CIENCIA Y TECNOLOGÍA

‘Si vis pacem’, define ciberguerra

El Ciudadano · 6 de abril de 2011

Los gobiernos exageran sobre la ciberguerra, para usarla como excusa en su afán de control del ciberespacio. Este fue el hilo conductor de la charla del respetado experto en seguridad informática Bruce Schneier, en la "Black Hat Europa".

Barcelona ha acogido esta convención, considerada entre la élite de los encuentros mundiales de *hackers*. La conferencia del norteamericano Schneier fue la estrella de la "Black Hat", que según la organización ha reunido a 500 personas.

"A pesar de todo el ruido que hacen los medios, aún no se ha visto ningún ejemplo claro de ciberguerra", aseguró **Schneier**, quien recordó ciberataques como los de 2007 contra **Estonia**, en los que jamás quedó claro si era un país el atacante o un adolescente con tiempo libre. Además, aseguró: "No existe una definición de qué es ciberguerra, de cómo és, cómo empieza o cómo acaba".

Schneier explicó haber participado en mesas redondas sobre este tópico, junto a jefes de la **Agencia de Seguridad Nacional** norteamericana y altos cargos de aquel país, quienes "exageraban usando como ejemplo ataques de los que jamás se supo el autor". Aún así, remarcó que cada vez se están viendo más tácticas que sólo un país podría llevar a cabo, como el espionaje al **Dalai Lama** y a disidentes chinos por parte de **China**, o virus contra centrales nucleares iraquíes, creados posiblemente en **Israel** y **EEUU**.

Ante estos ataques, aseguró Schneier, "la defensa es muy difícil porque no sabes quién ni por qué te están atacando: ¿Son espías? ¿Crimen organizado que quiere extorsionarte? ¿Un gobierno? ¿Unos críos?". Todos pueden usar las mismas herramientas, disponibles en la red, y las mismas tácticas, como el sabotaje, robo de información o espionaje. "¿Y a quién llamas? ¿A la policía? ¿A tus abogados?".

Schneier, apodado el **Chuck Norris** de la seguridad informática por su mente implacable, desplegó esta vez pocas afirmaciones tajantes y muchos interrogantes. Afirmó que cada vez más países están creando "cibercomandos" en sus ejércitos, sin tenerlo muy claro: "¿Dónde actuarán? ¿En la espina dorsal de la red o en determinadas aplicaciones? ¿Cómo sabrán cuándo un ataque es real y cuándo el enemigo es civil o militar? ¿A quién defenderán, a las corporaciones, a los individuos o sólo a los estados?".

Schneier destacó el interés que muestran los gobiernos por denostar el anonimato y espiar a su ciudadanía en nombre de la ciberguerra. Explicó que en el caso de **Gmail** no habría problema, ya que los mensajes se guardan en claro en los servidores de **Google**, pero otras comunicaciones, como las llamadas de **Skype**, van cifradas. Y se preguntó: "¿Habrá que descifrarlas para que puedan espiarnos? ¿Tendremos que cambiar **Internet** para que ellos puedan hacer la guerra, tendremos que ponerles un botón rojo?".

Otro punto delicado es quién se encarga de la seguridad de la espina dorsal de Internet. De momento está a cargo de las empresas propietarias de estas redes, que dan más o menos seguridad a lo que según ellas tiene más o menos valor, algo erróneo según Schneier: “El mercado no puede defender Internet, deben hacerlo los gobiernos marcando cómo se aseguran estas infraestructuras”.

El experto sugirió que los ataques vistos hasta ahora deberían llamarse “*hacking* políticamente motivado” y que, si se llegase de verdad a la ciberguerra, los gobiernos tiene ante ellos un largo camino de reflexión: “¿Habrá que firmar tratados y marcar qué es juego limpio? ¿Un estado puede decir a una compañía de teléfonos qué debe bloquear o qué protocolos usar? ¿Es lícito que China o EEUU estén sembrando de bombas lógicas el ciberespacio?”. Schneier acabó la charla promocionando su nuevo libro.

SOMBREROS LLENOS

La llaman *Black Hat* (Sombrero negro), pero es un encuentro de “*white hats*” (sombreros blancos) sin corbata. En la jerga, un “black hat” es un hacker malvado, frente al “white hat”, el hacker profesional, que trabaja en una empresa de seguridad informática. Entre 850 y 1.650 euros la entrada, por dos días de charlas sobre lo más caliente en su campo. Boyante negocio, si no el de la seguridad, el de este tipo de encuentros, donde además se ofrecen cursos con precios que oscilan entre los 1.500 y 3.000 euros.

La Black Hat nació en 1997 en Estados Unidos, como un encuentro con contenidos más serios que la mítica y festiva convención de hackers DefCon. Ambas se celebran en agosto, en **Las Vegas**, una después de otra, y ambas son obra del hacker **Jeff Moss**. Hace once años arrancó la versión europea de la Black Hat, en **Amsterdam**, hasta que en 2010 se trasladó a Barcelona. A pesar del tiempo transcurrido, la inmensa mayoría de asistentes siguen siendo hombres.

Entre las charlas de este año han destacado la securización de aplicaciones web; cómo defenderse ante bombardeos de denegación de servicio, como los que lanzó Anonymous contra diversas empresas a raíz del bloqueo a **Wikileaks**; el uso de la computación en nube para romper claves de cifrado y lo que se tercie, o el análisis forense de virus como **Stuxnet**, para saber de dónde vienen. El madrileño **Raúl Siles** ha sido el único español que ha dado un charla en esta Black Hat, donde el inglés era lengua oficial.

Por **Mercè Molist**

http://grn.es/

Fuente: El Ciudadano