¿*Hackeo* de cuentas o Vietnam cibernético?

La apropiación indebida de cuentas de correo y Twitter ha sacudido el ciberespacio venezolano. Aquí un recuento, un entorno y un vistazo a las diversas hipótesis.

FERNANDO NÚÑEZ NODA

A partir del 31 de agosto pasado empezaron a caer cuentas de Twitter (Ibeyise Pacheco, Eduardo Semtei, Radar de los Barrios, Berenice Gómez *–la bicha–*, Julio César Pineda, Rocío Sanmiguel… et al).

Han sido usurpadas por anónimos que actúan para defender la revolución chavista, según sus propias palabras. Literalmente robadas de sus creadores y dueños y ahora puestas en contra de esas mismas personas, transfieren al delincuente la administración de la cuenta. Las alarmas se encendieron, los *tuits* se multiplicaron. Circularon las palabras *hacker*, *cracker*, *lamer*, *pirata informático* y otras. Ha habido *hashtags* tipo #Hackeca, #AntiHacker, #Venezuelahackeada…

El vocero más protagónico, que se hace llamar N33 (suponemos que se trata de una denominación masónica, que contempla 33 niveles), otorgó algunas entrevistas, entre ellas una a *El Tiempo* de Colombia en la que afirmó que era Alberto Federico Ravell *la joya de la corona*, la cuenta más codiciada.

¿Qué ocurrió y aún ocurre? ¿la iniciativa perversa de un grupo a destajo? ¿un movimiento endógeno más amplio relacionado con un canal de TV del Estado? ¿o una conspiración digital desde el tope del régimen chavista?

Las guerras del siglo XXI

Ya venía sonando la llamada *Guerra de cuarta generación*, un término acuñado en 1989 por el ejército norteamericano, que implica un nuevo tipo de enfrentamiento cuyo contendiente no es necesariamente un Estado y en el cual los *soldados* pueden ser civiles.

El terrorismo, los conflictos de baja intensidad (como el palestino-israelí) y la guerrilla le son comunes. Para muchos, Vietnam es la primera guerra asimétrica contemporánea, entre un Estado y un grupo miliciano y de resistencia civil. El 11 de septiembre de 2001 fue otro punto cenital en el enfrentamiento de grupos autonombrados y países con ejércitos nacionales.

Obviamente, Internet es escenario de una guerra asimétrica, nueva, ideológica en este caso, global, que está en todas partes y en ninguna.

En Wikipedia en inglés se define la *cyberwarfare* o *ciberguerra* como "hacking motivado políticamente para ejecutar sabotaje o espionaje". Podríamos agregar "para posicionar un mensaje politico", si las cuentas son difusoras como Twitter o *blogs*.

La ciberguerra, según definió el Pentágono en 2010, es ya de *quinta generación*. Forma nueva de la confrontación, que compromete uno de los activos más valiosos del siglo XXI: la información digitalizada. El caso más emblemático es *Anonymous*, un grupo inespecífico que apunta sus acciones a corporaciones o estados, pero con una *agenda de base*, es decir, no centralizada ni muy jerarquizada, no circunscrita a un movimiento único, movida por una actitud anarquista.

Pero la más telúrica y global de las ciberguerras, es la que se estima habrá o ya hay entre estados nacionales. Sobre todo: China contra los Estados Unidos. Hace un año, por primera vez, los Estados Unidos advirtieron públicamente que los

chinos tienen una unidad de ciberguerra con expertos civiles y decenas de miles de operarios, que crean virus y perpetran entradas no autorizadas apuntadas a gobiernos y corporaciones occidentales.

Volviendo a la ciberguerra endógena

Pero el asunto se extendía. Recuérdese que una cuenta de Twitter tiene una de *email* asociado. Si se dispone de la dirección de *email* se puede cambiar la clave, de modo que el asunto involucraba el *hackeo* de al menos dos cuentas por persona.

En todos los casos, correos electrónicos que albergaban años de trabajo, mensajería y acopio. En el caso de Radar de los Barrios, el robo del correo de Gmail permitió no sólo la apropiación (aunque temporal) de la cuenta Twitter, sino del blog en Blogger que también borraron.

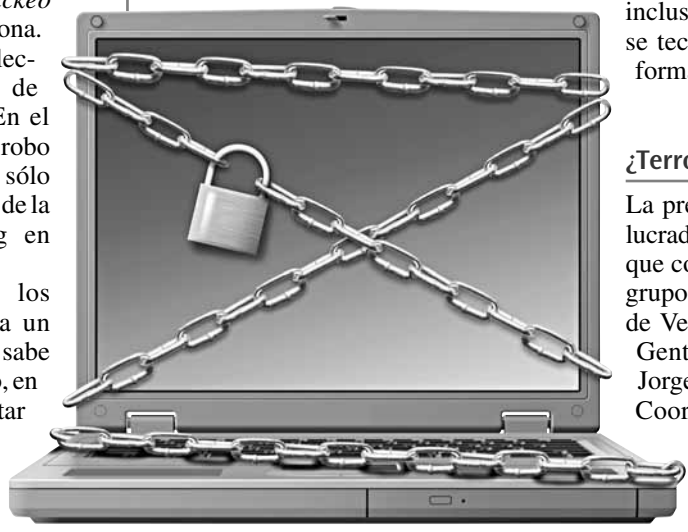
Ahora ¿cómo ocurrieron los ataques? ¿cómo piensa y actúa un *hacker*? No lo sé y tampoco se sabe si fue propiamente un *hacker* pero, en todo caso, si yo tuviese que ejecutar el trabajo empezaría probablemente por no hacerlo solo. Con otras personas puede parecer que el *hacker* no duerme, produciendo contenido, contestando, *hackeando* otras cuentas. Es más intimidatorio.

La disparidad en la redacción del supuesto *unabomber* digital venezolano (*Caín Supremo* es uno de sus nombres), hace deducir que son varios. Un *multibomber* pues. Luego de seleccionar una lista de objetivos (opositores al chavismo, con muchos seguidores en Twitter), trataría la mayor cantidad posible de maneras de *haquear* (prefiero usar la denominación semi anglicista, en vez del españolizado jaquear) a estas inadvertidas víctimas.

Lo primero es descifrar las claves. Y las fáciles primero, porque obviamente son más rápidas. Nombres propios o de familiares, fechas, teléfonos. Hay software que prueba combinaciones y permutaciones. Hay muchas otras formas no tecnológicas de capturar una clave. Como aprendiz de *hacker* me iría de pesca, pero sin salir de una habitación. El *phishing* sucede cuando se logra que un usuario visite un sitio web falso donde deja *login* y clave. Ocurre mucho con las estafas bancarias.

Uno recibe una supuesta notificación del banco (un movimiento extraño en su cuenta, un mantenimiento en los servidores) y le piden verificar su identidad en una página exacta a la del banco, excepto por el URL que casi nadie lee. Allí el usuario sirve en bandeja de plata sus datos. Lo mismo puede hacerse para captar los datos de correo. Si alguno en el equipo tuviese pericia en programación, desarrollaría una falsa aplicación asociada a Twitter, de las que parecen trabajar bajo la autorización del servicio de microblogging, pero sólo apuntan a entrar en el perfil y provocar el cambio de clave. Si la víctima es lo suficientemente poco tecnológica, la induzco a descargar un programa gratuito que prometa hacer cualquier cosa menos su verdadero fin: espiar. El *spyware* lee registros y, si es del tipo *keylogger*, incluso es capaz de registrar todo lo que se teclée. Hay, como dije, más de una forma de ejercer el delito informático.

> ***La disparidad en la redacción del supuesto* unabomber *digital venezolano* (Caín Supremo *es uno de sus nombres), hace deducir que son varios. Un* multibomber *pues.***



¿Terrorismo espontáneo u oficial?

La pregunta es ¿hasta dónde está involucrado el oficialismo? Entre las personas que consulté hay variadas hipótesis. Un grupo que opera en una ciudad del centro de Venezuela y no es Caracas, es uno. Gente relacionada con Mario Silva y Jorge Amorín, de "La Hojilla", es otro. Coordinados por Andrés Izarra, otra.

Las versiones más *conspirativas* hablan de técnicos en Cantv y Movilnet, tratando de desencriptar data que pasa por las conexiones ABA.

Las más audaces, de grupos de iraníes y chinos trabajando en el Hotel El Conde o en los alrededores de la Plaza Bolívar caraqueña. Y los *exógenos* indican que muchos ataques pudieron provenir del exterior de Venezuela. Mientras más involucrado esté el régimen, menos mérito técnico tienen los *hackers*, y más grave sería la situación.

FERNANDO NÚÑEZ NODA
Periodista venezolano. Autor de varios libros sobre el tema de Internet, redes sociales y periodismo digital.