



## Todos cifran menos nosotros

El pasado mes de enero se produjo cierto revuelo por la noticia<sup>1</sup> aparecida en el portal ZDNet Australia en la que se decía que un ex criptoanalista y traductor de árabe de la USAF<sup>2</sup> y de la NSA, había publicado en su *blog*<sup>3</sup> una sucinta revisión de la nueva herramienta criptográfica dirigida a los Jihadistas de Al Qaeda.

Según ese autor, el software en cuestión se autodenomina "Mujahedeen Secrets 2", y pone de manifiesto un ciclo de desarrollo de software con una considerable sofisticación entre versiones. Esta nueva versión incluye el cifrado y autenticación automática de mensajes, el cifrado de ficheros, la creación y verificación de firmas digitales y el borrado proactivo de ficheros. Lo más curioso de esta noticia es que viene a confirmar lo que cualquiera puede imaginar: que al igual que otros ejércitos, delincuencia internacional, fuerzas de resistencia o insurgencia, movimientos anti totalitarios, etc., los cruzados islamistas también tienen herramientas para proteger sus comunicaciones. No hacerlo sería un riesgo no asumible cuando se juega a la guerra.

Llegados a este punto, podríamos hacer la misma pre-

**Son varios los indicios de que la criptografía sigue siendo muy útil en escenarios bélicos actuales, y no es de extrañar ya que lo fue en otros pretéritos; sin embargo, la sociedad civil, la Sociedad de la Información, sigue sin protegerse. Quizás esto se deba a que muchos no ven enemigo del que protegerse, pero puede ser que sea esa misma sociedad su peor enemigo.**

portátiles se "pierden" con informaciones detalladas sobre instalaciones críticas o sobre planes de respuesta en casos de emergencia, pero es inexplicable cómo pueden ocurrir este tipo de "accidentes". La proliferación tecnológica está haciendo que se recolecten cada vez más y más precisos datos sobre los

En el mencionado artículo se informa de que el Comisario británico de interceptación de las comunicaciones acaba de revelar que casi 800 organismos públicos presentaban cerca de 1.000 solicitudes *diarias* para poder obtener "datos sobre las comunicaciones", que incluyen la intervención de teléfonos, los

antes no se toman medidas realmente eficaces para proteger los datos que genera y utiliza.

### Exigencia de medidas de seguridad

Aunque afortunadamente no nos movemos en un escenario bélico, sí debemos exigir niveles de seguridad equivalentes a los que se utilizan en los escenarios bélicos y de confrontación. En una guerra suele haber dos o tres bandos enfrentados con capacidades más o menos equivalentes—al menos mientras dura la contienda—, pero en la

***El propio funcionamiento de la Sociedad de la Información necesita y genera la recolección y estructuración de datos esencialmente privados, y quizás dicha sociedad de la información no pueda avanzar sin proceder de este modo, pero debería prohibirse su avance si antes no se toman medidas realmente eficaces para proteger los datos que genera y utiliza.***

ciudadanos, sus actividades y sus organizaciones.

En un artículo reciente<sup>4</sup>, Timothy Garton Ash<sup>5</sup> comentaba cómo la capacidad fisgona del estado británico está completamente descontrolada y como él *prefería seguir siendo más libre aunque eso pudiese incluso*

historiales de llamadas, el correo electrónico, las visitas a páginas web, etc.

Dejando para otra ocasión la conveniencia o no de que exista esa capacidad de control sobre la población en aras de una muy cacareada y poco verificable "seguridad", también

vida cotidiana siempre está el individuo sólo frente al mundo, y es tal desproporción lo que hace que los derechos del individuo siempre sean atacados y pisoteados por la mayoría. Aunque en la Sociedad de la Información no hay una guerra declarada, sí hay una agresión esencial a los individuos y a las minorías que emana de lo abismal de la diferencia entre las partes.

A menos que se tomen las medidas necesarias para proteger la confidencialidad, la integridad y la autenticidad de los datos personales y/o colectivos será mejor seguir siendo libre aunque eso pudiese incluso significar vivir en la periferia de la Sociedad de la Información.

Al *downtown* de esa futura Sociedad de la Información sólo merece la pena llegar si uno va con chaleco antibalas y con todos los derechos de su parte. ■

***A menos que se tomen las medidas necesarias para proteger la confidencialidad, la integridad y la autenticidad de los datos personales y/o colectivos será mejor seguir siendo libre, aunque eso pudiese incluso significar vivir en la periferia de la Sociedad de la Información.***

gunta pero en un escenario distinto: ¿es un riesgo asumible la no protección de la información en la sociedad civil? La respuesta es un tajante **No**. Sería injusto hacer más sangre con la pérdida de CDs conteniendo los datos privados de 25 millones de contribuyentes en el Reino Unido, o por el hecho de que ciertos

*significar vivir menos seguro*. En uno de sus libros, Garton cuenta las peripecias de la Seguridad del Estado de la antigua Alemania del Este, la Stasi, para vigilarle cuando hace 30 años llegó a aquel país y cómo, según ese autor, hoy en día a los ciudadanos de la Alemania del Este se les espía mucho menos que a los del Reino Unido.

debemos tener en cuenta que el propio funcionamiento de la Sociedad de la Información necesita y genera esa recolección y estructuración de datos esencialmente privados.

Quizás la sociedad de la información no pueda avanzar sin proceder de este modo, pero debería prohibirse su avance si

<sup>1</sup> Ver <http://www.zdnet.com.au/news/security/soa/Jihadists-get-world-class-encryption-kit/0,130061744,339285480,00.htm>

<sup>2</sup> USAF = United States Air Force

<sup>3</sup> Ver "Brave New World of Infosec" en [http://blogs.csoonline.com/blog/jeff\\_bardin](http://blogs.csoonline.com/blog/jeff_bardin)

<sup>4</sup> Ver [http://www.elpais.com/articulo/opinion/Stasi/britanica/elpepiopi/20080205elpepiopi\\_4/Tes](http://www.elpais.com/articulo/opinion/Stasi/britanica/elpepiopi/20080205elpepiopi_4/Tes)

<sup>5</sup> Timothy Garton Ash es catedrático de Estudios Europeos en la Universidad de Oxford y miembro de número de la Hoover Institution en Stanford. Escribió sobre su experiencia con la Stasi alemana en el libro titulado *The file: A personal history* (Random House Publisher, 1997. ISBN-10: 0-679-45574-4). Ver [http://en.wikipedia.org/wiki/Timothy\\_Garton\\_Ash](http://en.wikipedia.org/wiki/Timothy_Garton_Ash)

**JORGE DÁVILA MURO**  
Consultor independiente  
Director  
Laboratorio de Criptografía  
**LSIIS – Facultad  
de Informática – UPM**  
[jdavila@fi.upm.es](mailto:jdavila@fi.upm.es)