Technology. Tinker, tailor, hacker, spy. Who is benefiting more from the cyberisation of intelligence, the spooks or their foes?

Enviado por David Aguilar en Vie, 12/02/2016 - 11:27
Cita:

The Economist [2016], "Technology. Tinker, tailor, hacker, spy. Who is benefiting more from the cyberisation of intelligence, the spooks or their foes?", *The Economist*, London, 12 de noviembre, http://www.economist.com/news/special-report/21709773-who-benefiting-mor... [1]

Fuente:
The Economist
Fecha de publicación:
Sábado, Noviembre 12, 2016
Revista descriptores:
Competencia mundial. Disputa hegemónica [2]
Formas de la guerra [3]
Fronteras del capital [4]
Relaciones entre empresas estados y sociedad [5]
Sujetos de la guerra [6]
Tecnologías militares - tecnologías de uso dual [7]
Tema:
Las agencias de seguridad y el desarrollo de tecnologías de espionaje
Idea principal:

El internet ha cambiado todo. Se invierten millones de dólares al año en equipos conectados a la red, teléfonos, infraestructura y software. Los paquetes de datos ya no viajan en una línea dedicada para ello, sino que toman la ruta más conveniente en el instante, borrando la distinción entre las comunicaciones nacionales y extranjeras.

Se afirma con razón que este nuevo mundo presenta innumerables oportunidades para la vigilancia. Todo el mundo utiliza el mismo hardware y software, por lo que si alguien puede descifrar un dispositivo, puede hacer lo mismo con otros dispositivos similares en cualquier lugar.

Saber quién se comunica con quién es casi tan revelador como lo que se dicen. En una técnica llamada *contact chaining* las agencias utilizan información “semilla” – el número de teléfono o el correo de una conocida “amenaza”– como un selector para rastrear sus contactos y a los contactos de sus contactos. Una explosión de actividad puede ser señal de un ataque.

En 2015 el *contact chaining* permitió al GCHQ (Government Communications Headquarters) de Inglaterra, identificar una célula terrorista que fue desmantelada horas antes de que realizara su ataque.

Las posibilidades técnicas para la obtención de información son infinitas. Ahora las agencias de seguridad no sólo hacen más, sino que también gastan menos. Sin embargo, las agencias sólo tienen la capacidad de examinar una pequeña fracción de lo que está disponible. La NSA (National Security Agency) manipula el 1.6% de los datos que viajan a través de internet y selecciona sólo en 0.025% para su revisión.

Los datos son cada vez más difíciles de rastrear. Algunos protocolos dividen los mensajes de tal forma que pasan a través de diferentes redes. Otros asignan direcciones IP de forma dinámica, con lo que ésta puede cambiar muchas veces en una sola sesión, o se puede compartir entre muchos usuarios, lo que complica la identificación.

El cifrado, que protege la privacidad de algunas comunicaciones, ha beneficiado a algunos criminales y terroristas, por lo que algunos jefes de inteligencia han tratado de frenarlo, lo que sería poco práctico, ya que los programas de cifrado se desarrollan fuera de América y Europa, y hay poco que las autoridades puedan hacer al respecto. También sería poco inteligente, ya que al crimen organizado y los estafadores nada les gustaría más que un cifrado débil o nulo.

Existen también defectos en el software que los criminales cibernéticos utilizan para entrar a una máquina. Los más preciados son las llamadas vulnerabilidades de día cero (los ingenieros de software tienen cero días para escribir un parche que arregle el defecto).

Hubo un momento en que las limitaciones de las agencias eran técnicas y económicas ya que los códigos eran difíciles de romper y costosos de implementar. En una era tecnológica barata es difícil saber lo que la tecnología es capaz de lograr, por lo que las restricciones sobre ello deben ser legales y robustas.

Datos cruciales:

Se observa una gráfica de las políticas antiterroristas de Estados Unidos con dos líneas que muestran el porcentaje de ciudadanos estadounidenses que opinan que se ha ido muy lejos en la restricción de las libertades civiles y los ciudadanos que opinan que no se ha llegado suficientemente lejos para proteger el país.

Junto a la gráfica anterior se muestra otra del nivel de aceptación del monitoreo de las comunicaciones de los ciudadanos americanos, ciudadanos de otros países, líderes americanos, líderes en otros países y sospechosos de terrorismo.

Nexo con el tema que estudiamos:

El desarrollo tecnológico aplicado a el espionaje de comunicaciones se ha desarrollado bastante, sobre todo después de los ataques del 11 de septiembre de 2001 en Estados Unidos. Ahora los ataques informáticos y las respuestas a los mismos son cada vez más sofisticados.

Lo más importante es que el desarrollo tecnológico, sea por parte de gobiernos o de particulares,

siempre tiende a socializarse, y la aparición de sistemas tan sofisticados puede llegar a ser utilizada tanto por las agencias de seguridad como por los criminales cibernéticos, lo que genera inquietud sobre los alcances que esto puede tener en la vida cotidiana de la sociedad actual. En todos los casos, en el sector civil y en el militar, se crean nuevos campos de valorización intentando revitalizar al capitalismo decadente.

Otro ejemplo de la centralidad de la tecnología y de sus creadores, así como de la importancia de conocerlas y llegar a dominarlas.

Links
[1] http://www.economist.com/news/special-report/21709773-who-benefiting-more-cyberisation-intelligence-spooks-or-their
[2] http://let.iiec.unam.mx/taxonomy/term/12
[3] http://let.iiec.unam.mx/descriptores-let/formas-de-la-guerra
[4] http://let.iiec.unam.mx/taxonomy/term/18
[5] http://let.iiec.unam.mx/taxonomy/term/20
[6] http://let.iiec.unam.mx/descriptores-let/sujetos-de-la-guerra
[7] http://let.iiec.unam.mx/descriptores-let/tecnolog%C3%ADas-militares-tecnolog%C3%ADas-de-uso-dual