Inseguridad en el cibermundo

VLADIMIR CASTILLO SOTO :: 10/03/2024

En un mundo donde la guerra no tiene límites de ningún tipo, el ciberespacio es, sin duda, uno de los campos de batalla más activos

Hoy día, buena parte de la información sensible de los Estados, empresas y personas es procesada y almacenada en medios digitales. La generación eléctrica y su distribución, la producción industrial en general, el transporte masivo, las comunicaciones, la comercialización de todo tipo de bienes y servicios, las finanzas, los repositorios de información y muchas otras actividades se operan, resguardan y controlan a través de sistemas informáticos que hacen uso permanente y masivo de las plataformas de redes, las cuales en la mayoría de los casos están enlazadas con internet.

En un mundo donde la guerra no tiene límites de ningún tipo, el ciberespacio es, sin duda, uno de los campos de batalla más activos. La militarización del ciberespacio y su uso con fines de agresión militar tiene múltiples objetivos, desde la captura de información estratégica de la fuerza armada y gobierno del enemigo, pasando por campañas de desinformación que generen pánico, zozobra e incertidumbre entre la población, así como afectaciones a los servicios de comunicación, suministro de energía, agua y gas, entre otros, que perturben la vida de la población civil y las operaciones militares. Hackers y técnicos especialistas en hardware y software son fundamentales para actuar como operadores en este tipo de guerra, tanto para planificar y llevar a cabo ciberataques como para prevenirlos.

EEUU tiene grandes ventajas en el área de la tecnología digital, las cuales usa a su antojo y siempre en pro de sus intereses, militares, políticos y/o económicos.
Muchas de sus empresas tecnológicas han logrado conseguir posiciones monopólicas o cuasi monopólicas en diversas áreas del mundo digital. El sistema operativo que está instalado en la gran mayoría de las computadoras de escritorio y portátiles en el mundo pertenece a una empresa estadounidense, este sistema es manipulable de múltiples maneras, sobre todo por sus creadores y por los organismos del gobierno norteamericano, mucho más que por los hackers independientes o las agencias de otros gobiernos. Muchos programas antivirus, los más populares programas de manejo y almacenamiento de correo electrónico, así como las principales plataformas de redes sociales son propiedad de empresas estadounidenses las cuales, después del 11S de 2001 y la aprobación de la Ley Patriota, están obligadas a entregar a su gobierno toda la información requerida de los usuarios y clientes o permitir a las agencias gubernamentales el accionar sobre el software y el hardware de sus empresas para facilitar la interceptación o extracción de todo tipo de información privada.

El gobierno de EEUU ha espiado a millones de personas que utilizan redes de telefonía móvil y redes sociales desarrolladas por empresas estadounidenses. Según Edward Snowden, la Agencia Nacional de Seguridad (NSA por sus siglas en inglés), ha tenido acceso a los servidores de datos de esas empresas, con o sin su consentimiento, destruyendo la privacidad de millones de ciudadanos en EEUU y en el mundo. También han espiado a

dirigentes políticos de todo el mundo, incluidos sus socios más cercanos, como por ejemplo, la Canciller alemana Angela Merkel, otros miembros del gobierno alemán así como funcionarios franceses, suecos y noruegos, para lo cual contó con el apoyo y complicidad de los servicios de inteligencia daneses. Desde hace unos pocos días están circulando noticias, en medios absolutamente occidentales, que exponen el espionaje realizado sobre el señor Trump, candidato en el 2016, solicitado por el presidente Obama a los británicos, que asignaron la tarea a la agencia *Cuartel General de Comunicaciones Generales* (GCHQ), de espionaje tecnológico, la cual tenía experiencia en EEUU, ya que venía haciendo inteligencia, entre otros, a ciudadanos irlandeses residentes en ese país.

Por otra parte tienen el control sobre las herramientas (redes sociales, medios de comunicación y la industria cultural) y también los métodos (guerra cognitiva, guerra psicológica, guerra comunicacional) con los cuales, entre otras cosas, manipulan la conciencia social, propagan ideas supremacistas y extremistas, pretenden cambiar la historia y generan protestas antigubernamentales en aquellos países calificados de "indeseables", con el fin de cambiar sus gobiernos.

EEUU y sus socios más obedientes ratificaron la Convención sobre el ciberdelito de Budapest en 2001, propusieron el "llamado de París para la confianza y la seguridad en el ciberespacio" en 2019 y también en 2022 firmaron la Declaración sobre el futuro de Internet, todas estas propuestas son endulzadas con el lenguaje típico occidental. Libertad, equidad, derechos humanos, responsabilidad, internet libre, fiable y seguro, lucha contra las dictaduras, el terrorismo y el crimen de todo tipo son los términos repetidos en todas ellas que utilizan para tratar de imponer su mundo basado en normas neocoloniales e imperialistas. Los países del sur deben estar atentos para no dejarse entrampar en estas propuestas occidentales, que procuran mantener su capacidad de dominio, alargando la vida de la unipolaridad.

El imperialismo no tienen límites ni restricciones, por lo que utilizarán todo el arsenal que tienen a su alcance.

Es evidente, público y notorio que el gobierno de EEUU ha usado y usará todo el poder que tiene en el ciberespacio como arma de guerra en contra de todo el que se le opone, con el fin de manipularlo y tratar de empujarlo en la dirección que más le conviene, mientras además le acusa de violar la libertad, la democracia y los derechos humanos, de manipular elecciones, de robar secretos y de desestabilizar el mundo.

Es un deber de los países atacados defenderse. Prevenir y preparase para las agresiones es tarea fundamental, hacer contrainteligencia, usar sistemas operativos propios o basados en Linux, producir hardware o adquirirlo a empresas no controladas por occidente, desarrollar alternativas a sus redes sociales y otros sistemas informáticos sensibles, formar ingenieros y técnicos en el área rumbo a una mayor independencia científico-tecnológica, preparar a los ciudadanos para contrarestar las campañas de desinformación y tener buenos servicios de inteligencia son algunas de las tareas que se deben profundizar. La soberanía y la seguridad en nuestra parte del cibermundo es un componente clave que debe ser siempre atendido.

En la política y en la guerra la información hay que valorarla y protegerla tanto o más que la propia vida. Ya por el año 300 a.C., Kautilya, pensador y ministro indio planteaba la

necesidad del manejo adecuado de la información y la desinformación.
Establecía en su libro, el Arthashastra, toda una serie de medidas para proteger la información propia y recabar la del contrario así como generar campañas que le desinformaran. Espionaje, agentes encubiertos y otras tácticas son abordadas y explicadas por el autor, concluyendo que su uso adecuado puede dar grandes beneficios, así como su descuido o perdida puede acarrear grandes catástrofes, lo cual sigue siendo totalmente cierto en la era digital.

La Haine

---

https://www.lahaine.org/mundo.php/inseguridad-en-el-cibermundo