Manuel Hernández Borbolla

En el mundo, diariamente, se libra una guerra secreta en internet por el predominio del planeta. No se trata de una historia de ciencia ficción, sino, por el contrario, de un fenómeno cada vez más recurrente en los medios de información.

Se trata de la ciberguerra, un **nuevo tipo de guerra no convencional con la que se trata de debilitar al enemigo** a través de ataques coordinados en el espacio digital.

Esto, derivado del gran desarrollo de las nuevas tecnologías de la informaciónÂ en las últimas décadas, ha convertido a internet en un campo de batalla.

¿Qué es la ciberguerra?

En su libro 'Ciberguerra', Richard Clark y Robert Knake definen el término como "acciones efectuadas por una organización, nación o Estado con el propósito de **penetrar los sistemas informáticos** y redes de computadores de otra Nación-Estado, con el fin de causar **daños o interrupción** de los mismos".

Para Alejandra Morán, experta en derecho y ciberseguridad por la Universidad Nacional Autónoma de México (UNAM), la expresión refiere una disputa secreta entre grupos políticos antagónicos.

"En la ciberguerra todos los ataques se manejan a través de medios electrónicos y telecomunicaciones. Ya no son soldados disparando contra el enemigo frente a frente, ahora son **delincuentes informáticos operando desde la sombra**, en los que no se tiene ni idea de quién lo hizo, ni cuándo van a atacar de nuevo y que, además, tienen objetivos políticos y/o militares", señala la experta en entrevista con RT.

Un asuntoÂ que con el vertiginoso desarrollo tecnológico de las últimas dos décadas ha dejado de ser un asunto de escala menor para convertirse en un fenómeno de alcance global.

"Anteriormente se pensaba que los ciberataques tenían consecuencias limitadas, pero ahora se ha demostrado que los daños **han generado grandes pérdidas**, por lo cual, se considera que los ciberataques, reconocidos o no, son ya una de las armas más lesivas a los países y a los servicios públicos e información de sus pobladores", añade Morán.

Una disputa que se manifiesta de manera puntual entre las principales potencias económicas, políticas y militares del mundo.

Campo de batalla geopolítico

"El ciberespacio se ha convertido en **el quinto dominio de la guerra**, después de la tierra, el mar, el aire y el espacio. Actualmente hay una lucha muy fuerte por dominar el ciberespacio", señala Juan Pablo Salazar, investigador colombiano de la Universidad Complutense de Madrid, en entrevista con RT.

De acuerdo con el experto en derecho internacional y ciberguerra, el desarrollo de este fenómeno ha tenido diversas fases desde que surgió a finales del siglo XX, entre las que destacan:

- **La etapa temprana**

Comprende de 1994 a 2006. Durante este periodo ocurrieron algunos ataques de tintes

políticos en **Chechenia, Kosovo y Oriente Medio**. En ellos, se agredían sitios de partidos políticos o alguna autoridad estatal con el propósito de desconfigurarlos y mostrar el mensaje político del oponente. En esta etapa ocurrió un ataque contra la NASA, donde incluso la plataforma de lanzamiento de cohetes fue comprometida.

- **La etapa inicial**

Sucedió entre 2007 y 2009. El punto de inflexión se registró en **Estonia**, país que durante algunas semanas estuvo paralizado en todos sus servicios electrónicos por divergencias políticas de activistas, que lograron paralizar sistemas de gobierno y financieros mediante ataques de denegación de servicio.

- **Etapa de proliferación**

Comprende de 2010 a 2016. El punto de inflexión fueron los ataques contra **Irán**, cuando se logró detener el enriquecimiento de uranio a su planta nuclear de Natanz a través del 'malware' conocido como Stuxnet, que tomó el control de 1.000 máquinas que participaban en la producción de materiales nucleares y les dio instrucciones de autodestruirse.

Los informes especializados señalan que fue una agresión producida por EE.UU. a Irán para detener el enriquecimiento de uranio. A partir de ahí hubo ataques de un lado para otro. Irán respondió y creó una gran fuerza de ciberataques contra EE.UU. y otros países de la península arábica.

- **Etapa actual**

Pero todo cambió –refiere Salazar– a partir de los ataques cibernéticos a **Ucrania**. Esto, debido a que este tipo de actos dejaron de afectar objetivos militares o gubernamentales y comenzaron a atacar instalaciones civiles con el fin de causar afectaciones masivas en la vida diaria de las personas.

En diciembre de 2015, Ucrania sufrió un apagón masivo en el suministro de energía eléctrica en la región de Ivano-Frankivsk, dejando sin electricidad a 80.000 personas en plena

temporada de invierno.

Pero el especialista señala que fue en 2017 cuando ocurrió un punto de inflexión en la ciberguerra, con los ataques que paralizaron el aeropuerto de Kiev y provocaron paros en las líneas del transporte público, así como afectaciones en medios de comunicación rusos.

"A partir de 2017 ocurrió algo muy particular. Hasta entonces, parecía que los Estados estaban concentrados en probar las capacidades que tenían, pero no llegaban a producirse consecuencias directas en el mundo real, para la vida de las personas", explica Salazar.

Desde entonces, añade el experto, han ocurrido ataques grandes **contra el sistema financiero y criptomonedas**
, así como objetivos estratégicos que evidencian el poderío de algunas naciones que se han preparado para la ciberguerra.

"¿Qué quiere decir todo esto? Que los Estados tienen capacidades y se ha logrado un predominio del ciberespacio donde algunos países han perdido, y otros han ganado, predominio geopolítico. Los Estados tienen capacidades grandes contra cualquier objetivo, militar o bienes civiles", afirma.

El experto refiere que aunque no hay datos del todo precisos, a nivel internacional, las principales potencias en el ámbito de la ciberguerra son **EE.UU., China y Rusia**, seguidas de otros países como
Irán, Corea del Norte e Israel
. Esto, además de actores como
la OTAN y la Unión Europea
.

En contraste, los Estados latinoamericanos se encuentran muy rezagados en esta materia, a pesar de que países como **México** y **Chile** han registrado ataques de gran escala contra instituciones financieras.

Objetivos civiles

Una de las principales características de la ciberguerra actual es la manera en que algunos países y organizaciones han orientado sus objetivos **hacia instalaciones civiles**, principalmente con el fin de generar caos y desestabilización en los países atacados, como ha ocurrido con centrales eléctricas.

Pero ese es apenas uno de los muchos frentes de batalla donde se despliega la ciberguerra.

En este sentido, los expertos coinciden que en la ciberguerra **no sólo participan Estados**, sino también organizaciones de ciberactivistas, redes criminales, hackers individuales, empresas de mercenarios, vándalos digitales, sindicatos criminales y también unidades de servicios de inteligencia.

Algunas de las actividades ligadas a ciberataques en las últimas décadas son:

1. Fraude electoral
2. Espionaje industrial
3. Ruptura del mercado de valores por beneficio o diversión
4. Provocar derrames intencionales en instalaciones petroleras
5. Toma del control de la fábricas
6. Comprometer el teléfono de políticos
7. Chantaje masivo a través de las redes sociales
8. Ataque contra centrales eléctricas o hidroeléctricas
9. Centrales productoras de gas
10. Ataque contra aeropuertos
11. Sistemas de distribución y almacenaje de agua

Una situación que ha provocado que tanto los Estados como las organizaciones inviertan cada vez más recursos en seguridad informática.

Día Cero y la disputa por las telecomunicaciones

Otro factor crucial para entender los términos en que se despliega la ciberguerra es la batalla por el control de las telecomunicaciones.

"Los que detentan la infraestructura surgen como los líderes en el mundo digital, porque son quienes tienen la **propiedad de los cables submarinos**, sobre todo los tendidos de fibra óptica, además de los enlaces de microondas y satelitales", afirma Salazar.

Una situación que, en buena medida, permite entender el boicot de EE.UU. hacia la empresa china de tecnología Huawei, luego de que el presidente Trump afirmara que los teléfonos creados por la compañía eran usados para espiar a funcionarios estadounidenses.

{youtube}jtJutHO0kNU{/youtube}

"Estos activos cibernéticos se convierten en activos preponderantes de los Estados. Con la conectividad y el **despliegue** de la **red 5G**, los países que estén detrás de la infraestructura será quienes detenten el poder en el ciberespacio", agrega el experto.

Una batalla que podría conducir a escenarios catastróficos, ya que, incluso, algunos especialistas en informática hablan de que el mundo podría derivar en un ciberataque de gran escala, conocido como **Día Cero**, con el que **todos los sistemas dejarán de funcionar**, lo cual implicaría un gran apagón digitalÂ a nivel global.

"Es el gran ataque que **pondrá a nuestro mundo 'offline'**", dice Salazar.

Ataques recientes

En lo que va de 2019, las grandes potencias han intercambiado acusaciones de ciberataques y espionaje, tal como señaló EE.UU. en un informe reciente en el que califica a China y Rusia

como las mayores amenazas de ciberespionaje.

Una acusación con la que el presidente Donald Trump intentó justificar el boicot contra la empresa china Huawei.

{youtube}oU3rZepMUXg{/youtube}

En **marzo pasado ,** el presidente de **Venezuela**, Nicolás Maduro, afirmó que algunos apagones masivos en el **suministro de energía eléctrica** en su país estaban relacionados con ciberataques orquestados por EE.UU.

En **México** se descubrió una **red de noticias falsas** que buscaba afectar la imagen del entonces candidato presidencial, Andrés Manuel López Obrador, en los comicios de 2018.

Ese mismo mes, el Ministerio de Defensa de **España** **aseguró** que una "potencia extranjera" estuvo detrás de un ataque a su red informática.

En abril, el Gobierno de **Ecuador** **pidió** ayuda a Israel para protegerse por los más de 40 millones de ataques cibernéticos recibidos tras la **dete nción del activista australiano Julian Assange** , fundador de Wikileaks.

En junio, un **informe** del Equipo Técnico de Respuesta de Emergencia de la Red Informática Nacional de China señaló que la mayoría de los ataques cibernéticos contra el gigante asiático provienen de EE.UU., además de registrar un aumento de 90,8 % en el número de ciberataques respecto al año previo.

Días después, el diario **The New York Times** afirmó que el Pentágono y la Inteligencia de EE.UU. realizaron ataques masivos contra las **re**

des de suministro de energía eléctrica de Rusia
, señalamiento que fue
negado
por Trump. Un asunto que generó reacciones en Moscú, que
advirtió
que el ataque supondría un claro ejemplo de ciberguerra.

También en junio, medios estadounidenses **informaron** que Trump lanzó un ataque cibernético dirigido contra un grupo de Inteligencia con vínculos con la
Guardia Revolucionaria de la República Islámica
.

La agencia **Reuters** señaló que 'hackers' chinos intentaron sustraer secretos comerciales en ocho de los proveedores de servicios de tecnología más grandes del mundo.

El Centro Nacional de Coordinación de Incidentes Informáticos de Rusia aseguró que EE.UU. y la Unión Europea son las principales fuentes de ciberataques contra el país presidido por Vladimir Putin.

En **agosto** , el subsecretario del Consejo de Seguridad de Rusia, Oleg Jrómov señaló que EE.UU. intenta crear un mecanismo legal para culpar a otros países de realizar ataques cibernéticos sin necesidad de pruebas, con objeto de responder militarmente contra países incómodos.

{youtube}gu62eCSfBOM{/youtube}

Todos estos son acontecimientos recientes que marcan una nueva etapa en el desarrollo de la ciberguerra en la lucha por la hegemonía global.