revista pensamiento penal

¿Qué es la ciberguerra?

Por Gustavo Sain
@grsain

La **ciberguerra** es un área dentro de las agencias militares de los países que tiene como objetivo encontrar las vulnerabilidades técnicas de los sistemas o redes informáticas del enemigo para penetrarlas y atacarlas, tanto así como para extraer datos e información sensible. En este caso el ciberespacio es el campo de batalla y las armas son programas o aplicaciones informáticas. Las **tácticas** de combate son la infiltración en redes enemigas, la recopilación de datos, la interferencia de señales inalámbricas, los programas informáticos falsificados y contaminados (a partir de la instalación de "puertas traseras"), ataques a sistemas enemigos a través de virus, gusanos y bombas lógicas, entre otras. Algunas potencias en materia de ciberguerra son **Estados Unidos, China y Rusia**, mientras que en un segundo nivel se encuentran Israel y Francia. Otras naciones con capacidad para la guerra cibernética son Taiwán, Irán, Australia, Corea del Sur, India y Paquistán, entre otros.

El área de "guerra cibernética" surge a principios de los 90s en el seno de las agencias de seguridad de los Estados Unidos, donde los servicios de inteligencia comienzan a ver Internet como una potencial herramienta para el espionaje electrónico. Un nuevo concepto que adquiere significación a partir del desarrollo de este campo es el de **infraestructuras críticas de información,** también conocidos como sistemas SCADA (acrónimo de supervisión, control y adquisición de datos, en inglés). Son sistemas informáticos que hacen al funcionamiento de los servicios públicos de un país, como por ejemplo, los sistemas de gestión hidrológica, los conductos de gas, las redes de transmisión y distribución eléctrica, los sistemas eólicos, los sistemas de control medioambiental y los sistemas de control de tráfico aéreo, ferroviario o vial, entre

otros, que pueden resultar como potenciales objetivos en el marco de un conflicto bélico virtual.

Otros conceptos que hacen a la guerra cibernética son los de **atribución** y de **respuesta**. Una característica importante de este tipo de conflictividad es a diferencia de la guerra convencional, el atacante intenta ocultar su identidad para evitar represalias. Las comunicaciones se realizan en forma anónima ya que generalmente se utilizan tecnologías de encriptación para ocultar la identidad de los agresores y los ataques son producidos desde lugares públicos tales como cibers o locutorios. El anonimato plantea serios riesgos ante la posibilidad de respuesta -por medios informáticos o físicos- en caso que sea mal interpretado por el Estado agredido o simplemente pueda ser utilizado como excusa o justificación de ataque a otra nación por intereses políticos o económicos. Por otro lado, las operaciones bélicas realizadas en materia de guerra cibernética resultan más económicas para las fuerzas armadas de los países en tanto que no existe un gran despliegue de recursos y menos diplomacia entre los Estados en conflicto.

China ha desarrollado desde fines de los años ´90 capacidades muy desarrolladas en materia de ciberguerra. Por ejemplo, a partir de que descubrieron fallos en el software y hardware de las firmas Microsoft y Cisco, el Estado capacitó a hackers chinos o "ciberguerreros", como suele denominárselos, para un posible ataque informático a gran escala. El país cuenta con el llamado "gran cortafuegos chino" por donde el gobierno establece una vigilancia de las comunicaciones. De esta manera la supervisión del tráfico de datos por parte de los proveedores de servicio de Internet (ISPs) permite detectar y filtrar material subversivo en contra del régimen, tanto así como la derivación a sitios web con contenido propio. China es uno de los países con capacidad para desconectar las redes nacionales frente a un ciberataque contra el país.

Al igual que sucedió durante la Guerra Fría entre Estados Unidos y la Unión Soviética, en la actualidad, el gigante asiático y el norteamericano mantienen una disputa en el plano de la alta tecnología. En mayo de este año, el gobierno chino prohibió la instalación de Windows 8 en computadoras estatales por lo que ellos consideran la instalación de "puertas traseras" en los programas que facilitan la intrusión externa. Para tal fin, la Universidad Nacional de la Defensa Tecnológica de ese país creó un sistema operativo propio, el KylinOS. En el informe anual de 2012, el Pentágono señaló que desde 2006 hackers del Ejército Popular de Liberación chino intercepta comunicaciones de empresas contratistas de Defensa para el robo de información militar. Desde esa fecha hasta entonces, las declaraciones cruzadas entre ambos países son moneda corriente.

Otro país con capacidad en materia de ciberguerra es Rusia. Existe la creencia que los ex agentes del servicio de inteligencia de la ex Unión Soviética, la KGB, se encuentran detrás del desarrollo de las capacidades para la ciberguerra de ese país. La Agencia Federal de Comunicaciones e Información del Gobierno, un órgano subsidiario de la ex agencia es considerada la mejor escuela de hackers del mundo. Bajo el nombre de Servicio de Comunicaciones e Información Especiales a partir de 2003, originariamente estaba abocada a la creación y desciframiento de códigos secretos, la interceptación de señales de radio, la instalación de micrófonos e intervención de líneas telefónicas, con la aparición de Internet absorbió el principal proveedor de servicios de Internet ruso exigiendo al resto de los ISPs subsidiarios que instalaran sistemas de vigilancia.

En el año 2008, la Organización del Tratado del Atlántico Norte (OTAN) estableció su propia política en materia de ciberguerra para la protección tecnológica de los países

miembros. Para tal fin, creó la Autoridad de Gestión en Ciberdefensa, una unidad con capacidad de respuesta a incidentes informáticos.