Baterías de la ciberguerra

JORGE ELBAUM :: 27/09/2024

En ambos polos de la cadena productiva de los buscapersonas, aparecen confidentes de los servicios secretos del régimen israelí

La explosión de diferentes aparatos de comunicación acaecida hace dos semanas en El Líbano exhibe una nueva faceta de la guerra híbrida donde todas las esferas de lo cotidiano, sobre todo las vinculadas con el ciberespacio, se pueden reconvertir en aparatología bélica. Los tres mil buscapersonas (*pagers o beepers)* y la centena de *walkie talkies* que estallaron el martes y miércoles pasados fueron modificados para introducirles explosivos plásticos, pero su detonación simultánea apeló a un *software* remoto capaz de recalentar la batería para su posterior deflagración. Esta última posibilidad es la que nos interpela sobre los estándares de seguridad de los celulares y demás dispositivos informáticos, en relación con su posible voladura a distancia, incluso sin encontrarse acompañados por explosivos.

La conectividad global supone crecientes desafíos a las soberanías naciones. Dichos retos incluyen el seguimiento y monitoreo de actores políticos, militares o comunicacionales, la planificación de operaciones de espionaje sobre poblaciones enteras y la implantación de campañas propagandísticas destinadas a influir, condicionar y determinar formatos cognitivos y conductas sociales. En una primera etapa, el Mossad detectó el pedido que la empresa taiwanesa decidió otorgar a su licenciataria, la firma húngara BAC Consulting KFT, radicada en Budapest. El territorio chino de Taiwán, parte indisoluble de la soberanía de la República Popular, se comporta como socio estratégico de los EEUU, mientras que Viktor Orbán es uno de los pocos líderes europeos que defiende de forma consecuente a Bibi Netanyahu.

En ambos polos de la cadena productiva de los *buscapersonas*, aparecen confidentes de los servicios secretos del régimen israelí. El vocero del gobierno húngaro, Zoltan Kovacs, informó el jueves que los aparatos no habían sido producidos en su país y que BAC Consulting era solo "un revendedor”: los aparatos de comunicación reconvertidos en explosivos personales fueron fabricados en Israel, derivados a Budapest y luego embarcados a Beirut. El material plástico de alrededor de cincuenta gramos fue implantado junto a la batería y se lo asoció a un interruptor que se activó en forma remota.

El Mossad y la Unidad 8200 de las Fuerzas de Defensa de Israel son dos de los responsables del entramado C4ISR, sigla que refiere a las actividades de comando, control, comunicaciones, inteligencia, vigilancia y reconocimiento ligadas al ciberespacio. Los insumos provistos por ambas organizaciones fueron centrales en la detección de la solicitud presentada en octubre pasado, por parte de las autoridades libanesas de Hizbolá, a la empresa taiwanesa Gold Apollo, radicada en Taipéi.

Las plataformas a través de la cuales se llevan a cabo los procesos de vigilancia global son las mismas que se utilizan para monetizar las elecciones y aficiones individuales. Las redes sociales con las que nos comunicamos se inscriben en servidores que no controlamos y son

requeridos –llegado el caso– para sugerirnos contenidos o ubicarnos como destinatarios de determinadas visiones del mundo. Todos estos datos, ajenos a nuestro control, son insumos de esta guerra globalizada que lucha por la apropiación de las ciencias y la geolocalización de disidencias.

Para hacer más eficiente y exitosa esa confrontación bélica, se apela a la Inteligencia Artificial (IA) –que de "inteligencia" no tiene nada– para procesar de forma más veloz los datos recolectados, ofreciendo de esta manera respuestas más veloces y funcionales. Esta operación gigantesca se lleva a cabo gracias a una sistemática sustracción de la propiedad intelectual individual y pormenorizada de miles de millones de internautas, usuarios de computadoras y/o celulares.

Glenn Gerstell, actual referente de los estudios de ciberdefensa del Centro de Estudios Estratégicos e Internacionales (CSIS) y ex consejero de la Agencia de Seguridad Nacional durante el gobierno de Donald Trump, consideró en la última semana que "nuestra sensación de vulnerabilidad sobre cómo los aparatos conectados a internet pueden convertirse en armas mortales puede estar iniciándose". Su apreciación no deja en claro si se trata de una premonición o es directamente un anuncio de futuras tecnologías disponibles para la ejecución remota de oponentes.

La tecnología que usamos está cada vez más intervenida por formatos de espionaje y de operaciones encubiertas. Dado que la desconexión aparece como infructuosa e improductiva, los gobiernos deben plantearse medidas en relación con el control soberano de las infraestructuras digitales y las regulaciones institucionales de los contenidos. Eso es lo que están llevando a cabo Brasil (respecto a Elon Musk), EEUU (respecto a TiK Tok y Huawei) y la Unión Europea (en torno a Meta y Google). Para ellos –igual que para Rusia o China– la soberanía es una categoría relevante. Solo los portadores de mentes coloniales desechan sus atributos.

---

https://www.lahaine.org/mm_ss_mundo.php/baterias-de-la-ciberguerra