Para cuidar nuestras comunicaciones en momentos de revuelta

USAIN BOLT DESCALIFICADO Y ENCAPUCHADO :: 08/10/2011

Este artículo pretende ser una ayuda a quienes llevan siempre la gasolina en sus hombros, que no se tragan la repugnante moda políticamente correcta de "protesta ciudadana"

Y que saben con convicción que la única forma de acabar con la dominación impuesta por el Estado/Capital es la violencia callejera como respuesta a su histórica violencia económica-política-policial. Un pequeño aporte para proteger sus comunicaciones e información.

Para quienes buscan el no legítimo, pero si efectivo, camino de la violencia contestataria se aconseja proteger sus comunicaciones por internet de la siguiente forma:

(Se subentiende que *nunca* se debe comunicar por teléfono, ya sea celular o red fija)

1. Si es necesaria la comunicación por internet

No comunicarse u organizar eventos que evidencien sus intenciones mediante redes sociales como MSN Messenger, Twitter, Facebook, etc. Esto debido a que por normas legales la policía puede conseguir información de manera inmediata de algunos portales como Facebook y Twitter, además de intervenir conversaciones de MSN Messenger mediante sus servidores.

Para ello se recomienda utilizar clientes de mensajería instantánea con un complemento de encriptación como por ejemplo Pidgin y OTR. La idea de esto es encriptar (hacer indescifrable) la comunicación entre un emisor y un receptor, encriptando lo que se envía desde computador en computador, para que cuando la conversación pase por los servidores de Passport.net (por ejemplo en cuentas de Hotmail) no pueda ser descifrada por la policía; el descifrado se hace en cada computador mediante una llave única. Pidgin es el cliente de mensajería instantánea y OTR (Off The Record - Fuera de Registro) es el complemento de encriptación. Para esto es casi una obligación dejar de usar Windows y cambiarse a Sistemas Operativos libres.

Además se recomienda utilizar correos cuyos servidores estén debidamente protegidos con esto, por ejemplo Nodo50, Riseup, Sindominio, etc. **Nunca** enviar un correo con información sensible desde un servidor protegido a uno comercial (Hotmail. Google, Yahoo, etc), ya que la policía puede obtener la información de manera fácil en dichos correos, y si se envía de un servidor a otro distinto el correo puede ser intervenido; para evitar esto se recomienda enviar correos dentro de un mismo servidor, por ejemplo de xxxx@nodo50.org a yyyy@nodo50.org. Así evitamos enviar fuera del servidor el mensaje. Las contraseñas de los correos deben ser largas y que combinen letras con números. Por ejemplo en vez de escribir ’Santiago’ una alternativa es ’S4n7i4g0’ (obviamente debe ser mayor a 20 caracteres).

2. Si no es necesaria la comunicación por internet

Comuníquese siempre en persona en lugares donde no existan cámaras de monitoreo ni posibles micrófonos.

3. Si es necesario almacenar información en los computadores

Lo más recomendable es tener una partición aparte en el disco duro y encriptarla con sistemas como Truecrypt; también se pueden encriptar los ’pendrive’ (dispositivos de almacenamiento USB). La clave de encriptación debe ser muy larga, utilizando el mismo método que en el ejemplo de los correos y no se debe guardar en papeles. Se recomienda utilizar estrofas de una canción favorita para su fácil memorización.

4. Si no es necesario almacenar información en los computadores

No almecene su información y mucho menos si utiliza Windows.

¡Solidaridad con la memoria de Manuel Eliseo Gutiérrez Reinoso quien fue asesinado por los pacos! Ninguna agresión sin respuesta.

Relacionado: **Seguridad Contra la Vigilancia Tecnológica**

www.hommodolars.org
