UN PASO ADELANTE DEL ENEMIGO...

(CONSEJOS PARA CREAR UNA CULTURA DE SEGURIDAD Y MANTENERNOS LEJOS DE LAS MANOS DEL ESTADO)

Prólogo

Un saludo a todxs lxs que luchan. Esta publicación es una compilación de varios textos que tocan el tema de la seguridad para lxs luchadorxs por la liberación total. El nombre de la publicación ¨*Un paso adelante del enemigo*¨ refiere a la necesidad de estar siempre preparadxs ante los intentos del Estado por detener nuestras acciones y frenar el conflicto permanente que causa una gran molestia al sistema de dominación. Aunque pueda ser que en este momento no existan todos los tipos de vigilancia mencionados en esta publicación a tu alrededor (por ejemplo hasta ahora no es común encontrar micrófonos en casas de anarquistas en México), ten por seguro que un día llegarán y por eso siempre es mejor estar preparadxs para tales situaciones. Por otro lado, hay escenarios que son comunes universalmente, como la facilidad del enemigo para seguirnos en las redes sociales y por internet, lo cual es una realidad represiva hoy en día.

Los textos ¨*Cultura de Seguridad*¨ y ¨*Seguridad Activista en el Época Digital*¨ son traducciones editadas, el primero viene de un fanzine canadiense llamado ¨*Security Culture: a handbook for Activists*¨ y el segundo de la revista estadounidense por la liberación de la tierra ¨*Resistance*¨- agradecemos a lxs autores el aporte de estos textos importantes. Es bueno señalar que fueron escritos hace unos años, se debe tomar en cuenta que pueda haber nuevos desarrollos y cambios acerca de la represión digital.

Finalmente queremos decir que nosotrxs no somos ¨profesionales¨, todxs cometemos errores y así es como unx aprende y desarrolla su lucha. Sin embargo, estos consejos son hechos con el afán de compartir las lecciones aprendidas por compañerxs en sus trayectos, para poder seguir adelante en nuestra lucha por la destrucción del sistema de dominación. Tampoco nos gustaría que esta publicación hiciera que alguien eligiera no participar en la acción directa, por el contrario que sirvan estos consejos de alguna forma para poder minimizar el riesgo de que algún compañerx caiga presx y poder llevar a cabo una lucha eficaz y devastadora contra lxs enemigxs de la libertad.

Mexico D.F.
Deciembre 2012

Cultura de seguridad

¿Que es la cultura de seguridad?

La cultura de seguridad es una cultura en donde lxs compañerxs conocen sus derechos y lo más importante, los hacen valer. Lxs que pertenecen a una cultura de seguridad también saben lo que compromete la seguridad y se apresuran a orientar a las personas que, por ignorancia, olvido o debilidad personal, son partidarixs de un comportamiento inseguro. Esta consciencia de seguridad se convierte en una cultura cuando el grupo en su conjunto hace que las violaciones a la seguridad sean socialmente inaceptables adentro del grupo. La cultura de seguridad es algo más que solo lo dirigido a comportamientos específicos en lxs individuxs como jactancia, chismes o mentiras. Se trata también de comprobar los comportamientos y las prácticas del movimiento en su conjunto para garantizar que nuestras propias practicas opresivas (vicios sociales) no alimenten las operaciones de inteligencia que están llevando a cabo en contra de nuestra comunidad.

Por ejemplo, el racismo, el sexismo, los problemas personales entre compañerxs o las actitudes de competitividad en el movimiento pueden ayudar a crear una división, ayudando a hacer que algunas personas sean más vulnerables a lxs infiltradxs (lxs que se sienten marginadxs por las practicas opresivas del grupo), que crean oportunidades que pueden ser utilizadas por agentes del Estado para desarticular un grupo de acción.

Obviamente, nuestros movimientos tienen mucho trabajo que hacer antes de responder a las preguntas más grandes, lo importante aquí es reconocer como los comportamientos opresivos crean una mala cultura de seguridad.

Practicas (in)seguras

A lxs luchadorxs nos gusta hablar y hablar, generalmente podemos pasar horas y horas discutiendo la teoría, las tácticas y la estrategia. Mayormente esto es útil en la construcción de nuestro análisis y nuestro trabajo, pero en otros casos esto puede ser peligroso.

Lo que no hay que decir

Para empezar, hay ciertas cosas que son inapropiadas para discutir. Estas cosas son:

-Tu participación o la de alguien más en un grupo clandestino.

-El deseo de alguien más por involucrarse en un grupo clandestino.

-Preguntar a otras personas si son miembros de un grupo clandestino.

-Tu participación o la de alguien más en acciones ilegales.

-Hacer promoción a las acciones ilegales de otra gente.

-Tus planes o los de alguien más de hacer una acción ilegal en el futuro.

Esencialmente, es una mala idea hablar sobre la participación (pasada, presente o futura) en actividades ilegales. Estos son temas de discusión inaceptables, independientemente de si es un rumor, una especulación o un conocimiento personal.

Ten en cuenta: esto no quiere decir que es incorrecto hablar de la acción directa en términos generales. Es perfectamente legal, seguro y deseable que la gente hable en apoyo de la acción directa y de todas las formas de resistencia. El peligro está en la vinculación de lxs activistas con acciones o grupos específicos.

Tres excepciones

Solo hay tres ocasiones cuando es aceptable hablar de acciones específicas y la participación de compañerxs.

La primera situación sería si se planea una acción con otrxs miembros de tu grupo pequeño (tu célula o grupo de afinidad). Sin embargo, estas discusiones no deberían tener lugar a través del internet (correo electrónico), línea telefónica, por correo o en la casa o coche de unx compañerx, ya que estos lugares y formas de comunicación son frecuentemente controladas. Las únicas personas

que podrían y deberían oír esta discusión son lxs que están participando activamente en la acción. Cualquier persona que no va a participar no tiene por que saber y por tanto, no debe de saber.

La segunda excepción se produce después de que unx compañerx ha sido arrestadx y llevado a juicio. Si ella/el es encontradx culpable, estx compañerx puede hablar libremente sobre las acciones por las que fue condenado. Sin embargo, ella/él nunca debe de dar información que pueda ayudar a las autoridades a determinar quien más participó en la acción.

La tercera excepción es para las cartas, comunicados y entrevistas anónimas. Esto debe de hacerse con mucho cuidado y sin comprometer la seguridad.

Estas son las únicas situaciones en las cual es apropiado hablar de tu participación o la de otras personas, o tu intención de cometer una acción directa ilegal.

Medidas de seguridad

Luchadorxs veteranxs sólo permiten que unas cuantas personas sepan acerca de su participación en grupos de acción. Estas pocas personas son lxs miembros de su célula con quienes hacen las acciones y nadie más!

La razón de estas precauciones de seguridad es obvia: si alguien no sabe nada, no pueda hablar sobre ella. Después de una acción lxs activistas externxs no tienen las mismas consecuencias graves que las que tendrián aquellxs quienes llevaron a cabo la acción, pero cuando saben lo que hicieron lxs demás son mucho más propensos de hablar después de haber sido acosadxs e intimidadxs por las autoridades, porque no son lxs que van a terminar en la cárcel. Incluso aquellas personas que son fieles, a menudo pueden ser engañadxs por las autoridades para revelar información perjudicial e incriminatoria. Lo más seguro es que todxs lxs miembros de una célula mantengan la información de su participación en el grupo solo entre sí mismxs. El menor número de personas que lo conozcan significa menos pruebas a largo plazo.

Comportamientos que violan la seguridad

En un intento por impresionar a lxs demás, lxs compañerxs pueden comportarse de una manera que compromete la seguridad. Algunas personas hacen esto con frecuencia- son habitualmente chismosxs o presumidxs. Algunxs otrxs compañerxs dicen cosas inapropiadas cuando consumen alcohol. Muchxs compañerxs violan la seguridad ocasionalmente porque fue una tentación momentánea el decir algo o insinuar algo que no debería de haber dicho o insinuado. En la mayoría de todas las situaciones, el deseo de ser aceptadxs es la principal causa.

Las personas que tienden a ser las de mayor riesgo de seguridad son lxs compañerxs que tienen una baja autoestima y un fuerte deseo de aprobación de otrxs compañerxs. Ciertamente es natural el buscar la amistad y el reconocimiento por nuestros esfuerzos, pero es imperativo que nos mantengamos fuertes sobre estos deseos para no poner en peligro la seguridad de otrxs compañerxs o de nosotrxs mismxs. Las personas que anteponen su deseo de ¨amistad¨ y aceptación sobre la importancia de la lucha pueden generar un grave daño a nuestra seguridad.

Mentiras:
Para impresionar a lxs demás, lxs mentirosxs dicen haber realizado acciones ilegales. Tales mentiras no sólo comprometen la seguridad de la persona que las dice (lxs policías no entienden lo que se dice como una mentira) sino que también obstaculiza la solidaridad y la confianza.

Chismes:
Alguna gente piensa que puede ganar amigxs por tener información especial. Estxs chismosxs hablarán a cerca de quien hizo tal o cual acción o, si no saben quien lo hizo, adivinan quien creen que hizo las acciones, o simplemente difunden rumores sobre quien fue. Este tipo de conversaciones son muy dañinas. La gente debe recordar que los rumores son todo lo que se necesita la policía para iniciar una investigación o incluso presentar cargos.

Jactancias:
Algunas personas que participan en acción directa ilegal podrían tener la tentación de alardear de ella con sus amigxs. Esto no sólo pone en peligro la seguridad de la persona quien habla, sino también la de otras personas involucradas con la acción (con esto se puede ser acusadx y buscadx por asociación). Además de que las personas con quien ella/él habló pueden tener cargos como encubridorxs. Un activista que se jacta o presume también establece un mal ejemplo.

Jactancia Indirecta:
Lxs que se jactan indirectamente son personas que hacen una gran insinuación sobre como desea

mantenerse en el anonimato, evitar las manifestaciones y mantenerse ¨subterráneo¨. Quizás no salgan y digan que hacen acciones directas ilegales, pero de manera indirecta se aseguran de que todxs lxs que pueden oír sepan que están tramando algo.

EDUCAR PARA LIBERAR

La triste verdad es que hay algunas personas ignorantes de la seguridad en el movimiento y otras personas que probablemente han sido criadxs en un ¨escena¨ que se nutre de los alardeos y chismes. Esto no significa que estas personas son malas, pero sí significa que necesitan informarse y aprender sobre la seguridad personal y del grupo. Incluso lxs luchadorxs con experiencia cometen errores cuando hay una falta general de consciencia de seguridad en nuestros grupos.

Y ahí es donde ustedes, leyendo esto pueden ayudar. Debemos actuar para informar SIEMPRE a las personas cuyo comportamiento es inseguro. Si alguien que conoces está haciendo alarde de una acción o difundiendo chismes que comprometen la seguridad, es tu responsabilidad explicar a ella o a el por qué ese tipo de conversaciones viola la seguridad y es inapropiado.

Debes tratar de compartir este conocimiento en una forma que favorezca la comprensión de la persona y que cambie su comportamiento. Se debe hacer sin dañar el orgullo de la persona. Mostrar tu sincero interés en ayudar a el/ella para convertirse en un/a luchador/a más eficaz. Mantén tu humildad y evita tener una actitud de superioridad. Un enfoque insensible puede aumentar las defensas de una persona y evitar que escuche y haga uso a los consejos ofrecidos. El objetivo de abordar estas cuestiones con lxs demás es para reducir los comportamientos inseguros y no para mostrar cuanto más consciente eres de la seguridad. Comparte tus preocupaciones y el conocimiento con alguien en privado, para que la persona no se sienta como si fuera una humillación pública. Hacer frente a la persona lo más pronto posible después de haber violado la seguridad, esto aumentara la efectividad.

Si cada unx de nosotrxs nos hacemos responsables de platicar la información sobre la seguridad con la gente que comete ciertos errores, podemos mejorar la seguridad en nuestros grupos y actividades. Cuando la gente reconozca que las mentiras, los chismes, el presumir y las conversaciones inapropiadas hacen daño a sí mismxs y a otrxs, estos comportamientos pronto se terminarán. Mediante el desarrollo de una cultura en donde la violación de la seguridad es señalada y desanimada, todxs lxs luchadores sincerxs rápidamente lo entenderán.

COMO LIDIAR CON LOS PROBLEMAS CRONICOS DE LA INSEGURIDAD

Entonces, ¿qué hacemos con lxs activistas que violan repetidamente las precauciones de seguridad, incluso después de haber sido informadxs en varias ocasiones? Desafortunadamente para ellxs, lo mejor que se puede hacer es cortar la relación. Discutir el tema abiertamente y pedirles que se alejen de las reuniones, campamentos y organizaciones. Con el avance o la creación de nuevas leyes, y la abrogación de leyes anti-terroristas que exigen sentencias más duras para las acciones políticas y con las cortes dictando sentencias más largas por motivos ¨políticos¨ , las apuestas son demasiadas altas como para permitir que lxs ofensorxs crónicxs de la seguridad puedan trabajar entre nosotrxs.

Al crear una cultura de seguridad, tenemos una defensa eficaz contra informadorxs y agentes que tratan de infiltrarse en los grupos. Imagina un/a informador/a del estado que, cada vez que pregunte a otra activista sobre sus actividades, solo reciba información acerca de la seguridad- se frustraría el trabajo del informante. Cuando otrxs luchadorxs descubran que él o ella continúan violando las medidas de seguridad después de haber sido informadx en varias ocasiones, habría motivos suficientes para aislar a la persona de nuestros grupos. Y eso sería un/a informante menos para nosotrxs.

SEGURIDAD ACTIVISTA EN LA EPOCA DIGITAL

La vigilancia del gobierno hacia los movimientos sociales no es algo nuevo, pero las herramientas y métodos que están disponibles para la ley se mantienen en constante cambio con cada avance tecnológico. La mayoría de lxs activistas no son tan diferentes al público cuando se trata de nuestra dependencia al internet, nuestras computadoras personales, celulares y - lamentablemente - paginas de redes sociales.

La mayoría de nosotrxs estamos familiarizadxs con la cultura de seguridad, pero fallamos en reconocer que una de las violaciones más grandes de nuestra privacidad y la amenaza a nuestra seguridad está en nuestras casas, nuestras oficinas y nuestros salones.

Lo físico:

La seguridad de una computadora, así como todos los tipos de seguridad, comienza con lo físico. Si no puedes asegurar físicamente tu computadora, no puedes garantizar su seguridad. Con un poco de tiempo, las fuerzas de la ley pueden instalar un registro del teclado (una programa que recordara todo lo que escribes) que puede derrotar todos los mecanismos abajo descritos. Por ejemplo una cámara escondida o un registro del teclado podrían capturar fácilmente tu llave privada PGP.

La manera más sencilla para asegurar tu computadora es cargándola contigo. Una lap pequeña es una buena opción para esto. Esto no quiere decir que tienes que tirar a la basura tu computadora de escritorio, sino que tienes que tomar en cuenta que no puedes saber que o quien podría haber estado cerca de ella. Un ejemplo es el de un activista al que la policía hizo una redada en su casa, un año después del cateo fue detenido. Continuó usando la misma contraseña PGP (ver abajo información sobre PGP) después del cateo, y entonces su PGP no sirvió para nada porque las fuerzas de la ley pudieron descifrar sus correos. Estos correos fueron usados después como evidencia en su juicio.

SiISTEMA OPERATIVO:

Otro elemento básico es tu sistema operativo (SO). La mayoría de la gente está familiarizada con el SO de Microsoft. Por razones numerosas, lxs luchadorxs no deberían usar Microsoft. Es una fuente totalmente cerrada, esto significa que no sabemos qué hace el código, si hay una ¨puerta atrás¨, y sencillamente no es seguro- es susceptible a Malware, sea criminal o del gobierno (virus, spyware, trojans etc.) como CIPAV. CIPAV es un programa de spyware creado y difundido por el FBI, que monopoliza remotamente la computadora de la persona siendo investigada, mandando los datos al gobierno. Documentos obtenidos recientemente por un solicitud FOIA detallan el uso de CIPAV por el FBI, encontraron que en todos los casos en que detectaron este programa, solo funcionó en los SOs de Microsoft. Mac OS X o Linux/Ubuntu son buenos sustitutos de fácil uso como Microsoft pero con la seguridad y un código open source (Mac OS X es parcialmente open source, Linux es totalmente abierto). Acostumbrarte a Linux puede ser un poco difícil al comienzo, pero requiere menos mantenimiento que Windows. Linux normalmente funciona con cualquier Microsoft hardware. Ubuntu o cualquier otra distribución de Linux puede ser descargado gratis en sus páginas web.

Los datos encriptados:

El próximo elemento básico

es la encripción de datos, que nos permite asegurar nuestros datos mientras están en nuestra computadora (en el caso de una orden de registro) y cuando están en tránsito (por correo electrónico por ejemplo). Hay niveles diferentes de encriptación, puedes encriptar un correo antes de que lo envíes, un archivo en tu disco duro, una partición (una sección de tu disco duro) o tu disco duro entero. Usuarixs de Mac tienen un montón de elección de encriptado de disco duro como PGP y TruCrypt. CheckPoint software ofrece una alternativa para usuarixs de Linux pero aun no la hemos probado. En cualquier combinación de SO y hardware, es imperativo que uses tecnología encriptada.

Las denuncias penales están llenas de referencias a documentos incriminatorios recuperados de computadoras durante redadas y es mejor que vayas creyendo que las computadoras son las primeras y más importantes cosas en la lista de ítems para secuestrar (claro, después de material, explosivos etc.). PGP funciona en computadoras Mac y Linux. GNuPG es un buen sustituto para usuarixs de Linux pero debes de instalar un frontend grafical como Seahorse también. Ambos funcionan creando una llave-par: una es privada y la otra es pública, y es intercambiada solo con gente con quien necesites comunicarte de manera segura. Los mensajes solo pueden ser encripados y abiertos cuando hay una llave-par que es igual. Hay tutoriales buenos en el internet, solo asegúrate saber cómo usar el software y recuerda que si tu computadora ha estado comprometida durante un cateo, por ejemplo tu llave-par también estará ya comprometida, dando a la ley la capacidad de descifrar TODAS tus comunicaciones o archivos que usan esa llave. Igualmente Hushmail no está suficientemente encriptado, en el pasado han cooperado con el gobierno. También debes saber que mientras cruces cualquier frontera tu laptop puede ser revisada y si encuentran material ilegal o sospechoso, requerirás producir una nueva contraseña a estos documentos o partes de ellos después. Si deseas saber más o mirar otros ejemplos, busca en la red el caso Boucher.

La anonimidad en línea:

Un componente principal de la seguridad de la computadora es la anonimidad en línea. Si te conectas al internet, tu computadora usa algo que se llama dirección IP. Hay demasiado que se puede decir sobre eso pero la cosa básica es que esta dirección está registrada por el proveedor de servicio del internet que te da la conexión a internet (en caso de México, Telmex por ejemplo) o el de un café internet y el servidor al que te estás conectado.

Tu dirección IP te sigue a todos lados mientras que estas en línea y cuando es registrada puede ser retenida por un tiempo indefinido, y también no sabes quien la usará. No es perfecto, pero TOR logra un nivel de anonimidad en línea. TOR se describe como un ¨router cebolla¨ que significa que tu conexión a otro servidor rebota de otros intermediarios. Estos intermediarios no tienen ni idea de en donde se originó tu tráfico o a donde va. Esto garantiza que el servido final (un servidor de web por ejemplo Telmex) no sabe de cual sistema viene la solicitud. TOR puede ser instalado fácilmente usando un paquete de software que se llama Vidalia. TOR tiene sus limitaciones - es lento y el trafico mandado por la red TOR no es cifrado. Necesitas recordar eso si planeas mandar un correo u otro archivo usando TOR. Conexiones SLL (Https) con archivos cifrados deben ser usadas para garantizar la privacidad. TOR solamente te proejará del análisis del tráfico.

www.torproject.org

No deja ni un rastro en la red:

Si no estás usando encripción en tu disco duro como PGP, encriptar tus archivos individuales no es suficiente. Cada letra que escribes, si estas escribiendo un documento o mirando la web, estás dejando un rastro que no sabes que existe. Denuncias penales refieren mucho a búsquedas en línea que usuarixs han hecho o documentos medio escritos enterrados dentro de su disco duro. La mayoría de gente conoce la memoria RAM; esta es donde las aplicaciones están guardadas. Se pierden todos los datos cuando tu computadora se apaga (lo contrario de tu disco duro que tiene memoria permanente). Además, cada computadora usa algo que se llama Swap File que ayuda a mejorar la función de la misma. Esencialmente, tu SO designa una parte de tu disco duro como memoria adicional RAM. El problema es, cuando la computadora está apagada el dato que está guardado allí no se pierde. Cuando estas escribiendo un documento que quieres encriptar más tarde, una versión de este archivo podría estar guardado en el Swap File. También cuando borras un archivo, en realidad no está borrado. El titulo es eliminado y el espacio se hace

disponible para otros archivos, pero no está totalmente borrado hasta que otro archivo se escriba sobre este espacio. El comando de eliminación segura es una herramienta disponible para usuarixs de Linux que te deja borrar un archivo con seguridad, el contenido de tu Swap File y el espacio libre. El encriptado de todo tu disco duro resuelve ambos problemas. Puedes apagar tu Swap File pero tienes que tener mucha memoria RAM instalada antes de hacer eso, lo cual normalmente no está disponible con laptops.

Similarmente, cuando buscas en internet, las imagines, las cookies, los textos buscados, todo esto se está guardado en tus archivos temporales, en tu computadora. Debes de estar consciente de la acumulación de estos datos! Una buena opción es usar una opción en tu navegador web que se llama ¨Private Browsing¨ o ¨Busqueda privada¨ disponible con Safari y Firefox, como Stealther add-on para Firefox. Los dos desactivan la retención de datos que pasa comúnmente cuando buscas en el internet, previenen que esto se guarde desde el primer momento. Pero ningún sistema es perfecto, aun deberías limpiar los datos privados en el menú de cada browser y buscar y borrar cualquier dato que queda en tus carpetas temporales.

https://addons.mozilla.org/en-US/firefox/addon/1306

El sentido común:

La parte final es el sentido común. El uso de páginas de redes sociales como Facebook por luchadorxs no es solamente desalentador sino que también ha tenido como resultado un montón de órdenes de búsqueda y captura y denuncias penales. Facebook da una vista muy clara al estado de nuestras vidas personales y un mapa de asociaciones de lxs compañerxs dentro del ¨movimiento¨- lo cual el enemigo puede usar para interrumpir nuestras acciones. Grupos e individuxs radicales no tiene nada que ganar con anunciar información en un foro social como este. Además, tu lista de ¨amigxs¨ detalle tus conexiones mejor que cualquier herramienta sofisticada usada por las fuerzas de la ley, además les da una idea sobre nuevxs individuxs para vigilar y acosar. MySpace por ejemplo ha sido usado por el FBI para instalar CIPAV. Órdenes de búsqueda confirman que el Messenger de MySpace ha sido usado para infectar la computadora de algunxs individuxs.

Recientemente se encontraron dos páginas de liberación animal distribuyendo Malware ¨criminal¨. Todo lo que unx tuvo que hacer fue visitar una de estas páginas desde un buscador como Google e inmediatamente una descarga maliciosa se puso en marcha. Se pudo capturar ese virus y quitar la infección pero esto ilustró un punto crucial, que paginas de contra-información o cualquier otra puede ser usado como punto de distribución de Malware para uso ¨criminal¨ o del gobierno. Documentos obtenidos del CIPAV vía una solicitud de FOIA documentaron que el gobierno infecta páginas para instalar su Spyware en las computadoras de lxs individuxs de sus investigaciones (que fueron atraídxs a las páginas). Nunca instales un ítem de software si no sabes exactamente qué es lo que estas instalando y si no has visitado directamente la página oficial del software. Actualizaciones falsas de Flash comúnmente están usadas para engañar a lxs usuarixs para descargar un programa malicioso (la víctima recibe un pop-up que dice que se tiene que descargar la actualización de Flash). Es seguro asumir que el gobierno está usando el mismo Malware y las vulnerabilidades de lxs que usan lxs ¨criminales¨ (por ejemplo quienes hacen fraudes electrónicos o bancarios etc.)

Activistas por la libertad de Tibet fueron víctimas de una campaña grande de hackers chinxs para espiar e interrumpir sus actividades, que se refiere como GhostNet. Anuncios infectados de manifestaciones en forma de documentos de Word y PDF fueron enviados varias veces a estxs activistas. Los programas de Spyware también son capaces de prender la Webcam de la computadora remotamente. Tienes que ser honestx, si recibes un flayer sobre una protesta o actividad o un nuevo fanzine en PDF, lo más probable es que lo abrirías. Asegúrate que sabes quién esta mandándote el documento y que lo estas esperando. Además, utilizar un buen escáner de Malware como Clam AV (gratis para usuarixs de Mac y Linux) para escanear documentos antes de abrirlos (solo tienes que guardarlo en tu escritorio y escanearlo desde ahí). Si esto pasa no sabrías que tu computadora está infectada, especialmente por el gobierno.

www.clamav.net

CINCO PUNTOS BASICOS DE LA SEGURIDAD DIGITAL

Aunque los siguientes puntos pueden sonar algo paranoicos, están construidos en base a realidades represivas alrededor del mundo tanto como en México. En la guerra social debemos estar siempre un paso adelante del enemigo, ser listxs y estar preparadxs para las acciones represivas y ofensivas del enemigx. Estas propuestas para la seguridad están escritas en pro de no tener más guerrerxs presxs ya que afuera podemos dar una lucha más eficaz que desde adentro de la cárcel.

1 El teléfono celular es una forma muy útil para escuchar tus conversaciones por parte de la policía. La policía puede activar el micrófono ambiental que tiene una magnitud de aproximadamente 4 metros, por medio del cual pueden grabar o escuchar tus conversaciones. Lo mejor es que si tienes un teléfono celular cerca quites la batería y el chip antes de comenzar una charla que pueda comprometer tu libertad o la de algún/a compañerx. En algunos casos en Inglaterra han podido prender el micrófono ambiental todavía mientras el celular está apagado y en algunas ocasiones cuando se quitó la batería ya que ésta guardo un poco de energía. En el mejor de los casos no uses o no portes tu celular a una reunión. También no lo lleves a una acción ya que pueden seguirte mediante el rastreo o usar estos datos después para vincularte a la acción.

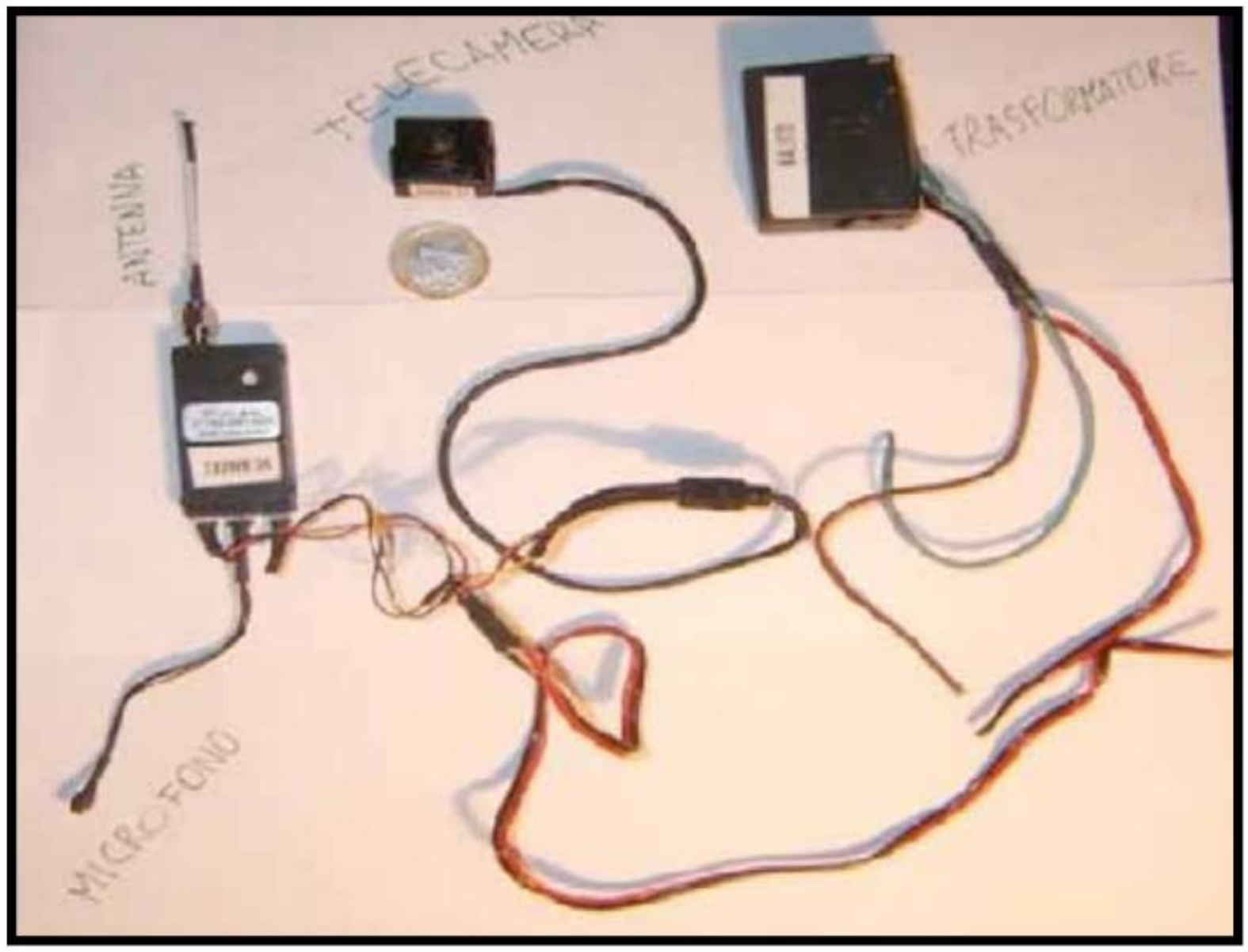
2 No envíes correos comprometidos o comunicados de acciones desde tu correo personal ya que es muy fácil que alguien más lo pueda leer o encontrar el origen y aun más cuando escribes palabras ¨claves¨ (por ejemplo, ¨explosivos¨, ¨armas¨ etc.) Toma en cuenta que los servidores de páginas web de apoyo al movimiento son frecuentemente vigilados por la policía cibernética. Por ejemplo hemos sabido que la policía cibernética mexicana frecuentemente trata de hackear la cuenta de correo electrónico de la página Liberación Total en Chile y otras páginas parecidas. Crea un mail único para enviar cada comunicado y créalo desde un café internet, lejos de tu casa o zona. Por lógica tampoco los envíes desde tu PC personal.

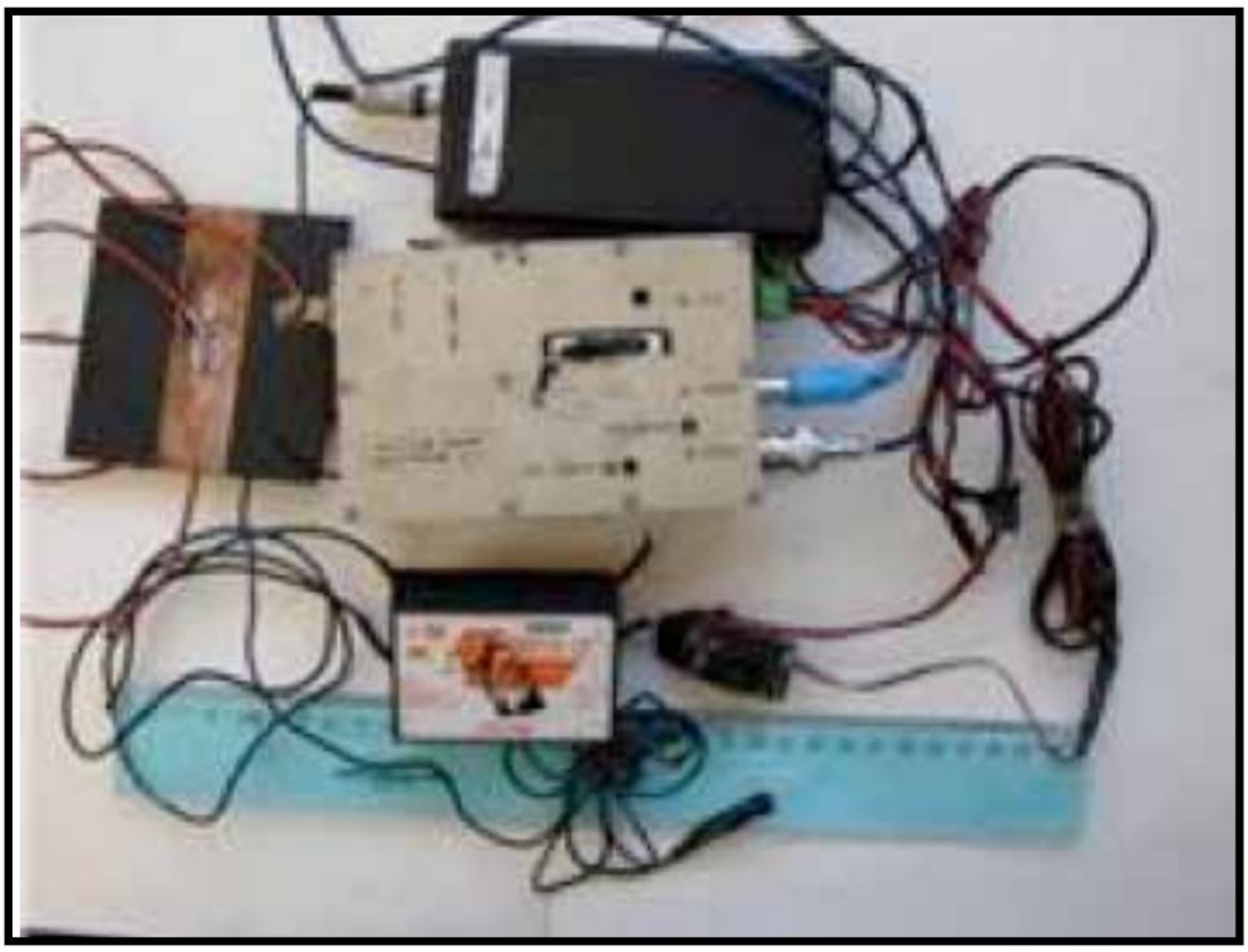
3 Cuando hables por teléfono, no insinúes cosas que tu u otra persona ha hecho o no haga insinuaciones obvias ni menciones lugares o fechas. Mejor evita hablar de cosas comprometidas por teléfono ya sea fijo o celular. Pero si es absolutamente necesario que hables por teléfono, crea claves que tengan un sentido común. Estas claves deberán ser creadas con anterioridad y memorizadas.

4 No utilices redes sociales, especialmente Facebook y Twitter para hacer supuestas amistades, ya que estas páginas proporcionan datos directamente al gobierno. **Al usar estas redes sociales tu mismx estas dando tu información personal al enemigx, dándoles permiso a vigilarte y ver tus asociaciones y movimientos.** También publicar fotografías tuyas es un error si eres un luchador y aun más si estas en posible búsqueda.

5. No hables de cosas que te comprometan dentro de tu casa y en especial en centros sociales o anarquistas ya que pueden estar llenos de micrófonos ambientales colocados previamente por la policía para vigilar el movimiento. Un ejemplo es el caso de Italia y los montajes contra el movimiento anarco-insurreccionalista en el que lxs compañerxs han encontrado comúnmente micrófonos escondidos en las cajas de los apagadores de luz en sus casas o hasta encontrado GPS colocados en sus motos. Si tienes automóvil tampoco es conveniente hablar dentro de él.

Microfonos y cámaras encontradas en casas de compañerxs anarquistas en Italia





para expandir la revuelta y la insurreccion
¡Guerra Social!

LA LETRA ARMADA