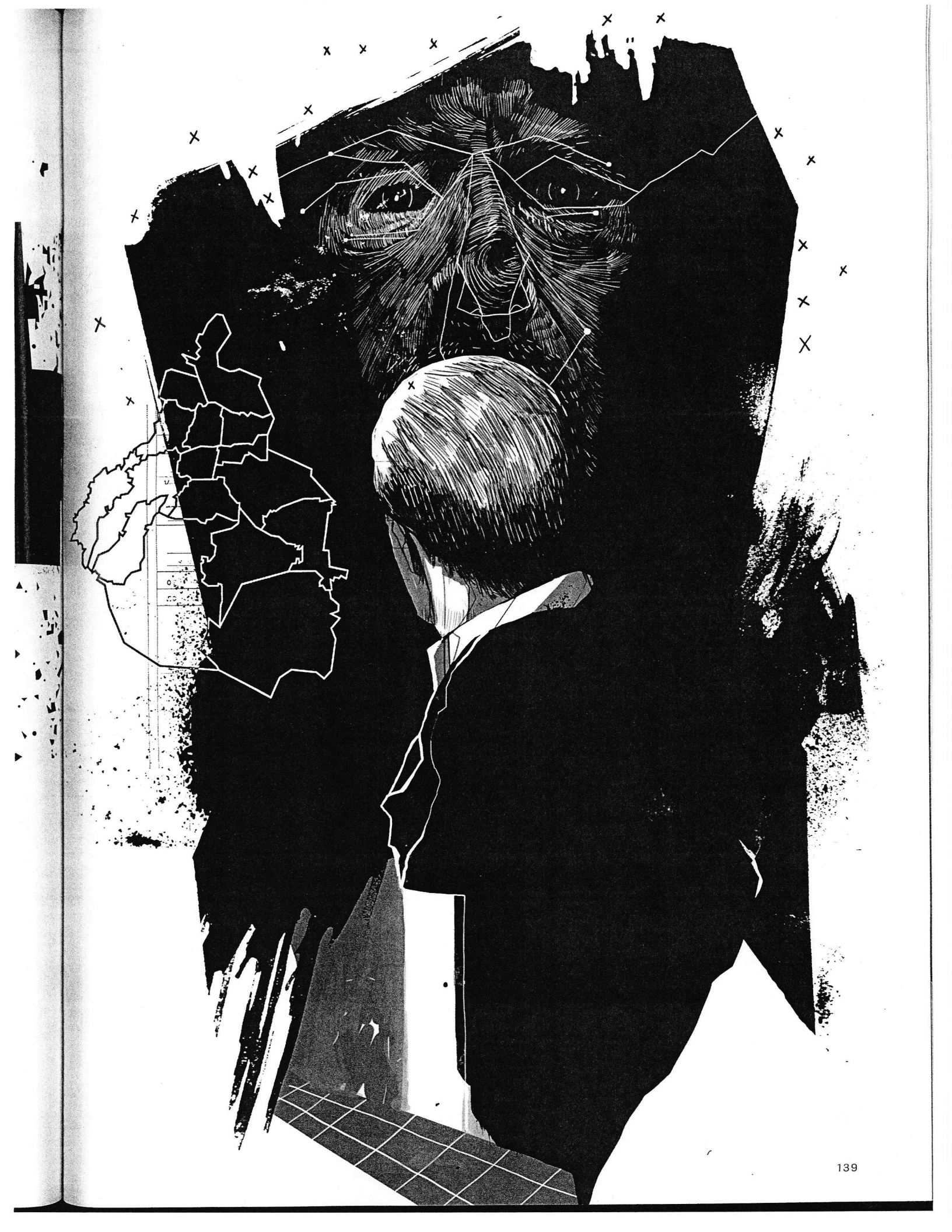
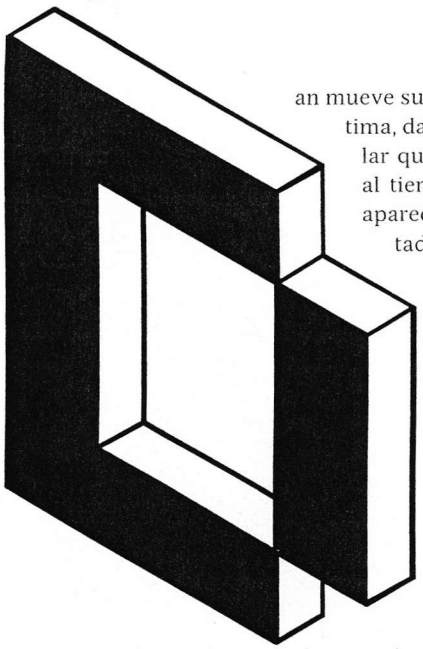
# A LA SOMBRA DE LA RED

DESDE SU BUNKER EN EL DF, UNO DE LOS *HACKERS* MÁS EXPERIMENTADOS DE MÉXICO NOS CUENTA EL VERDADERO ESTADO DE LA CIBERSEGURIDAD EN EL PAÍS. NO SÓLO FALTA SEGURIDAD POLICIACA Y CONOCIMIENTO DE LOS USUARIOS; ANTES QUE TODO, LO QUE EL INTERNET MEXICANO NECESITA ES MÁS *HACKERS* PARA DESCUBRIR LAS VULNERABILIDADES DEL SISTEMA Y CORREGIRLAS.

POR | JULIO GODÍNEZ HERNÁNDEZ
ILUSTRACIONES | IGNACIO HUIZAR





an mueve su dedo índice como un buitre buscando víctima, dando vueltas mientras señala un espectacular que domina el cielo de la tarde. "¡Ésa! –dice al tiempo que señala la página de internet que aparece allí en letras enormes–. Abre tu computadora y métete a esa página", me pide mientras echa a andar un programa en su pantalla. Teclea algunos comandos en una ventana negra. "Listo. Actualízala". Con la pericia de un prestidigitador, Dan ha desaparecido la página. Pero para ello no usó ninguna magia: el *hacker* tiene un ejército de computadoras que lanzan peticiones de acceso a la página meta, que ha sido puesta fuera de línea. En su lugar ahora aparece una leyenda: "El servidor no ha podido localizarse".

Es un jueves cualquiera en un café de la ciudad de México. Cientos de clientes reciben en su *ticket* la clave con la que podrán conectarse a internet a través de la red del local. Algunos de ellos se conectarán a redes sociales, correos electrónicos, quizás incluso a la página de su banco para confirmar depósitos. Decenas de operaciones *online* ocurrirán sin que nadie sepa que a pocas mesas de distancia está sentado un experimentado *hacker*, que además de tirar páginas es capaz de obtener datos personales y financieros.

"¿Existen buenos *hackers* en México? ¿Cómo sabré cuando esté frente a uno de ellos?", le pregunté meses antes de ese jueves de café a un experto en seguridad informática. "Que te muestre lo que sabe hacer", respondió. Ese encuentro, que justamente valía para observar las habilidades de quien ahora recomponía la página vulnerada, parecería sencillo de lograr, pero resultó no ser así. En nuestro país apenas existen un puñado de *hackers* como Dan, quien vive alejado del ajetreo de la ciudad de México, y que ha pasado de adolescente curioso a especialista en informática. Por años estos anónimos navegantes de la red, concebidos como arrogantes y muy inteligentes, han sido etiquetados como delincuentes, a eso se suma que hoy corren el riesgo de despertar el interés de grupos que quieren aprovechar sus conocimientos para cometer crímenes en el mundo virtual y real.

**45,1 MILLONES DE USUARIOS MEXICANOS NAVEGAN LA RED DIARIAMENTE. PARA PROTEGERLOS DE ATAQUES Y ROBO DE INFORMACIÓN, EXISTEN SÓLO 200 AGENTES EN EL PAÍS.**

Meses antes de conocer a Dan yo entendía de seguridad en informática tanto como sabe de biología cualquier estudiante de arte promedio, es decir: casi nada. Para entrar en contacto con él y otros *hackers* busqué por meses a expertos en la materia, me reuní con gerentes de firmas famosas de antivirus, charlé con abogados y víctimas que no han encontrado solución a un ataque informático que creían lejano; perseguí a funcionarios de alto nivel y conversé con uno de los pocos policías cibernéticos que existen en nuestro país. No obstante sabía que para entender que hoy los 45,1 millones de cibernautas de nuestro país navegan a su suerte en internet tenía que encontrar a quienes viven en las trincheras, aquéllos que habitan a la sombra de la red. Conocerlos me permitió ver la dimensión real de la ciberdelincuencia y los delitos informáticos, y algo incluso más allá: los malhechores informáticos operan en México gracias al estado de anarquía en materia de seguridad cibernética.

## BUSCADOR DE AGUJEROS

La historia de M-byT3 es la de quienes han explorado vulnerabilidades prácticamente desde que nuestro país se conectó a internet por primera vez hace 25 años. Por entonces daba sus primeros pasos como programador y encontró un agujero en un sistema informático de una importante empresa automotriz. A pesar de su entonces corta edad, el joven hurgó entre información confidencial con la destreza de un maestro; navegó por cientos de documentos clasificados como datos de empleados, detalles de nómina, bases de datos de clientes con información bancaria y secretos industriales por los que más de uno hoy estaría dispuesto a pagar mucho en el mercado negro. No obstante M-byT3 dice que escribió el tipo de vulnerabilidad y se fue sin dejar rastro, "como hacen los verdaderos *hackers*". Más tarde les llamaría por teléfono a los encargados del sistema para alertarlos, pero nunca le hicieron caso y la puerta se quedó abierta por mucho tiempo.

En ese entonces M-byT3 era apenas un curioso adolescente capitalino sin otra intención más que probar sus habilidades para meterse donde no lo llamaban. Han pasado muchos años desde aquella primera gran incursión ilegal al sistema de la empresa automotriz, la primera de muchas más que vendrían, según me cuenta en su residencia, una suerte de búnker que cumple con todos los clichés: se trata de una deteriorada casona de la ciudad de México, donde una impresionante iMac de 27 pulgadas descansa sobre un enorme y oscuro comedor que seguramente vivió mejores épocas. Junto a un cenicero rebosante de colillas M-byT3 enciende otro cigarrillo y mira de reojo la pantalla como si descubriera allí dentro algo que nadie más ve. Por un momento la casa (que M-byT3 solicitó no localizar geográficamente) me recuerda a la que Carlos Fuentes describió en *Aura*: una luz tenue de tarde apenas se filtra a través de los vidrios polvosos de las ventanas, paredes de yeso a punto de desprenderse, puertas de metal negras que chillan al abrirse. Ahí me asegura que nunca nadie lo ha buscado, que desde que comenzó a

**MÉXICO ES UNO DE LOS PAÍSES CON MÁS DELITOS INFORMÁTICOS EN EL MUNDO. EN 2012 LOS ATAQUES CIBERNÉTICOS AUMENTARON 40 POR CIENTO RESPECTO A 2011.**

meterse donde nadie lo llamaba, a finales de la década de los ochenta, jamás se sintió intimidado por autoridad alguna ni de México ni de otro país, pero aclara que siempre fue muy precavido.

Con el paso del tiempo, y tras interminables noches sentado frente a su Commodore modificada, y después con una Texas Instruments –con las que aprendió programación muy básica a los ocho años– en la habitación de la casa de sus padres, M-byT3 se convirtió en uno de los contados especialistas del *underground* nacional capaz de vulnerar una red sin ser detectado. Nadie nunca supo de sus intrusiones porque fue lo suficientemente cauteloso para no dejar rastro, justo como lo hace ahora al pedirme que lo llame con un mote para guardar su identidad. En aquellos primeros años sabía perfectamente que estaba cometiendo actos ilícitos, aunque en ese momento no se consideraban delitos informáticos. Fue hasta 1999 que las intrusiones de *hackers* y *crackers* (estos últimos considerados malintencionados) se incluyeron en el Código Penal Federal, según me aclaró en su oficina del sur del Distrito Federal Alberto Nava, un destacado investigador en derecho penal y autor del libro *Delitos informáticos*.

No obstante, frente a la pila de cajetillas de cigarros y de tazas con café seco, M-byT3 me cuenta que el peligro no necesariamente viene de la persecución de la ley. Me dice que recientemente el crimen organizado le ha pedido asesoría para instalar redes de comunicación cifradas, prácticamente imposibles de penetrar. "Un día –cuenta mirando de reojo sus servidores instalados en Europa del Este– una camioneta se detuvo junto a mí mientras iba a la tienda. Me preguntaron que si yo era (...); les dije mintiendo que no. Aun así me pidieron que los acompañara. Una vez arriba de la camioneta me volvieron a preguntar si yo era la persona a la que buscaban, que estaban muy interesados en que colaborara con ellos. Afortunadamente no llevaba ninguna identificación, les dije una y otra vez que yo no era esa persona. Me creyeron y me dejaron ir". Aquel encuentro con el crimen organizado se repitió en otra ocasión. Una vez más se volvió a negar.

## TODO MENOS NERD

Dan y M-byT3 son todo menos adolescentes jugando al ladronzuelo. Ambos superan por varios años las tres décadas de edad y están lejos de la estereotípica imagen del *nerd* con que se ha pintado a los especialistas en informática. M-byT3 tiene pareja, descendencia y su propio negocio que lo hace pasar horas frente a la computadora. Los dos hoy se dedican a proteger sistemas de importantes empresas que en su mayoría han sufrido fuertes ataques a sus sistemas. Son los perfectos guardianes.

En nuestros encuentros Dan y M-byT3 insistieron en que en un país como México, en materia de informática, "la mejor defensa es el ataque". La frase no es gratuita: actualmente estamos clasificados por organismos como la Organización de los Estados Americanos (OEA) como uno de los países con más delitos informáticos a nivel mundial. Según esa institución, en 2012, los ataques cibernéticos en México aumentaron en 40 por ciento respecto al año anterior, siendo la denegación de servicio (DDoS) –el ataque que llevó a cabo Dan en el café–, la vandalización de páginas web y los ataques de secuencias de comandos en sitios cruzados (XSS) e inyecciones SQL los más recurrentes. Sin dejar de mirar de reojo su computadora, y con el tono engreído de quien está seguro del conocimiento, M-byT3 me pregunta: "¿Sabes cuál es el verdadero problema del *hacking* en México? Que no hay *hacking*".

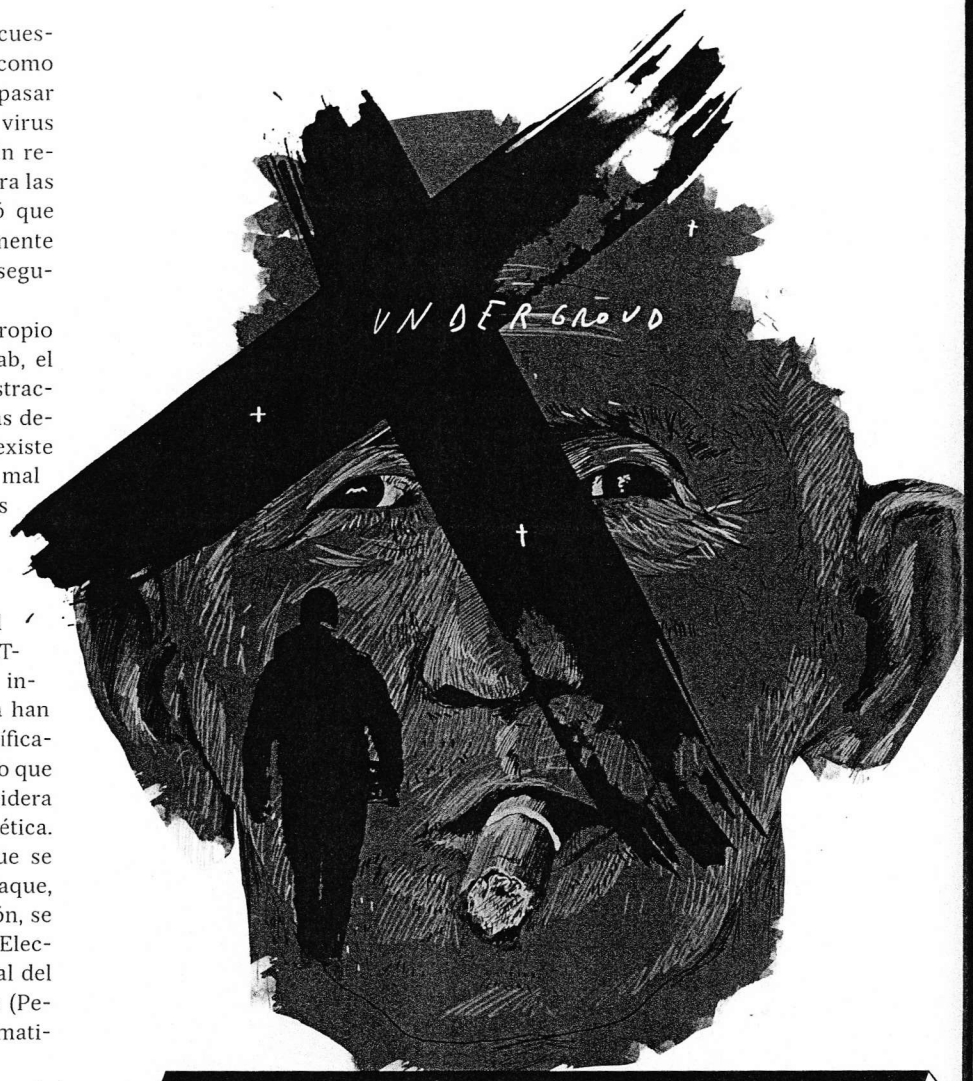
aseguró que el *cyberbulling* y los secuestros de computadoras personales, como el de quien recientemente se hacía pasar por la Policía Federal a través de virus que bloquean la máquina, seguirán representando un dolor de cabeza para las autoridades; sin embargo aseguró que estas amenazas no están remotamente cerca de representar un riesgo a la seguridad informática del país.

Al respecto, según me dijo el propio Roberto Martínez de Kaspersky Lab, el verdadero problema está en la sustracción de información personal y a las dependencias de gobierno. Además existe el riesgo de que algún especialista mal intencionado o a sueldo ataque las infraestructuras públicas, también conocidas como infraestructuras críticas del país.

Durante nuestra conversación el propio Fernando Fuentes del CERT-MX aceptó que algunos sistemas informáticos del estado mexicano ya han recibido ataques de *software* específicamente diseñado para este fin, un acto que en el ámbito internacional se considera como hostilidad de guerra cibernética. Entre los sistemas de gobierno que se encuentran más expuestos a un ataque, que pondrían en riesgo su operación, se encuentran la Comisión Federal de Electricidad (CFE), la Comisión Nacional del Agua (CNA) y Petróleos Mexicanos (Pemex), al contar con sistemas automatizados.

Además de la venta de drogas, armas y hasta la contratación de asesinos a sueldo a través de internet, otra gran preocupación es la pornografía infantil: actualmente México ocupa el primer lugar en producción y distribución de estos contenidos. Incluso la propia Coordinación para la Prevención de Delitos Cibernéticos cuenta con una oficina especializada en este ámbito. Según M-byT3 el problema de México es que no hay un plan nacional de seguridad informática. "Quizá los únicos que se han preocupado por sus sistemas en los últimos años son los bancos, y eso con sus reservas", sostiene.

Sobre la revelación del caso de espionaje masivo de Estados Unidos, por parte del ex operador de la CIA Edward Snowden, asegura que el espionaje industrial en nuestro país está a la orden del día, "sólo hay que dar una mirada a lo que venden en la red empleados descontentos que al ser despedidos de su trabajo se llevan las bases de datos de sus empresas en una memoria USB".




"¿QUIEREN QUE DEJEN DE ESPIARLOS? –PREGUNTA EL *HACKER*– DEJEN DE USAR SERVICIOS GRATUITOS COMO GMAIL Y FACEBOOK".

"¿Quieren que dejen de espiarlos? –pregunta el *hacker*– Dejen de usar servicios gratuitos como Gmail y Facebook. No importa dónde estén, las políticas de esas empresas les permiten entrar a sus cuentas porque sus servidores están en Estados Unidos (gracias a una ley conocida como Patriot, creada después de los ataques del 11 de septiembre). El problema real de internet es que la gente quiere todo gratis", sentenció la última vez que nos vimos en un café cercano a su casa de la ciudad de México. Aunque abogados y las autoridades me lo negaron una y otra vez , M-byT3 y Dan insistieron en que los usuarios de México "están prácticamente a su suerte" en materia de seguridad informática en este momento. "Debemos desconfiar de todo lo que no esté cien por ciento acreditado en internet", un lugar que bien podría haber descrito el filósofo político y revolucionario francés del siglo XIX Pierre-Joseph Proudhon como un sitio sin amo ni soberano.

# GQ MÉXICO

GENTLEMEN'S QUARTERLY

## LA HISTORIA REAL DE CÓMO FACEBOOK ATRAPÓ A INSTAGRAM

## AUTOS JAPONESES
EL PODER DE LA FUERZA FLEXIBLE

## LOS HOMBRES MEJOR VESTIDOS DE MÉXICO 2013

## LOS TRES MAGNÍFICOS DE LA NFL EN ESTA TEMPORADA

## ATUENDOS BÁSICOS PARA ENTRAR A LA OFICINA Y SALIR DE ELLA

# ANA * BRENDA
COMO NUNCA LA HABÍAS VISTO (Y COMO QUIZÁ NUNCA LA VUELVAS A VER)

+

## EL EMBATE DE LOS ROBOTS
TE MOSTRAMOS LOS MÁS INNOVADORES

ESPECIAL
## MÉXICO SUSTENTABLE
LOS PROYECTOS QUE BATALLAN CONTRA LA DEPREDACIÓN DEL PAÍS

ANA BRENDA FOTOGRAFIADA POR **TITO TRUEBA**

WWW.GQ.COM.MX
OCTUBRE 2013
MÉXICO $ 42.00

09
7 12744 61022 2