LA NUEVA INDUSTRIA DE LA CIBERSEGURIDAD Y LA HEGEMONÍA GLOBAL

Dr. Roberto Morales Estrella
Profesor Investigador de la UAEH

27 noviembre de 2023

Cuando se descubrió que la información era un negocio, la verdad dejó de ser importante, dijo Ryzard Kapuscinsky (, El Observador, 2023), el manejo de la información, a pesar de que es la sociedad la que la genera, su manejo y aplicación en ésta época, donde la tecnología del ciberespacio es cada vez más omnipresente, son los medios y los políticos los que la manejan, el predominio de los medios ha transformado los grandes flujos de información, en una mercancía, siendo el mercado de las ciberarmas las que determinan la interpretación y su aplicación social.

Javier Barracal lo evidencia conceptualmente al decir que "la idea de que lo tecnológico y lo científico son realidades absolutamente neutrales, puros medios indiferentes filosóficamente, que no implican unos u otros valores o significados, sino que simplemente sirven a quienes los utilizan en una u otra dirección práctica, a causa de su naturaleza o esencia de instrumentos (Mairal , 2021).

Si bien la verdad es un constructo social, ahora la construcción de lo que se acepta, obedece a intereses mercantiles, políticos y militares, convenciendo a la sociedad de lo que es bueno aunque no lo sea; para que sus acciones queden libres de responsabilidad, aunque sean exactamente lo contrario; por ejemplo la información que difundió Benjamin Netanyahu, aplicando su estrategia denominada "Hannibal" respecto a la matanza de 364 jóvenes que se localizaban en el festival de música Nova, informando que había sido Hamas, cuando fue él propio ejército israelí, el que perpetró tan atroz crimen, según lo difundieron los rotativos israelíes Haaretz y Yedioth. La información es un arma en los conflictos bélicos geopolíticos.

La acelerada carrera de la transformación digital ha propiciado una hiperconectividad, a la misma velocidad ha surgido la vulnerabilidad de toda la sociedad, frente a un fallo ya sea de hardware y/o de software, para el cual no existe ninguna herramienta tecnológica para solucionarlo, por eso se le ha dado el nombre de "día cero" (Nicole , 2022), descubierto el fallo se tiene cero días para solucionarlo.

Así como el Sars-cov-2 provocó el covid-19; el gusano denominado Stuxnet, descifrado en 2010 por Ralph Langer y especialistas bielorrusos en ciberseguridad, se le considera una Amenaza Persistente Avanzada (APT), es un malware imperceptible que identifica vulnerabilidades en los servidores (, Redacción KeepCoding, 2023).

Se ha especulado que una acumulacion de días cero en programas industriales tanto de Microsoft como de Siemens, facilitó que los espías norteamericanos e israelíes, sabotearon el programa nuclear de Irán (ob.cit), el Stuxnet fue infiltrado en las instalaciones de uranio de Irán, mediante una usb, siendo capaz de identificar los controladores lógicos programables (PLC) de los sistemas de control y supervisión industrial, provocando que las máquinas funcionaran mal.

El Stuxnet-días cero es una arma cibernética usada por los hackers para insertarse en los iPhone de forma remota, y tener acceso a todas las actividades digitales de sus propietarios, la privacidad es ya una vulnerabilidad social, puesto que el usuario no se da cuenta. Los espías chinos utilizaron el stuxnet-día cero para robar el código fuente de silicon valley.

Eduard Snowden filtró documentos de la Agencia Nacional de Seguridad (NSA) de los EEUU donde se identificaba que la agencia aplicaba el stuxnet-día cero para actividades de espionaje; hay diversos organismos que se dedican a identificar vulnerabilidades y las venden en un mercado de ciberarmas, entre esas organizaciones están Tailor Access Operation (TAO) de la NSA de los EEUU; Mandiant es una organización apoyada por China; Dragonfly es un grupo dedicado al ciberespionaje del Servicio Federal de Seguridad Ruso.

La industria de la ciberseguridad es tan amplia, como la vulnerabilidad de todos los sistemas industriales, de las organizaciones públicas y privadas, sin que se escapen las financieras, el mercado de las ciberarmas está integrado por los hackers de sombrero blanco, que generan herramientas de defensa y los de sombrero negro, que son los mercenarios cibernéticos, quienes identifican y venden las vulnerabilidades al mejor postor y los gobiernos, transformando los virus y sobre todo el stuxnet en ciberarmas, para imponer su hegemonía al interior de sus países, como en la lucha geopolítica por la hegemonía global.