

Internet y nuevas tecnologías

ROBERTO PLÁ
Coronel del Ejército del Aire
<http://robertopla.net/>

INTERNET

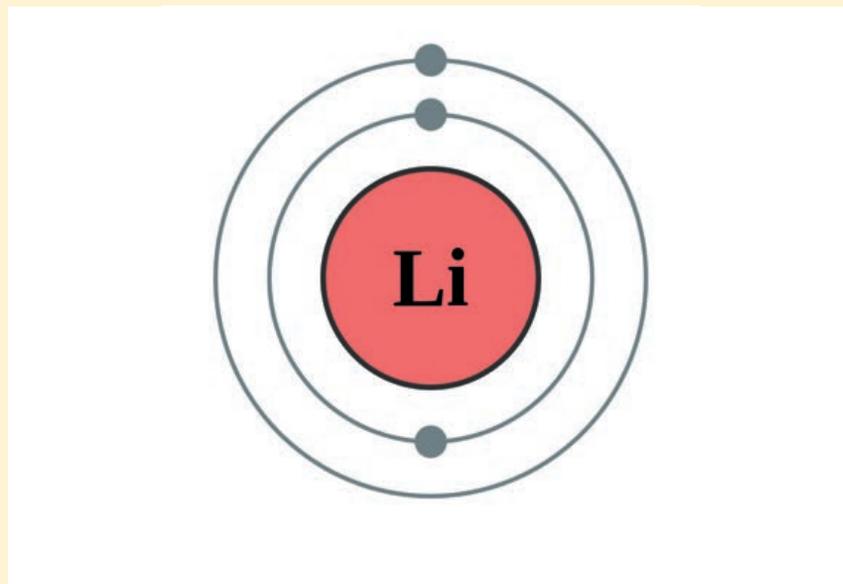
UN SIMPLE ANUNCIO

Sin duda alguna, los anuncios de compra y venta son uno de los tipos de contenidos más interesantes de la red; o al menos, de los más visitados si no tenemos en cuenta las páginas dedicadas al sexo. Tanto si te quieres comprar un teléfono nuevo, una mochila o vender la olla a presión programable que nunca usas, los anuncios te proporcionan información fiable de los precios del mercado o puedes encontrar donde se vende algo de lo que quieres comprar en cualquier parte del mundo.

Desde los sitios de subastas como el conocido eBay, las webs de anuncios de gangas o tesoros de segunda mano a las webs de gigantes como Amazon o Ali-Exprés la red es un inmenso zoco donde puede encontrarse de todo. ¿De todo? Sí, realmente. Por eso los servicios de inteligencia ven este inmenso mercado como una fuente de inteligencia abierta. Solo hay que mirar con ojos curiosos para encontrar un anuncio de venta de Litio 6. Esta “piedrecita” es un metal alcalino, de color plateado y que se oxida rápidamente en el aire o el agua, es el metal y elemento sólido más ligero. Resulta sumamente útil en aleaciones conductoras del calor, en baterías eléctricas como las famosas baterías de polímero de litio y, hasta sus sales se usan para el tratamiento del trastorno bipolar.

Sin embargo no son sus usos en psiquiatría lo que interesa a los servicios de inteligencia. Resulta que el Litio 6 tiene la capacidad de convertir fácilmente una bomba atómica de las normalitas, en una bomba de hidrógeno.

Según publicó el New York Times a principios de abril, cuando apareció en la red un anuncio online ofreciendo la posibilidad de comprar diez kilos



de Litio 6 al mes, para entregar en el puerto chino de Dandong, los servicios de inteligencia se pusieron en marcha, para averiguar con sorpresa que el teléfono que se ofrecía como contacto en el anuncio correspondía al tercer secretario de la embajada norcoreana en Beijing.

En un momento en el que el presidente Trump está empeñado en un pulso por mostrar mayor determinación y acierto que sus predecesores para anular la amenaza coreana e impedir su acceso a la tecnología nuclear más peligrosa, el anuncio podría indicar, según los expertos, que Corea del Norte ya ha obtenido esa tecnología y que incluso tiene sobrantes de materias primas. Ni que decir tiene que son muchas y muy importantes las repercusiones de esa conclusión en como se juegan los siguientes lances de esta partida. Pero naturalmente, a cualquiera lo suficientemente desconfiado como para ser analista de inteligencia se le ocurre la pregunta evidente: ¿Se trata de un farol?. Lo único que está claro es que, para ser un simple anuncio online, ha dado bastante de sí.

CIBERGUERRA

CIBERGUERRA CONTRA ARTILLERÍA

Ya he escrito otras veces sobre la maravilla tecnológica que suponen los smartphones, tan capaces de conectarnos con nuestra familia para una llamada cariñosa, como para controlar el funcionamiento de un nanosatélite.

La popularidad de estos ordenadores de bolsillo ha hecho que se desarrollen aplicaciones para los usos más inverosímiles. La parte desagradable es que la popularidad también ha atraído a las empresas de publicidad, los recopiladores de datos para su venta a usuarios de aplicaciones de explotación de Big Data o simplemente a los fabricantes de malware con los propósitos más diversos.

Pero ¿qué pasa en la guerra? Existen smartphones especialmente diseñados para la guerra. Resistentes a los impactos físicos, al agua y la humedad, con baterías de larga duración, comunicaciones cifradas y otras características especialmente diseñadas para formar

redes seguras que permitan la circulación de información, transmisión de órdenes, geoposicionamiento o uso de aplicaciones de una forma segura sin interferencias del enemigo.

Pero estos sistemas son caros, y al fin y al cabo, cada elemento humano que participa en una contienda viene de su casa equipado de serie con un smartphone. Hoy nadie va a la guerra sin llevarse el teléfono para seguir *whasapeando* con Purita, enviarle fotos a su madre o poder seguir los resultados de su equipo de fútbol y eso sin contar el entretenimiento que supone leer los memes que nos envía ese amigo pelmazo conocedor de todas las fuentes de estupideces de la red. Y esto es malo: malo para las operaciones y malo para la seguridad.

Para empezar, un montón de información que debería permanecer discreta se convierte en pública a través de las redes sociales. Desde la ubicación o intenciones de una unidad incluido su geoposicionamiento a través de metadatos de fotos enviadas a familia y amigos en retaguardia a la difusión de imágenes que pueden llegar a contradecir, obstaculizar o destrozar la política informativa de la organización, por no hablar de su efecto sobre la moral de la retaguardia.

Pero podemos continuar por la amenaza que supone para una unidad implicada en el curso de operaciones militares, la introducción, con esos teléfonos privados, de software espía que puede dedicarse a recopilar aún más información de la que su impudente usuario envía a sus cuentas en redes sociales. Detalles como la agenda de contactos, las comunicaciones o imágenes y sonidos captados mediante el uso fraudulento de los sensores del teléfono pueden convertir a cualquiera de estos dispositivos en el mejor aliado del enemigo.

Ni que decir tiene que el uso de estos dispositivos privados para establecer una red de comunicaciones en la unidad, establecería una jerarquía y un mapa claro de su funcionamiento para uso y disfrute del enemigo de una forma casi tan cómica como las llamadas de Gila al enemigo.

Pues para dar un paso más hacia un escenario completamente surrealista imaginemos que tenemos la posibilidad de instalar una aplicación que funciona como un calculador de tiro para la pieza de artillería más popular de nuestro alegre ejército, que reduce el cálculo de los parámetros de disparo de varios minutos a quince segundos. Esto ha ocurrido en la Guerra del

Donbáss, entre Ucrania y los rebeldes pro-rusos. Los resultados han sido que si bien el conjunto de las unidades de artillería ha sufrido unas pérdidas del 50% de las piezas, las unidades dotadas con piezas del modelo D-30 de 122mm. para el que se desarrolló la aplicación, han sufrido unas pérdidas del 80% de las piezas.

Ante la sugerencia de que la aplicación pueda estar infectada con un malware que pase información directamente a las unidades enemigas que realizan fuego contrabatería, la reacción del ejército ucraniano ha sido simplemente negar la mayor. Tal cosa "no puede" haber sucedido, la distribución de la aplicación es segura y en general somos más listos que el enemigo, como ocurre siempre en todos los bandos de todas las guerras si nos atenemos a los comunicados oficiales. Pero las matemáticas son una ciencia insidiosa y tozuda y cualquiera que quiera usar la cabeza para algo más que cortarse el pelo sabe que las casualidades no existen. •

Las páginas consultadas como fuentes para estas reseñas están recopiladas en la siguiente dirección: <https://del.icio.us/rpla/raa863>

