canalizado: *el operador debe atravezar el puente para mantener el control del objetivo.*

Moviéndose a través de **terrenos canalizados** se puede exponer a los operadores de vigilancia observándolos. Los terrenos canalizados son cuando todo el tráfico (a pie o vehículo) deben pasar a través de un restringido pasaje o apertura. Un puente es un ejemplo de tal terreno, un túnel, etc. En orden de mantener el comando, un equipo de vigilancia deberá ser asignado a entrar y cruzar el terreno. A pie un objetivo puede caminar hasta la mitad de un puente, detenerse como si disfrutara del paisaje, luego darse vuelta y volver (vuelta en u) para ver la respuesta de otras personas a pie.

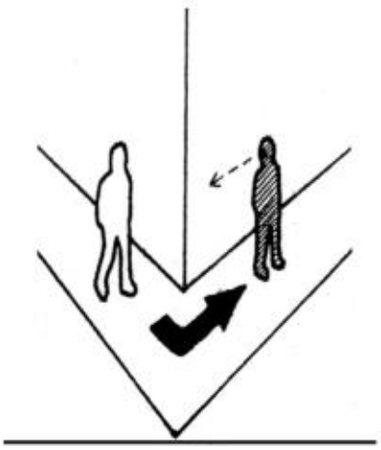
Cuando se camina o se maneja, repentinas **vueltas en u** pueden forzar

a los operadores de vigilancia a una respuesta, por lo tanto revelar su actividad. Los operadores pobremente entrenados o sin experiencia rápidamente darán la vuelta en u y retomaran el seguimiento. Un agente mejor entrenado pasara de largo y luego girara, entregando el comando del objetico a otro vehículo/operador.

Respuesta estandar a las vueltas en U: *el vehiculo controlador continua derecho, mientras el vehiculo de apoyo da la vuelta para comenzar el seguimiento.*



Cuando se camina o maneja, una **curva ciega** puede usarse para forzar alguna respuesta inesperada del operador de vigilancia. Una curva ciega es cuando se gira inesperadamente en una esquina en donde el objetivo se detiene y espera observar las acciones de un potencial operador de vigilancia. Una respuesta estándar de la vigilancia será seguir su camino pasando la esquina mirando disimuladamente las acciones del objetivo. Él/Ella comunicara esto a los otros operadores y pasara el comando a otro miembro del equipo. Los operadores menos experimentados pueden simplemente girar en la esquina y verse enfrentados con el objetivo, posiblemente forzando una reacción inesperada.



Curva Ciega

A pie, la única oportunidad para discretamente observar hacia atrás es en una intersección. Cruzar repentinamente en la mitad de la calle (**jaywalk**) también permite vistas hacia atrás y puede atrapar a los operadores fuera de guardia. Entrando en **locales públicos**, tales como malls, complejos de oficina, etc. puede forzar a la vigilancia a entrar contigo y exponerse a una observación más cercana. Llendo de arriba

o abajo por una serie de escaleras permite giros de 180 grados para observar hacia atrás. Los elevadores pueden forzar a los operadores a una proximidad más cercana. Múltiples niveles también permiten al objetivo observar grandes áreas desde una posición dominante y en altura.

El transporte público también puede ser usado para detectar la vigilancia. Subiéndose a buses o metros pueden forzar a los operadores a disminuir proximidades o el riesgo de perder el comando. Cuando los operadores tienen que subirse a un medio de trasporte público junto al objetivo, proveen una buena exposición de las características faciales y puede provocar respuestas poco naturales de los operadores. Observar aquellos que llegan a las paradas de bus después de ti y abordan el mismo bus que tú, como también aquellos que están ya en el bus y se sientan detrás de ti, o aquellos que se suben en las paradas subsiguientes. Los operadores a pie pueden ser desechados luego de que el objetivo se baje, por lo tanto si es que un mismo vehículo es visto cerca de la ruta del bus, o incluso siguiéndolo, podría ser un indicador de la vigilancia.

En autopistas, estacionarse en las áreas de descanso puede forzar a la vigilancia a retroceder y esperar. Manejando a través del área de descanso, un objetivo puede observar que vehículos se encuentran en el lugar para luego identificarlos en las locaciones subsiguientes. Al igual que en el metro, las autopistas se caracterizan por las grandes velocidades que pueden exponer a los operadores fuera de guardia. Rampas de salida, curvas, áreas de descanso, vueltas en u, curvas ciegas, etc. pueden ser explotadas a tu favor en las autopistas. Las autopistas también ofrecen una observación de largo rango y por extendidos periodos de tiempo.

En ambas vigilancias a pie y vehículo, el comando puede ser cambiado frecuentemente para minimizar la exposición de los operadores. A menudo, impredecibles o repentinos movimientos pueden forzar a los equipos de vigilancia a reaccionar. Sin embargo, si tu patrón a este punto ah sido rutinario y predecible, los operadores podrían sospechar. La detección de la vigilancia es mejor cuando es encubierta dentro de lo posible. En vehículo usa los espejos retrovisores. Colocarse lentes oscuros puede también añadir una observación más discreta escondiendo los ojos.

Rural: Desde nuestra locación potenciales PO pueden ser identificados. Ellos tienen que tener una línea de visión para observar. La única forma posible de encontrar los PO es físicamente recorrer

el área. Los sitios de PO pueden ser identificados por ser lugares alterados o distorsionados en pos de sentarse o dormir en ellos, al igual que caminos, literas, equipo botado por los operadores, etc. El conocimiento de caminos puede asistir de gran forma para identificar sitios de PO. En términos largos PO pueden consistir en escondites dejados en el lugar. Su detección puede ser complementada con perros, como también la observación de la respuesta de animales y aves (en muchas redadas policiales, los perros son los primeros en ser baleados).

Detectando la Vigilancia Técnica

La vigilancia técnica es difícil de detectar, especialmente si corresponden a telecomunicaciones. Una regla general en cuanto a la vigilancia técnica es asumir que esta siempre es posible y proteger la información como si fuera objetivo de la vigilancia. Incluso usando contra-medidas tecnológicas para detectar aparatos o tecnología de vigilancia no garantiza la seguridad. Nuestro enemigo tiene lejos mejores recursos tecnológicos, incluyendo acceso a facilidades de las telecomunicaciones, corporaciones, etc. Esto determina nuestros propósitos de seguridad contra la vigilancia técnica.

Uno de los propósitos de la vigilancia física es facilitar a los agentes de la inteligencia policial planes para poder irrumpir en orden de colocar los aparatos técnicos. Equipos especializados de entrada pueden primero irrumpir en la residencia, lugar de trabajo, o vehículo y fotografiar las paredes interiores, fisuras, capas, objetos, etc. Con esto determinan las mejores locaciones y tipos de aparato para ser usados. Luego se van, preparan los aparatos, y regresan.

En muchos casos, no hay señales obvias de irrupción y nada es tomado. Si es que hay perros dentro de la casa, estos pueden actuar raro debido a aparatos ultra-sónicos usados para cubrir las irrupciones de la policía. En otros casos, robos pueden ser escenificados. Equipos de reparadores del teléfono, la TV, eléctricos, o plomeros pueden ser usados para ganar acceso. Un cooperador arrendatario puede proveer llaves. Las redadas y allanamientos son también buenos momentos para que los aparatos sean puestos en su lugar. Objetos decomisados por la policía durante redadas, tales como computadores, reproductores de VCR, etc. y luego devueltos pueden tener aparatos instalados. Los mismo es cierto para vehículos impounded durante la noche o regalos inesperados como estéreos o TVs (caballos de troya). Un posible indicador de vigilancia electrónica (bichos o cámaras trasmitiendo) son irregularidades en la

radio, TV o conexiones de celulares.
Antes de la tecnología digital, los pinchazos de teléfono eran torpes y a menudo resultaban en sonidos crujientes, volúmenes bajos, etc. Hoy, el pinchazo de un teléfono puede ser echo eficientemente sin sonidos delatores.
La búsqueda de aparatos técnicos debe ser conducida los más discretamente posible, llevándola a cabo mientras se pretende hacer el aseo, etc. En algunos casos, sospechosos han sido allanados luego de haber encontrado aparatos de escucha en sus residencias o vehículos. La búsqueda debe hacerse sistemática y planeada, desde el techo hasta el piso, incluyendo todos los objetos, aparatos, interruptores de luz, enchufes, arreglos en la luz, tomas de aire, detectores de humo, etc. en cada habitación. En las superficies de las paredes, pequeños trozos de diferente color, diferencias en la textura, o pequeñas hendiduras, pueden ser detectadas. Usando pequeños destellos de flash para enfocar áreas de reducido tamaño ayuda en la observación. Todos los artículos electrónicos deben ser desmantelados e inspeccionados, todos los cuadros y espejos movidos. Las alfombras y las cortinas deben ser revisadas, al igual que las plantas, los muebles, escritorios, etc.
Aparatos de escucha o mini-cámaras pueden ser introducidas en una locación como "caballos de Troya", escondidas en regalos como relojes, radios, reproductores de CD, televisores miniaturas, etc.
La búsqueda en vehículos debe ser llevada a cabo luego de un lavado de auto. Estaciona el vehículo en un lugar discreto (por ejemplo un garaje) e inspeccionar debajo del auto por aparatos pegados a través de imanes. Mira dentro del maletero y el motor. También en el interior, incluyendo techo, paneles de las puertas, tablero, espejos, asientos, en búsqueda de aparatos.
Aparatos de escucha que funcionen con radio frecuencias pueden ser detectados a través de monitores RF. Si es que radios, televisores, o teléfonos empiezan a tomar frecuencias distintas, tener estática, o comportarse extraño, podría ser un indicador de estar vigilado.
Si es que aparatos técnicos son encontrados, es una confirmación clara de la vigilancia. Lo que se hace con esta información dependerá de la situación. Los aparatos pueden ser dejados en su lugar, ya que removiéndolos pueden promover una redada de la policía en orden de buscar el aparato y/o remplazarlos por aparatos más sofisticados. Puedes proveer información falsa. O en el último momento, cambiar a otro vehículo los aparatos de rastreo, etc.

Seguridad contra la vigilancia técnica

En espacios cerrados como habitaciones o vehículos conocidos por la inteligencia policial, o cualquier medio de telecomunicación, es casi imposible asegurarse contra la vigilancia técnica. Cuando información protegida o actividades deben ser discutidas, **evita todos los espacios cerrados** asociados con uno u otros miembros del movimiento, y **evita usar las telecomunicaciones.** La mejor forma de comunicarse es cara a cara.

La regla es: **contra la alta tecnología, usa la baja tecnología (o no uses tecnología).** No trates de sobrepasar la vigilancia técnica usando medios técnicos.

Telecomunicaciones

Asume que todas las telecomunicaciones son vulnerables a la vigilancia y evita discutir información protegida o actividades por teléfono, internet, etc. Desde que las operaciones de contra-insurgencia están basadas en todas las fuentes, evita discutir información personal por teléfono e internet, incluyendo rumores, cahuines, o detalles privados de vidas individuales. Usa códigos de palabras y nombres pre-arreglados si es que es necesario usar las telecomunicaciones.

Celulares

Los celulares pueden ser usados como dispositivos de rastreo y escucha y no deben ser llevados con uno durante ninguna actividad secreta o cuando se discuten materias sensibles. Las baterías deben ser removidas.

Computadores e Internet

Las siguientes recomendaciones básicas son de A Practical Security Handbook for Activist & Campaign (Un Manual Práctico de Seguridad para Activistas y Campañas), publicada por la resistencia en el Reino Unido (www.ActivistSecurity.org). Sobre todo, sin embargo, todas las telecomunicaciones deben ser consideradas formas inseguras de comunicarse.

Seguridad del Computador

1. Instala y regularmente actualiza programas de anti-virus y firewall. Programas gratis tales como AVG (www.grisoft.com) y ZoneAlarm (www.zonealarm.com) están disponibles para Windows. El asunto importante es que actives las actualizaciones automáticas para que siempre tengas la última versión.

2. Instala un detector de programas espías como el Ad-Aware

que se encuentra gratis en www.lavasoft.de

3. Borrar archivos no significa removerlos del disco duro, etc. En orden de hacer esto es necesarios limpiarlo apropiadamente, usando un programa dedicado para eso. Algunas recomendaciones son el Clean Disk Security y el PGP.

4. Encripta cualquier archivo sensible en tu computador, CD, o diskette usando un programa como el PGP (o GPG). Idealmente, pondrás todos los archivos en un archivo más grande (usando WinZip o StuffIt) y lo encriptas. Esto significa que incluso los nombres de los archivos estarán escondidos. Limpia los archivos originales. Esto debe ser cada noche cuando termines de usar tu computador, Alternativamente usa la encriptación de discos.

5. Escoge contraseñas que sean efectivas – mayores a 16 caracteres, incluyendo mayúsculas y minúsculas, números y símbolos si es que se permiten. Contraseñas débiles son rotas con facilidad. Las contraseñas para proteger computadores no son seguras para los infiltradores preparados por lo tanto la encriptación de cualquier archivo sensible es necesaria.

- Las contraseñas deben ser cambiadas regularmente
- No las escribas y las pegues debajo de tu silla o escritorio – este es el primer lugar donde los espías buscan.
- No las hagas basados en nombres de la familia, mascotas o fechas de nacimiento
- No uses palabras simplemente del diccionario.

6. Respalda tu computador por si lo roban, pero guarda los respaldos en algún lugar seguro.

7. Considera cambiar tu sistema operativo Windows por otros sistemas como Linux o Mac.

8. Evita los teclados inalámbricos ya que pueden trasmitir a distancia al igual que a tu computador.

9. Mantén la información sensible/importante y las llaves PGP en aparatos removibles como tarjetas de memoria o pendrives.

Privacidad en Internet

1. Los Emails no son seguros, y son monitoreados con facilidad. Para mantenerlos privados, usa la encriptación PGP (www.pgpi.com). No digas nada en un mail que no tengas preparado para justificarlo en una corte.

Si es que quieres contactarte con una persona sin que ellos sepan quién es tu contacto prepara cuentas de mail falsas...y usa estas en vez

de las otras. Considera usar el sistema de botar emails (no mandes los mails, guárdalos como borradores – te comunicaras con otros a través de los borradores dejados en el mail).

2. Mantente atento de los spam – mail no solicitados, incluso si lucen genuinos, como de un banco. Nunca compres nada, o cliquees en los enlaces a páginas web contenidos en mail no solicitados.

3. Cada vez que accedes a internet dejas un rastro que puede ser usado para llegar a ti. Si es que visitas una página web que no quieres que la gente sepa que estas interesado, usa un programa de anonimato para la web o un cibercafé. Si sospechas que estas siendo monitoreado, no hagas nada sensible desde el computador de tu casa. Cuídate de las cámaras CCTV en los cibercafés por lo tanto elije los pequeños y obscuros (o usa un disfraz)

Aparatos de escucha/Mini-Cámaras

Para protegerte contra la entrada y colocación de aparatos en una residencia o vehículo, usa medidas estándar antirrobo. Esto incluye buenas y fuertes cerraduras y candados en puertas y ventanas, alarmas, cámaras de vigilancia, y perros. Los vehículos pueden ser estacionados en garajes seguros con sistemas de alarma. Ninguna de estas medidas garantiza seguridad contra entradas encubiertas, sin embargo.

Pandillas de motoqueros comenzaron a usar scanners en sus residencias y clubes para detectar trasmisores escondidos en infiltrados o informantes. En respuesta, la policía creo grabadoras con formas de bíper e interruptores de on/off por lo que sí se sabe que usaran un scanner el aparato puede ser apagado.

Los motoqueros también compraron e instalaron sistemas de cámaras CCTV es sus residencias, laboratorios de droga, y clubes, para monitorear entradas escondidas o a la fuerza. Grabadoras escondidas que se activan con la voz son también usadas en un esfuerzo por identificar entradas a escondidas.

Para perturbar la vigilancia policial, las pandillas de motoqueros tienen entradas vigiladas y patrullas por lo menos a 4 cuadras a la redonda del punto de encuentro (club, casa, etc.). Esto obliga a los operadores encubiertos a retroceder y encontrar áreas seguras desde donde puedan recibir las trasmisiones. Otra técnica es encontrarse en una locación (un punto rendezvous) y luego ir a otra, solo conocida para algunos seleccionados, esto ofrece un buen terreno contra la vigilancia. En un caso, los motoqueros se juntaron en un área rural cerca del aeropuerto, limitando el uso de un avión pequeño usado

como recibidor de respaldo.
Para neutralizar aparatos de escucha, los motoqueros empezaron a usar dry-erease o chalk-boards para escribir información secreta y después borrarla. Escribir notas en un pedazo de papel contra una superficie plana (para evitar impresiones) y luego destruirlo es una variante de esta técnica.
Para evitar aparatos de escucha (micrófonos parabólicos), conduce conversaciones secretas mientras caminas por áreas cerradas o con mucha interferencia.
Usando códigos de palabras o números pre arregladas para evitar referirse a cierta información.
Código: letra-numero. Escoge una palabra de 10 letras en donde no se repita ninguna letra y asígnale un número a cada letra:
J A M E S B R O W N
1 2 3 4 5 6 7 8 9 0
Ejemplo: WRNE-WBNA = 974-9602
Código en el teléfono: El cantante negro

Aparatos Rastreadores

Para contrarrestar el uso de aparatos rastreadores, no uses tu vehículo personal para ninguna actividad secreta. Los modelos de autos más nuevos vienen con rastreadores GPS integrados, como los On-Star. Muchas compañías que arriendan autos están instalando aparatos GPS para rastrear sus autos. Es posible también que la policía instale un rastreador GPS en una bicicleta. Cualquier vehículo usado para burlar la vigilancia debe ser "frio"- sin ninguna ligazón contigo o cualquier compañero.

Rastreador GPS WorldTracker, disponible en el mercado.

Vigilancia Aérea y Visión Nocturna

Para evadir la vigilancia aérea ve dentro de malls, edificios de apartamentos, estaciones de transito, o cualquier edificio que tenga múltiples salidas y grandes multitudes. Cámbiate la chaqueta y el gorro si es posible. Para evadir la vigilancia aérea de noche (visión nocturna/termal) en una área urbana o suburbana, ve dentro de edificios grandes, bajo puentes de concreto, debajo de vehículos, dentro de sistemas de alcantarillas o túneles, etc.
En áreas rurales ve debajo de puentes, tuberías de drenaje, bajo el

agua, cuevas, bosques espesos, túneles, etc. para evadir vehículos aéreos en la noche.

Un peligro al esconderse en posiciones fijas es que si estas siendo ya monitoreado por la vigilancia aérea ellos verán esto y dirigirán las unidades de tierra a tu locación. Puedes no enterarte que estas siendo observado ya que la vigilancia aérea está siendo conducida en una altitud más allá de tu rango de escucha.

Algunas medidas reportadas para usar en contra de las imágenes infra-rojas y termales incluyen el uso de "mantas de supervivencia", una manta de aluminio que atrapa el calor del cuerpo (y reduce las señales térmicas) y sumergirse bajo el agua (que también reduce las señales térmicas).

8. Vigilancia y Evasión

Acciones contra la vigilancia son usualmente usadas en orden de evadir la inteligencia policial mientras se llevan a cabo actividades secretas.

Para prepararse en la contra-vigilancia, un individuo objetivo debe tomar en cuenta sus patrones de movimiento y actividades sobre el periodo de tiempo previo. Esto identifica posibles tiempos, locaciones, o métodos con los cuales evadir la vigilancia. Lugo de un largo tiempo vigilando, los operadores pueden caer ellos mismo como víctimas de esta rutina y convertirse vulnerables para acciones de contra-vigilancia.

La meta principal de la contra-vigilancia es evadir a los agentes de inteligencia de la policía. Si se es capaz de escapar al stakeout o caja de vigilancia inicial, por ejemplo, el objetivo derrota la vigilancia y se puede mover sin la amenaza de ser observado. Las técnicas usadas para detectar la vigilancia, como las vueltas en u, ir y devolverse, esquinas ciegas, etc., también pueden ser usadas y construidas para evadir la vigilancia.

Evadir stakeouts o cajas de vigilancia se puede hacer desde cualquier locación no necesariamente de nuestra residencia. Locaciones públicas con múltiples e incluso escondidas salidas pueden ser usadas. El transito público puede ser utilizado para quebrar equipos de vigilancia dirigiéndolos a una locación más cómoda, etc.

Los Disfraces pueden ser de gran ayuda para acciones de contra-vigilancia. Los operadores deben reconocer al objetivo para poder seguirlo/la. Aunque las características faciales son la mejor forma de reconocer a un individuo en específico, los operadores también se fijan en la contextura corporal, la vestimenta y los gestos. La apariencia

física de uno puede ser alterada de muchas maneras:

- Ropa ancha o suelta pueden alterar la forma. llenándola uno se puede ver más ancho y grande.
- Cambiando el estilo de la ropa y los colores.
- Cambiando la postura y forma de caminar.
- Usando pelucas o maquillaje de teatro.

Si es el uso de un disfraz es detectado, los operadores de la vigilancia asumirán que el objetivo está tratando de evadir sus esfuerzos y está preparando algún tipo de actividad protegida.

Gran cuidado y mucho planeamiento debe ser puesto en cualquier accione de contra-vigilancia, y los disfraces deben ser efectivos. Las consideraciones también tienen que tener en cuenta cambiarse los zapatos.

En un ambiente urbano, las acciones de contra-vigilancia llevadas a cabo a pie tienen más chances de ser efectivas que aquellas hechas en vehículo. Hay áreas limitadas donde un vehículo puede viajar (calles, autopistas, callejones, garajes, etc.). Además, pueden tener algún aparato de rastreo atado a la carrocería, así que no importa cuántas curvas o vueltas en u sean usadas, los operadores aun sabrán donde está el vehículo.

En contraste, los viajes a pie casi no tienen límites. Los objetivos que se mueven a pie pueden explotar el terreno y las rutas de viaje para quebrar o eludir a los equipos de vigilancia. El transporte público, especialmente los metros, son difíciles de seguir para los operadores, debido a las altas velocidades, la habilidad para cambiar de dirección, múltiples salidas de las estaciones, etc. Las locaciones públicas como malls, complejos de oficinas, etc., también son locaciones difíciles dada las múltiples salidas, diferentes niveles de piso, elevadores, escaleras, etc. En una emergencia (como una alarma de incendios) los operadores tienen aun más dificultades de seguir a un objetivo.

Evadir la vigilancia siempre es más fácil de noche o con mal clima (como una tormenta), en orden de limitar la visibilidad.

En una ambiente urbano, y en una locación publica, es a menudo que los movimientos más ilógicos son los que pueden identificar operadores o limitar su capacidad de seguimiento (lo que también puede alertar a los operadores que se está haciendo algún tipo de acción anti-vigilancia). Tomar un elevador y subir un piso y luego bajar es ilógico, cualquier otra persona que lo haga será muy sospechosa. Esperar en las paradas de buses o en la estaciones del metro mientras pasan puede forzar a los operadores a abordar alguno de estos, o

arriesgarse a la exposición. Tomar un bus o un metro hasta el final de la línea y luego regresarse puede también identificar a potenciales operadores. Subiéndose o bajándose del trasporte público repetidas veces puede a la larga romper equipos de vigilancia.

9. Informantes e Infiltrados

Los informantes e infiltrados son espías que recopilan información de la resistencia y se la proveen al enemigo. También pueden tomar un papel más activo. Estos actos pueden resultar en capturas, arrestos, aprisionamientos y muertes. El término colaborador es usado para cualquier miembro o ciudadano que adhiera a asistir a nuestro enemigo.

Los informantes e infiltrados proveen única y especial inteligencia humana (como estados emocionales, planes, intenciones, etc.) que no pueden ser recopiladas de ninguna otra forma. En adición, los infiltrados y colaboradores pueden físicamente perturbar o sabotear actividades del movimiento. Pueden difundir desinformaciones o mitos maliciosos, creando división y paranoia. También pueden granar declaraciones o acciones incriminatorias. Pero por sobre todo, son una parte esencial y elemento activo en las operaciones de contra-insurgencia como también las investigaciones criminales.

Los Informantes son persona reclutadas por las fuerzas de seguridad estatales para proveer información. Ellos son civiles, usualmente amigos o asociados del grupo objetivo. Pueden ser camaradas amargados que se sienten ofendidos o incluso traicionados por el grupo. O, pueden ser miembros genuinos arrestados y sometidos bajo presión. La policía se refiere a estos como "Informantes Confidenciales" o "Fuentes Confidenciales.

Un método estándar para reclutar informantes es encontrar personas (dentro o cerca del grupo) con problemas. Las personas más vulnerables para convertirse en informantes son aquellos que buscan protección, que buscan venganza, drogadictos, alcohólicos, aquellos que sufren de algún trauma o deficiencia mental, aquellos que enfrentan largas sentencias en prisión y aquellos en situaciones comprometedoras (chantaje). La intimidación y coerción pueden ser usadas también para convertir a una persona en informante. El dinero puede ser un factor motivador en hacer que una persona se vuelva informante, y mantener sus servicios en un extendido periodo de tiempo.

Potenciales informantes también pueden ser identificados por la

vigilancia. Relaciones personales, problemas con dinero o drogas, actividades sexuales, conflictos de personalidad, luchas de poder internas, etc., son todas analizadas en orden de encontrar alguna apertura por donde adherir presión sobre un potencial informante.
Miembros del movimiento que son arrestados y sujetos a presión pueden quebrarse y colaborar con la policía. En algunos casos, esto puede resultar con el poco compromiso en la lucha. Es importante que los miembros no sean presionados, cohesionados, o intimidados para realizar una acción, si no que lo hagan por una fuerte creencia de lo que se está haciendo. Estudios han demostrado que los que más se resisten a la tortura son motivados por sus creencias, no por el interés económico personal o prestigio social, por ejemplo.
Una vez que la persona se convierte en informante, es enormemente dependiente de sus "manejadores" de la inteligencia policial para su protección, habiendo traicionado a sus amigos y compañeros. Los informantes pueden ser miembros con un perfil bajo o asociados que silenciosamente recopilan información y observan, mientras otros pueden ser animados para convertirse en más activos por sus manejadores, actuando como agentes provocadores (un informante o agente que provoca a la acción, usualmente ilegal la que guía a un arresto).
Los infiltrados son civiles reclutados por las fuerzas de seguridad estatales (o corporaciones), o agentes de la inteligencia policial. Se insertan ellos mismos en grupos posando como genuinos miembros de la resistencia, en mayor o menor grado. Pueden ser de cualquier raza o etnia, tamaño o forma, etc. (dependiendo del grupo objetivo obviamente). Informantes de la policía han probado en ocasiones ser bastante adeptos a interpretar su rol, observando y actuando como uno más (como los investigadores encubiertos en las pandillas de motoqueros).
Los infiltrados pueden ser de largo término y adentrarse mucho en un grupo, formando amistades íntimas, teniendo una función general en recopilar información o como parte de una investigación criminal. O pueden ser temporalmente operativos quizás con una meta específica (como neutralizar a los "lideres" o grupos). Algunos infiltrados son también referidos como agentes provocadores por su rol protagónico en instigar actividades (a menudo ilegales).
Los infiltrados usualmente se desarrollan sobre un periodo de tiempo, en el cual conocen y se compenetran (en relación amistosa) como miembros del grupo objetivo. Esto puede comenzar con encuentros

fortuitos, intereses compartidos, en mítines, eventos, marchas, etc. Todos esto, obviamente, son resultado de una extensa vigilancia y perfil sicológico (saben cuando y donde estar y como actuar). Un método común es que un informante se introduce para infiltrar al grupo. Los infiltrados pueden ser amigos de un miembro en orden de ganar contacto con todo el grupo. Los infiltrados pueden entrar como genuinos miembros de otras áreas o regiones, donde primero hicieron contacto con el movimiento. Pueden decir conocer a ciertas personas o haber estado en ciertos lugares y eventos, en un esfuerzo de establecer credibilidad. Una cubierta usada para grupos de radicales es la del estudiante, de hecho, las universidades son terreno para reclutamiento de agentes de inteligencia en general.
En algunos casos, a los infiltrados que les proveen recursos, incluido dinero, vehículos, armas o información – cosas que son de gran valor y elevan su perfil e influencia en el grupo. También pueden entrar en confianza con los "lideres" o asumir "liderazgo" y posiciones de seguridad en orden de extender su influencia y acceso a la información (ver más abajo Técnicas del FBI COINTEL-PRO).

Notas sacadas de "Security Culture: A Handbook for Activists" (Cultura de Seguridad: Un Cuadernillo para Activistas) Edición de Nov. 2001:

Tipos de informantes

- El tipo "aparecido": son personas que regularmente aparecen en mítines y acciones pero generalmente no se involucran. Ellos recolectan documentos, escuchan conversaciones y anotan quien es quien. Este rol de observación es relativamente inactivo.

- El tipo "dormilón": tiene un modus operandi parecido al "aparecido", excepto que su absorción de información es usada para activar su rol más adelante.

- El tipo "novato": poseen un rol un poco más activo, pero se confinan a sí mismos a los trabajos menos prominentes. Ellos no toman la iniciativa, pero el trabajo que hacen es valorado. Esto les ayuda a construir confianza y credibilidad.

- El tipo "súper activista": aparecen de la nada, muy de repente y están en todos lados. Sea esto un mitin, protesta, o acción, esta persona siempre aparecerá en ellas. Ten en mente que esto puede

ser la marca de un nuevo activista, aquellos que son entusiastas y comprometidos y quieren combatir al poder a cada minuto.
"Se dice que con varios de estos modus operandi, el comportamiento es difícil de distinguir con personas que se están recién involucrando. ¿Cómo los distinguiremos? Bueno, un infiltrado preguntara un montón de preguntas acerca de los grupos de acción directa, individuos y actividades ilegales. Él/Ella puede sugerir objetivos o reconocerse y participar como un miembro más de la acción. Los infiltrados también tratan de construir perfiles de individuos, sus creencias, hábitos, amigos, y debilidades. Al mismo tiempo, los infiltrados escudaran su verdadero yo de otros activistas."
"Cualquiera que pregunte un montón de preguntas sobre acciones directas no es necesariamente un infiltrado, pero hay ALGUNOS con los que se tiene que tener cuidado. Por lo menos, ellos necesitan estar informados de las materias de seguridad. Activistas nuevos deben entender que las acciones directas pueden ser riesgosas (¡por lo cual algún riesgo habrá que tomar!) y que hacer demasiadas preguntas poner en peligro a personas. Si la persona persiste en hacer preguntas, hay un problema y medidas apropiadas deben ser tomadas. Activistas que nos puedan entender la necesidad de la seguridad deben ser apartados de situaciones en las que pueda incriminar a otros."

El Infiltrado Encubierto

"Un agente fuertemente adentrado está equipado con un carnet falso (usualmente manteniendo el primer nombre para que él/ella no se le olvide responder a su nombre), un esqueleto de su historia personal, como también a dueños de negocios que verificaran que han trabajado para ellos (y que luego notificaran a la policía que alguien estuvo preguntando). Los trasfondos de los agentes pueden estar basados en la verdad para evitar algún desliz. Finalmente un agente fuertemente adentrado puede trabajar en un trabajo real, arrendar una casa o departamento, y vivir su rol 24 horas al día."
"Un policía encubierto trabando bajo una cobertura ligera puede también tener un carnet falso, pero es más común que vuelva a casa donde su familia y su vida "real" (usualmente en otra ciudad). A veces oficiales de narcóticos y otros agentes especialmente entrenados serán llamados para estas tareas."
("Ecodefense: A Field Guide to Monekywrenching" [Ecodenfensa: Una guía de campo para el sabotaje], Foreman and Haywood, Abzzug Press, Chico CA 1996, p.296).

Reuniones Entre Informantes y Controladores

Como una parte de las operaciones encubiertas, el Infiltrado/ Informante deben intercambiar información, equipamiento o dinero con sus "controladores". El método más seguro es en reuniones frente a frente. El FBI, por ejemplo, ah habilitado departamentos para que informante y controlador se reúnan, como una "entrega muerta" para dejar mensajes, grabaciones, etc., y como una casa de seguridad donde dormir. En otras ocasiones el controlador y el informante se encuentran en estacionamientos o entrando al auto del otro:

"Para mantener la seguridad, Tait (un informante de los Hells Angels) y el agente se juntan en lugares secretos...Un agente deberá detenerse en una estacionamiento cubierto y Tait se subirá a su auto. Manejaran a un ciudad diferente para hablar en un motel o lugar público mientras otros dos agentes realizan labores de contra-vigilancia." *(Hells Angel: Into the Abyss, por Yves Lavgne, HarperCollins Publisher Ltd., Toronto 1996, pp. 237-38)*

Cuando se tienen que comunicar por teléfono, uno llamara al bíper del otro y dejara un numero donde lo pueda llamar. Incluso ahí las conversaciones son breves y en código:

"Tait llamo al bíper de McKinley (Controlador del FBI) en Oakland para darle noticias. El nunca llamaba a McKinley a su casa porque los Hells Angels tenían acceso al registro de la compañía de teléfonos...Al igual, McKinley llamaba siempre al bíper de Tait." *(Hells Angels: Into the Abyss, p. 147)*

Lidiando con Informantes e Infiltrados

Al igual que la vigilancia, detectar informantes e infiltrados puede ser dificultoso. Algunos trabajan muy duro en camuflar sus actividades e interpretar el papel de un genuino miembro del movimiento. Intuición, observación, y análisis de las actividades y conductas de una persona pueden ayudar a identificar posibles informantes e infiltrados. Los chequeos de trasfondo deben ser llevados a cabo en personas sospechosas para confirmar su identidad (aunque una operación bien organizada tendrá un respaldo para cualquier identidad falsa del infiltrado). Los grupos pueden organizar sus propias operaciones de vigilancia para aprender más de personas sospechosas.

A menos que allá fuerte evidencia, denuncias y acusaciones públicas pueden hacer más daño que bien. Pueden aparecer paranoias sobrevaluadas, ataques/rivalidades personales, etc., especialmente

si no existe evidencia concreta. En muchos casos, infiltrados bajo sospecha pueden discretamente prevenir involucrarse en actividades críticas (ej. Comunicaciones, fondos, transporte, discusiones tácticas y estratégicas, etc.).
Cuando infiltrados e informantes se ven confrontados, la reacción más común es negar la acusación tajantemente. Ocasionalmente enfatizan todos los riesgos, sacrificios y lealtades que han desplegado. Usan las respuestas emocionales para ganar simpatía de otros miembros del grupo (que pueden no estar advertidos o encontrar inconcebible que la persona sea un informante o un infiltrado).
Si una persona es identificada como un infiltrado o informante (ej. Como resultado de una declaración en la corte, encontrando notas o aparatos de grabación o admitiendo el hecho), se le deberán tomar fotos en orden de avisar a otros. Una declaración en video debe ser obtenida en lo posible. Cualquier material o área en la que se confirme que el infiltrado o informante tuvo acceso debe ser limpiada por el riesgo, cambiar los códigos de seguridad, etc.

Chequeos de Trasfondo

"¿Cuáles son algunas formas de investigar la posibilidad que alguien sea un informante? Primero, a menos que tengas razones concretas o evidencia que alguien es un infiltrado, difundir rumores hará daño al movimiento. Rumores escuchados deberán ser cuestionados y rastrear sus fuentes. El trasfondo de una persona puede ser buscado, especialmente en el activismo que dicen tener participación en otros lugares. ¿Tus contactos en esos lugares conocen a la persona, y su involucramiento? ¿Ha habido algún problema? Una importante ventaja de tener enlaces con lugares lejanos, es dificultar la fabricación de actividades de los informantes.

"¿Cuales son las formas de vida de una persona? ¿Quiénes son sus amigos? ¿Cuáles son las contradicciones entre su discurso y su forma de vida?" *(De Security Culture: A Handbook for Activists)*
En una operación encubierta de la ATF en contra de los Hells Angels (Operación Black Biscuit), el agente que estaba bien respaldado con una identificación falsa y una historia que la contrainteligencia de los motociclistas, que involucraba un extensivo chequeo de trasfondo, fallo en encubrir su real identidad. Investigadores privados contratados por los motociclistas, sumándole otras fuentes de inteligencia, solo reafirmaron la identidad falsa del agente, y proporcionaron una falsa sensación de seguridad en la banda.

10. FBI COINTEL-PRO

Campaña de Contra-Insurgencia Domestica (1960s – 70s)

El tristemente célebre Programa de Contra-Inteligencia del FBI (COINTEL-PRO) debe servir como un escalofriante recuerdo de lo lejos que el enemigo puede ir a favor de destruir nuestra resistencia. Esto es especialmente verdadero desde que veteranos de esos tiempos están aun con vida, y muchos permanecen en prisión hasta el día de hoy como resultado (ej. Leonard Peltier, Mumia Abu-Jamal, etc.). A la vez muchos están muertos, asesinados por la policía, y paramilitares durante los 1960's y 70´s. Nuestra falla en aprender de esos tiempos no solamente nos dejaría vulnerables a las mismas tácticas, además seria una deshonra a los sacrificios hechos por las anteriores generaciones

COINTEL-PRO tiene sus raíces en la campaña anti-comunista de los años 50 (cuando comenzó la Guerra Fría). Sus primeros objetivos fueron grupos comunistas y socialistas, al igual que los movimientos por los derechos civiles afroamericanos. En los años 60, nuevos movimientos de liberación emergieron alrededor del mundo. EEUU se involucro en Vietnam y la fiera resistencia hecha por el pueblo vietnamita contribuyo a un clima de insurgencia y rebelión, la que se extendió dentro del mismo EEUU.

Para estos tiempos, COINTEL-PRO fue expandida alrededor de la nación, involucrando extensa vigilancia, informantes, colaboradores, asaltos, cargos falsos, encarcelamientos, fabricación de comunicaciones, campañas de rumores y desinformación, robos, vandalismo, incendios intencionales, al igual que fuerza letal. Muchos organizadores claves fueron asesinados, y muchos aun siguen en prisión. Entre los golpes más fuertes se encuentran a los Panteras Negras y el Movimiento de Indios Americanos, al igual que a los Chicanos, y Puertoricenses, los movimientos anti-guerra también fueron objetivos.

La meta de esta campaña de contra-insurgencia era la de destruir los movimientos de resistencia organizados, usando cualquier medio necesario. Uno de sus mayores enfoques fue el de instalar una sensación de ***paranoia y miedo*** entre los movimientos, en orden de neutralizarlos. Aquellos que se rehusaron a someterse fueron objetivo de métodos aun más duros, y algunos asesinados. Asaltos violentos y muertes contribuyeron en aumentar la paranoia y la inseguridad. Explotando divisiones internas en momentos de una intensa represión, el FBI y la policía fueron exitosos en neutralizar esta primera fase de resistencia en Norte América (aunque no pudieron matar el espíritu).

COINTEL-PRO fue expuesto cuando personas desconocidas irrumpieron en los archivos del FBI, en las oficinas de Pennsylvania en 1971. Declaraciones y promesas gubernamentales dieron la impresión de que COINTEL-PRO había terminado; sin embargo, la represión domestica continuo a través de los años 70's, 80's y 90's. Hoy, nuevas leyes anti-terroristas como la PATRIOTIC ACT legitimizaron mucho de lo que ocurrió bajo COINTEL-PRO y han incluso extendido los poderes del FBI, la policía y de las agencias de inteligencia.

En Canadá, la RCMP ah sido unos de los mejores estudiantes del FBI, sirviendo como algo similar a la policía nacional con un rol de "policía política" al igual que fuerza temprana para colonizar. En los años 70's la RCPM fue expuesta en llevar a cabo actividades ilegales en contra de grupos disidentes, esto incluía, pillaje, vandalismo, robos, e incendios intencionales. Durante 1995 en Ts'Peten (Lago Gustafen, BC) la RCPM fabrico incidentes con tiroteos y uso fuerza letal en acuerdo de establecer zonas de "no disparo". Un oficial relacionado con la RCPM fue capturado en un video diciendo: "Las campañas de SMEAR son nuestra especialidad".

Técnicas de COINTEL-PRO:

1. Vigilancia

Extensiva y ampliamente abierta vigilancia fue usada para obtener información de grupos e individuos, con ambas técnicas, técnica (bichos, teléfonos, correo, fotos y video) y física (personas y vehículos). Esta información a menudo forma las bases para operaciones complejas de COINTEL-PRO. El FBI y las agencias policiales locales, junto con otras agencias de la ley, estuvieron involucradas. La vigilancia en si fue a menudo usada para inducir paranoia y miedo. (Siendo los vigilantes obvios y beligerantes).

2. Infiltrados, informantes y colaboradores

El uso ampliamente esparcido de infiltrados e informantes fue clave en la campaña del FBI, COINTEL-PRO. Informantes, usualmente miembros poco afectivos o asociados a grupos, fueron reclutados a través de la intimidación y/o dinero. Ellos proveían inteligencia humana crítica. En el caso de infiltrados y colaboradores, también activamente irrumpían en organizaciones para que el FBI/policía llevara a cabo asaltos mortales, montajes, etc.

Infiltrados incluidos agentes del FBI, policías encubiertos, y civiles. En algunos departamentos de policía, "escuadrones rojos" trabajaron junto a unidades anti-pandillas para prevenir uniones entre pandillas

y movimientos de resistencia. También reclutaron infiltrados de las pandillas que enfrentaban la cárcel o por dinero.

Infiltrados fueron a menudo capaces de proveer información y recursos (vía FBI/manejadores de la policía) al grupo. Debido a su experiencia con armas y violencia, fueron a menudos promovidos a posiciones más elevadas en sus organizaciones, con algunos dejados a cargo de la seguridad en algunos capítulos o lideres.

¿Cómo es que los movimientos fueron tan fuertemente infiltrados?

Eran totalmente abiertos y organizaciones públicas. Los infiltrados fueron fáciles de colocar. La única área en la que fueron tomadas las medidas de seguridad fue al nivel de los liderazgos, y es aquí donde fueron hechos los peores errores.

En ambas Las Panteras Negras y AIM, los infiltrados lograron acceso al círculo interno, frecuentemente en cargos de seguridad para el grupo en sí. Algunos interpretaron el papel del "ultra-militante", promoviendo la violencia o intentando dirigir al grupo hacia acciones ilegales. Criminales/estafadores se convirtieron en infiltrados y fuentes de drogas, armas, y violencia anti-social entre grupos. Otras actividades incluidas plantar evidencia, robar fondos, sabotajes al equipamiento o a los esfuerzos organizados, proveer información que terminan en arrestos o muertes, como al igual que difundir desinformaciones, paranoia y división.

3. Chaqueta-Mala , o Chaqueta-Entrometida

Cuando un miembro genuino del movimiento es retratado de ser un informante (o ladrón, violador, etc.). A menudo, otros informantes son usados para esparcir rumores, plantar evidencia, etc. En su esfuerzo de colocar chaquetas-malas, los policías frecuentemente arrestan objetivos en las redadas, pero rápidamente a uno/a o algunos/as los/las dejan ir (mientras otros siguen en prisión). La policía misma puede crear chismes o dejar evidencia indicando a una persona como informante.

El propósito de una chaqueta-mala es neutralizar objetivos individuales como a un organizador efectivo. Los resultados de esta técnica terminan en interrogatorios, asaltos, e incluso en ejecuciones de sospechosos de ser informantes (como ocurrió entre Las Panteras Negras).

4. Comunicaciones Falsas

Cartas falsas fueron envidas entre individuos o grupos con información ficticia (ej. alegatos de aventuras sexuales entre miembros, amenazas de muerte, etc.). Cuando existieron hostilidades entre grupos, estas fueron explotadas hasta el punto de propiciar asaltos e incluso

muertes.
Otro ejemplo de comunicaciones falsas fue el de producir falsos periódicos, afiches, etc. hechas por el FBI/policía, y distribuidos como publicaciones genuinas del movimiento. Esta técnica fue efectiva en para recortar el presupuesto para el programa de desayunos de las Panteras luego de que comics ofensivos fueran enviados a los fundadores.

5. Desinformación Mediática

En colaboración con las corporaciones mediáticas, el FBI y la policía pudieron conducir campañas de "difamación y desinformación" en contra de movimientos, organizaciones, e individuos, retratándolos como violentos, criminales, terroristas, o locos.

6. Arrestos/evidencia falsa/montajes

Cargos insignificantes y montajes descarados fueron usados para atar a personas o grupos al sistema judicial, y para aprisionar a muchos con duras sentencias. Constantes o masivos arrestos drenaron el tiempo y los recursos del movimiento, divirtiéndolos desde la resistencia de la defensa legal. El aprisionamiento sirvió para neutralizar organizadores espantando así a los menos comprometidos. Varios prisioneros políticos y POWs permanecen en las prisiones de EEUU hasta el día de hoy, los aprisionados en los 70's como resultado de COINTEL-PRO. Arrestos y aprisionamientos también sirvieron para criminalizar movimientos y grupos.

7. Otros Acosos

Otras formas de acosos usados por el FBI y la policía incluyendo el acercamiento a arrendatarios, empleadores o familiares para sumar presión a los miembros (ej. teniéndolos desahuciados, perdiendo sus empleos, o enfrentando el ostracismo hecho por la familia). Agentes incluso lograron cancelar reservaciones hechas por un grupo organizado, o anunciar que los mítines, marchas, etc. fueron cancelados.

8. Robo, Vandalismo e Incendios Intencionales

El FBI y la policía local rutinariamente irrumpieron en oficinas y hogares en orden de robar documentos, copiarlos, y/o para destruir equipamiento. Oficinas también fueron incendiadas, destruyendo recursos valiosos como una imprenta, documentos, archivos, etc.

9. Seudo-Pandillas

Grupos falsos colocados por agentes de la inteligencia policial para desacreditar al movimiento y entrampar a genuinos miembros del movimiento. En los 60's y 70's, el FBI coloco muchas seudo-pandillas para irrumpir en campañas (ej. entre puertoricences Independentistas,

grupos contra la guerra, etc.)

10. Fuerza Letal

Organizadores claves fueron asesinados por la policía durante redadas y asaltos, hechos por vigilantes (incluyendo racistas de derecha), hechos por el FBI-policía infiltrado, o como resultados de un "chaqueteo-malo". Muchos fueron muertos durante los 50's, 60's y 70's, incluyendo:

- Fred Hampton y Mark Clark (Panteras Negras) fueron ambos asesinados en una redada policial en su casa de Chicago, en 1969.
- Alpretice Carter y Jon Huggins (Panteras Negras) fueron asesinados en 1969 por miembros de un grupo rival, todo esto instigado por el COINTEL-PRO.
- George Jackson, un prisionero y prominente Pantera Negra, fue asesinado durante un presunto intento de fuga en 1971
- Fred Bennett, un SF Pantera Negra, fue ejecutado por compañeros luego de ser efectivamente "chaquetado-malo" por un infiltrado del FBI, en 1969. Uno de los Panteras involucrado en esto, Jimmie Carr, fue el mismo "chaqueteado-malo" y ejecutado por otras Panteras en 1972 (¡!).

11. Asistiendo a Escuadrones Paramilitares de la Muerte

En la reservación de Pine Ridge en Dakota del sur, por lo menos 67 miembros o asociados de AIM fueron asesinados por policía BIA, FBI, y fuerzas paramilitares (los Guardianes de la Nación de Oglala, GOON como se referían a sí mismos) desde 1973-76. Los GOON, empleados por un corrupto y tribal presidente, estaban armados, equipados, y financiados por el FBI como parte de su esfuerzo contra-insurgente contra la resistencia Indígena. Ellos llevaron a cabo un reino del terror en contra de AIM y tradicionalistas de la reserva, incluyendo bombas molotov, asaltos, tiroteos desde autos en movimiento y muertes.

Otros ejemplos del uso de grupos paramilitares y vigilantes incluido la asistencia del FBI a grupos de derecha como los Minutemen, Secret Army Organization, y el Ku Klux Klan. Estos y otros grupos fueron provistos de información, equipamiento y armas para llevar a cabo asaltos y ataques letales. Algunos también fueron enlazados a las unidades de la inteligencia militar de EEUU. Los escuadrones paramilitares de la muerte son comunes al sur del globo.

Casos Estudiados del COINTEL-PRO

Asesinato de Fred Hampton y Mark Clark en 1969

Fred Hampton y Mark Clark fueron miembros de las Panteras Negras, sección Chicago. Hampton era un joven y una promesa de líder, un organizador altamente efectivo el cual había comenzado a realizar alianzas con otros movimientos e incluso con las pandillas en Chicago, incluyendo a los Blackstone Rangers.

En 1968, un infiltrado del FBI llamado William O'neal se unió a la sección. O'neal fue un criminal de poca monta, acusado de robo de autos y robo de identidad al pasar un carnet falso a un agente del FBI. A cambio de deponer los cargos, O'neal acepto infiltrarse a la sección de Chicago. Rápidamente se volvió jefe de seguridad y guardaespaldas de Hampton. Esto basado en su experiencia con armas y violencia.

En orden de detener la alianza entre Panteras y los Blackstone Rangers, fueron enviadas cartas falsas a ambos grupos instigados por O'neal.

William O'neal, Gangster Infiltrado del FBI

O'neal constantemente agitaba para realizar ataques armados y robos, ofreciendo entrenamiento y armas (el "ultra-militante"). El recomendaba conseguir un avión para bombardear la alcaldía, que todas las Panteras estuvieran armadas, y que fuera instalada una silla eléctrica en orden de interrogar/torturar a sospechosos de ser informantes (todas rechazadas). El mismo llevo armas usadas como pretexto para una redada policial en junio de 1969 a las oficinas de las Panteras. Dichas redadas fueron llevadas a cabo nuevamente en julio y octubre de ese año.

O'neal junto con otros infiltrados, también robaron financiamiento para discos, documentos, libros, casetes, películas, etc. en orden de sabotear sus esfuerzos. El FBI también manufacturo comics falsos, los que fueron enviados a los fundadores del programa Breakfast (desayunos). Los comics fueron tan ofensivos que muchos fundadores les retiraron el apoyo.

En noviembre de 1969, el FBI y la policía local comenzaron a planear el asesinato de Hampton. O'neal facilito un detallado plano del apartamento de Hampton, incluyendo su cama y la locación de la cabeza mientras duerme.

El 4 de diciembre del '69, 40 efectivos fuertemente armados allanaron

el apartamento usando una orden para buscar "armas ilegales". Temprano esa misma noche, O'neal había hecho la cena, incluyendo un Kool-Aid alterado con tranquilizantes. A eso de las 4:30am, la policía patio la puerta e inmediatamente disparo contra Mark Clark, el cual estaba sentado en la habitación de entrada y armado con una escopeta (seguridad en contra de una posible redada). Lamentablemente, Clark estaba desmayado por el Kool-Aid de O'Neill.

Luego la policía dirigió sus armas en contra del muro donde estaba la cama de Hampton a la altura de su cabeza. Ambos, Hampton y Clark fueron asesinados, mientras otros fueron heridos. La policía de Chicago declaro que esto fue un "tiroteo salvaje" con fuerte armamento por parte de las Panteras, al contrario el único tiro efectuado por las Panteras fue cuando la escopeta de Clark se disparo como reflejo al ser baleado por la policía. (O'neal fue declarado muerto por suicidio en los '80)

Douglas Durham, 1973-75

Douglas Durham fue un infiltrado no-Indígena en el American Indian Movment (Movimiento de los Indios Americanos), que trabajaba para el FBI. El era un policía formal de Iowa que también había trabajado para la CIA y que tenía alguna experiencia en las Fuerzas Especiales militares. Fue entrenado para demoliciones, sabotajes, robos, etc.

A principios de los '60 estuvo involucrado con el crimen organizado, incluyendo los círculos de la prostitución. Esta actividad llevo a conflictos con su esposa, que murió como resultado de un violento asalto por Durham en julio de 1964. Fue dado de baja en la policía y descrito como un esquizoide violento "que no encajaba para el servicio público".

Durham comenzó nuevamente a trabajar como agente de la inteligencia policial en 1971. Estuvo presente en el sitiamiento de Wounded Knee en 1973, posando como reportero. Luego se unió a la sección de Iowa de la AIM, debido a su cabello negro y a lentes de contacto café. Declaro ser descendiente Chippewa.

Basado en su trasfondo y habilidades, Durham se convirtió en la cabeza de la seguridad nacional de AIM y en guarda espalda de Dennis Banks, uno de los líderes nacionales de AIM. Durante los juicios de Wounded Knee, Durham observo todas las discusiones legales y de estrategia, como también tomo el control de prácticamente toda la administración de AIM a través de su oficina nacional en Minneapolis (incluyendo fondos).

Como otros infiltrados, Durham propuso rabiosos esquemas, incluyendo secuestros de políticos, confrontaciones armadas, etc. Es sospechoso de por lo menos la muerte de una persona- Jacinta Eagle Deer, quien fuese asesinada en abril de 1975. Durham fue la última persona en verla con vida luego de recogerla en la casa de un pariente. Eagle Deer había acusado a William Janklow, en ese entonces abogado general de Dakota del sur (mas tarde fue gobernador), de violación.
En marzo de 1975, abogados que trabajaban en el comité de defensa de Wounded Knee obtuvieron documentos del FBI como parte de un caso los cuales contenían un reporte firmado por Durham. Cuando lo confrontaron, Durham reconoció su rol como un infiltrado federal. Al ser expuesto desmoralizo fuertemente a la AIM, que estaba en ese momento bajo una intensa represión, incluyendo muertes, asaltos, y el aprisionamiento de sus miembros.

Para mas información de estos casos: *"Agents of Repression: the FBI's Secret War against the Black Panther Party" y el "American Indian Movement", de Ward Churchill y Jim Vander wall, South End Press, edicion de 1990.*

11. Casos Estudiados de Informantes e Infiltrados

Infiltrado en el Frente de Liberación de Quebec

En los '60 y principios de los '70 el Frente de Liberación de Quebec (FLQ) llevo a cabo una lucha de guerrilla urbana. Carole de Vault fue una joven activista del Partido Qebecois, un grupo de liberación nacional que compartía una meta similar con el FQL por su independencia. Ella se unió a la lucha del FQL, pero se convirtió en una informante pagada. Su real activismo fue con los reformistas del PQ; ella no estaba de acuerdo con los militantes del FQL ni sus acciones desde que amenazaba el trabajo "legitimo" del PQ. Esto es un ejemplo de una informante que logra infiltrarse en un grupo pero al mismo tiempo es una activista que se convierte en informante.

Arrestos de Germinal, 2001

El arresto del grupo militante "Germinal" en su camino a la protesta contra el Tratado de Libre Comercio de las Américas en la ciudad de Quebec en abril del 2001, fue el final de meses de una larga operación encubierto. El grupo, con sus bases en Montreal, fue el objetivo de

una operación de la policía basada en la vigilancia que indicaba que un miembro del grupo estaba buscando trabajo.

La policía creó una compañía falsa de mudanzas de mueblería completa con oficina y camiones, donde todos sus trabajadores era agente de la policía encubierto, los que pegaron las solicitudes de empleo en el vecindario donde el miembro del grupo residía. El califico, y por varios meses trabajo junto a los agentes de la policía que eventualmente lograron infiltrar el grupo.

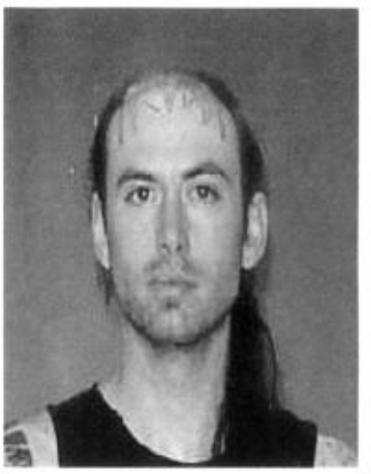
Los arrestos fueron en la víspera de las masivas protestas del 20-22 de abril, y fueron foco de una gran cobertura de los medios la cual la policía uso para justificar su masiva operación de seguridad. Los arrestados fueron capturados con mascaras de gas, granadas de humo, y Thunderflashes (un potente "fuego artificial" usado por los militares como simulador de granadas durante el entrenamiento). A pesar de esto, la policía y los medios los retrataron como un "grupo armado".

Este ejemplo muestra como las policías con un gran presupuesto para operaciones de seguridad mayores pueden invertir cientos de dólares para arrestos de alto-perfil contra militantes de "baja intensidad".

Operación Backfire: Arresto del ELF por el FBI, 2004-2006

En el 2004, el FBI lanzo la Operación Backfire, comenzando siete investigaciones en la oficina de Portland, Oregón. Estos involucraban 16 diferentes ataques llevados a cabo por el Frente de Liberación de la Tierra (ELF) entre 1996-2002 al este de EEUU los que causaron 80 millones de dólares en daños.

En diciembre del 2005 y enero del 2006 el FBI implico a cinco mujeres y seis hombres con un total de 65 cargos, incluyendo incendios intencionales, uso de aparatos destructivos, conspiración, y la destrucción de una estación de energía. Un prisionero se suicido mientras estaba en custodia. Estos arrestos fueron primariamente el resultado de un solo informante: Jacob Ferguson.



Hippy Informante del FBI, Jacob Ferguson

Ferguson participo en algunas acciones del ELF que estaban bajo investigación del FBI proveyendo nombres de otros involucrados. Uso dispositivos de grabación para capturar y luego crear declaraciones incriminatorias de las acciones. Basado en esto, órdenes de cateo

fueron usadas en casa y negocios, donde el FBI confisco computadoras, manuales, identificaciones falsas, ropa, herramientas y otros equipos que fueron puesto bajo investigación forense.
Ferguson fue reportado como un adicto, de larga data a la heroína que comenzó a colaborar con el FBI en el 2004. A pesar de su adicción, al parecer gozaba de la confianza y la confidencia del grupo, que hablo abiertamente con el acerca de acciones ilegales mientras eran secretamente grabados por él.

12. Líneas Guía para la Seguridad

1. **Establece líneas guía de seguridad apropiada para el nivel de actividad del grupo.** La no colaboración con la policía o las agencias de inteligencia es un buen punto de partida. No discutir actividades ilegales en un mitin o espacio público. Mantén controlado el acceso a llaves, documentos, fondos, equipo, etc. entre las manos de los miembros confiables. Hace duplicados de documentos/ información importante, etc., y guárdalos en una locación segura y secreta. Establece un grupo con miembros de confianza a los cuales otros puedan consultar sobre seguridad, infiltración de la policía, informantes, etc.

2. **Discute directa y abiertamente** con la forma y contenido de lo que haga o diga cualquiera, si es un sospechoso de ser un agente, o tiene problemas emocionales, o es simplemente iluso.

3. **Mantente alerta de los Agentes Provocadores y elementos criminales** que constantemente están avocando por riesgosas acciones ilegales, los que muchos tiene n acceso a armas u otros recursos que quieran compartir con el grupo. Muchos grupos de los ’60 y ’70 claramente comprometieron principios básicos en orden de acomodarse a este tipo de infiltrado.

4. **No aceptes todo lo que escuchas o lees como un hecho.** Revisa con fuentes confiables la información antes de actuar. Comunicación personal entre miembros confiables pudieron prevenir o limitar muchas operaciones del FBI en los ’60s y ‘70s.

5. **No reproduzcas rumores dañinos** acerca de otros- habla con amigos confiables (o miembros de grupos responsables

de lidiar con intervenciones encubiertas). Evita los chismes de otros, especialmente en las telecomunicaciones.

6. **Verifica y revisa varias veces todos los arreglos** de hospedaje, transporte, habitaciones de reuniones, etc., para asegurarse que no han sido canceladas o cambiadas por otros.

7. **Documenta todas las formas de abuso**, robos, asaltos, redadas, arrestos, vigilancia, intentos de reclutar informantes, etc. para identificar patrones y objetivos. Esto también puede ser usados como reportes y defensa legal.

8. **NO hables con ningún policía o agente de inteligencia**. NO permitas que entren a ninguna residencia sin una orden. Trata de obtener fotos de los agentes involucrados. Si miembros ilusos entran en conversaciones con la policía o agentes, explícale en el daño que puede resultar.

9. **Alerta a otros si es que los abusos de la inteligencia o la policía aumentan**, (realizan mítines, confecciona comunicados de prensa, etc.). Esto hace que otros grupos estén atentos a la represión y puede limitar un abuso mayor a través de la exposición.

10. **Prepara a otros miembros del grupo para que sigan organizando** por si arrestan a los "lideres", etc. Esto incluye compartir conocimientos y habilidades, contactos públicos, etc.

¿FIN?