EL CIBERESPACIO: EL NUEVO TEATRO DE GUERRA GLOBAL

Luis Recalde H.,
Universidad de las Fuerzas Armadas - ESPE

Resumen

Finalizada o controlada la tradicional guerra convencional, el mundo tiene un nuevo teatro de operaciones llamado ciberespacio. De allí se han desprendido diversos ataques que traspasaron las fronteras virtuales; así, la tecnología de vanguardia ha formulado el nuevo campo de batalla global, desarrollado por los nuevos sistemas cibernéticos.

Palabras clave: ciberespacio, fronteras virtuales, espacio tridimensional, ciberguerras

Introducción

El teatro de guerra es una zona del globo terráqueo relativamente extensa, compuesta por los espacios terrestres, marítimos y aéreos que están - o estarían - potencialmente implicados en operaciones de guerra. Bajo esta perspectiva, estaríamos hablando de una determinada zona geográfica "tangible" de la tierra compuesta por los dominios tridimensionales de las operaciones militares convencionales, y que puede estar involucrada en una acción bélica determinada.

Hace algunos siglos, cuando se comenzaron a estudiar las guerras, generalmente se analizaban las formas de enfrentamientos básicos, por ejemplo la falange griega o la romana, éstas se enfocaban en el empleo táctico de las fuerzas en un determinado teatro de operaciones, hasta que Jomini (1838) pensó que, siguiendo una serie de leyes, un contingente militar podría estar en condiciones de vencer más fácilmente. Estas leyes se referían no solo al enfrentamiento y al combate en sí (es decir, la táctica de la que todos se habían ocupado hasta ese entonces), sino también a la maniobra de aproximación y retirada y a la logística de sostenimiento de las operaciones. A la combinación sincronizada en el terreno de estos aspectos previos al hecho táctico se lo conoce hoy como el "arte operacional" (Vergara, 2003).

Mientras Clausewitz (1831), concebía que la guerra era demasiado compleja, impredecible y un arte muy especial, porque se ejercía sobre elementos que reaccionan en función de su empleo y conducción. Pero lo más importante es que quería probar la naturaleza fundamental de la guerra y su lugar en el espectro de la actividad humana, por lo que la guerra fue orientada a una sistematización en el pensamiento de la conducción militar que, para una mejor interpretación, la guerra podía definirse en tres niveles:

- El que fijaba las causas por las que se debía ir a la guerra, al que llamaron nivel estratégico
- El que entendía los movimientos (maniobras) y la logística de las tropas en el terreno, al que llamaron nivel operacional
- El de los enfrentamientos en sí, al que llamaron nivel táctico (Vergara, 2003).

Por lo tanto en la guerra tradicionalmente visualizada, las fuerzas militares beligerantes emplean sus medios en un espacio tridimensional definido (aire, mar y tierra), y que es uno de los elementos decisivos para la consecución de un objetivo preestablecido en el nivel estratégico militar.

Con el vertiginoso desarrollo de las Tecnologías de Información y Comunicación (TIC), de la era posmoderna, se ha dado origen a un sin número de aplicaciones basadas en sistemas satelitales y terrestres de telecomunicaciones, redes de informática, telemática, dispositivos móviles que procesan, almacenan y transmiten información en tiempo real, elementos que sirven fundamentalmente para la conducción y toma de decisiones en el campo militar. Es aquí donde se origina un espacio intangible para realizar operaciones militares en los niveles operacionales y estratégicos. Este campo se lo denomina "Ciberespacio" y es donde - en los últimos años - se han librado ya grandes batallas.

Breve reseña de las guerras recientes en el ciberespacio

A finales del siglo pasado, ya se produjeron varios ataques utilizando el ciberespacio como un campo de batalla virtual. Con el pasar de los años, estos tipos de conflictos cibernéticos han ido creciendo y cada vez son más sofisticados y letales. A continuación se realiza una breve reseña de las principales "ciberguerras" producidas en los últimos años.

1999 - Guerra de Kosovo

Durante la intervención de los aliados en la Guerra de Kosovo, más de 450 expertos informáticos, al mando del Capitán Dragan, se enfrentaron a los ordenadores militares de los aliados. Este grupo integrado por voluntarios de diferentes nacionalidades, fue capaz de penetrar a los computadores estratégicos de la OTAN, la Casa Blanca y al portaaviones norteamericano Nimitz. Esto solo como una demostración de fuerza, ya que dicho portaaviones no era su objetivo principal; además, de ser una fuente alternativa de información en Internet, sirvió como grupo coordinador de actividades contra la guerra fuera de Yugoslavia.

2003 - Taiwán

En 2003, Taiwán fue amenazado con un "posible" ataque maquinado por las autoridades chinas. No hay pruebas pero dejó sin servicio a diversas infraestructuras como hospitales, la Bolsa y algunos sistemas de control de tráfico. El supuesto ataque provocó un caos progresivo y con una aparente organización; que, además, incluyó virus y troyanos, llegando a la conclusión de que el objeto no sólo sería robar información sensible, sino también paralizar al país.

2007 - Estonia

En ese año, Estonia culpó a las autoridades de Rusia de diversos ataques continuados que afectaron a medios de comunicación, bancos y diversas entidades e instituciones gubernamentales. El origen del conflicto habría sido el retiro de una estatua en memoria del Ejército soviético que se hallaba en la principal plaza de la capital.

2008 - Georgia

Durante la guerra Rusia - Osetia del Sur – Georgia, se produjeron ciberataques a esta última nación por parte de Rusia, orientados hacia sitios gubernamentales.

2010 - Irán

Este país del Medio Oriente también registró un ataque a las centrifugadoras del programa de enriquecimiento de uranio -programa nuclear iraní-. El troyano, virus o programa infiltrado recibió el nombre de Stunex. Irán acusó a Estados Unidos de su autoría.

2011 - Canadá atacada desde China

Según las autoridades canadienses, los sistemas de contraseñas del Ministerio de Finanzas fueron víctimas de un ciberataque procedente de máquinas instaladas en China.

Guerra cibernética en el 2012

EE.UU, Reino Unido, Alemania, India y China ya cuentan con equipos especiales de hackers y centros técnicos para proteger sus bases de datos estratégicas, e incluso para responder proporcionalmente en caso de un ciberataque. Especialistas en seguridad de redes advirtieron de una guerra cibernética para el 2012. Numerosos ataques podrían perpetrarse gracias al avance de las tecnologías de robo de datos y espionaje.

Holanda - 2013

En este año se realizó el mayor ciberataque del mundo, cuando diez millones de holandeses se quedaron sin firma digital y no pudieron acceder a la declaración de renta. La agresión se basó en la modalidad de denegación de servicio (DDOS), que consiste en el bloqueo del portal debido a una avalancha de solicitudes. Desde el Ministerio del Interior holandés explicaron que: "Es como si sonara una alarma continuamente y la puerta estuviera cerrada. Los ladrones están fuera pero desgraciadamente los visitantes normales también".

Ciberataques masivos a Estados Unidos - 2015

En los últimos años, Estados Unidos ha sufrido un sinnúmero de ataques que, de acuerdo a los organismos de seguridad de este país, provienen de hacker chinos, uno de los cuales pudo haber accedido a las bases de datos de cuatro millones de empleados y ex colaboradores del Gobierno federal. La oficina de administración de personal del Gobierno estadounidense, que es la encargada de las investigaciones de los potenciales funcionarios de gobierno, informó que podrían haberse contaminado los datos de altos funcionarios del gobierno (Huerta, 2013).

Definición del ciberespacio desde el enfoque militar

El Departamento de Defensa de Estados Unidos precisa que:

"El ciberespacio es un ámbito operativo cuyo carácter distintivo y único está enmarcada por el uso de la electrónica y el espectro electromagnético para crear, almacenar, modificar, intercambiar y explotar la información a través de las tecnologías de información y comunicación (TIC) y basadas en sistemas interconectados con sus infraestructuras asociadas" (Kuelh, 2006)

Por notro lado, Greg Rattray plantea que:

"El ciberespacio es un entorno artificial para la creación, transmisión y uso de la información en una variedad de formatos, fundamentalmente constituido por el hardware electrónico, redes, sistemas operativos, estándares y políticas de transmisión ".

Bajo estos conceptos, se podría reconocer que el ciberespacio es un teatro de guerra global creado en forma virtual o artificial, y que es una mezcla de electrónica, energía electromagnética, infraestructuras de red y la información en su conjunto.

Para la conducción de las operaciones militares convencionales, los Estados Unidos habían establecido cuatro dominios físicos para sus operaciones, a saber: terrestre, marítimo, aéreo y aeroespacial. Cada uno de ellos tienen radicales diferencias y características físicas únicas, y son valiosos sólo a través de la utilización de la tecnología para explotar esas características. Ahora han añadido al ciberespacio como el quinto dominio, ya que se ha constituido como un factor decisivo y de supremacía militar, por lo que en la actualidad se trata de controlarlo y explotarlo con fines políticos, estratégicos, económicos y militares del poder nacional.

Según el Departamento de Defensa estadounidense, el ciberespacio tiene las siguientes características:

- Es creado, mantenido, operado y de propiedad de los actores públicos, privados y de gobierno, y está disponible en todo el planeta
- Varía dependiendo de la tecnología, arquitectura, procesos y conocimientos para generar nuevas capacidades para su empleo militar
- Está sujeto a la disponibilidad del espectro electromagnético
- Permite altas tasas de maniobra operativas y toma de decisiones ya que capitaliza el hecho de que la información se mueve a velocidades que se acercan a la velocidad de la luz
- Facilita las operaciones a través de los dominios aéreo, terrestre, marítimo y espacial
- Trasciende Fronteras geopolíticas y organizacionales
- Se constituye por la interconexión de los sistemas de transmisión de información y datos, infraestructuras de soporte crítico, dispositivos que recopilan, procesan y transmiten datos, el uso de software, hardware y sistemas de información
- Incluye los datos de voz y vídeo " en reposo " y " en movimiento "
- Es de fácil acceso en distinto grado y a otras naciones, organizaciones, al sector privado, a los cibernautas y también para los enemigos de una nación
- Es la base del almacenamiento y trasmisión de la información y el conocimiento en tiempo real (The National Military Strategy For Cyberspace Operations, 2006).

Conclusiones

La aparición del ciberespacio como un nuevo teatro operacional, presenta nuevas oportunidades para el empleo de sistemas electrónicos, redes e infraestructura en operaciones militares. Por otro lado, es necesario determinar sus vulnerabilidades para diseñar estrategias de defensa en este domino virtual. Entonces podríamos decir que la ciberestrategia es el desarrollo y el empleo de las capacidades para operar y explotar el ciberespacio, integrada y coordinadamente con los otros teatros operacionales para lograr - o contribuir - al logro de los objetivos a través de los componentes de un poder nacional.

En los dominios de la guerra (aire, mar y tierra), las fronteras nacionales están claramente delimitadas; en tal virtud, se puede determinar cuándo existían acciones hostiles externas contra un país o acciones provocados por agentes internos; siendo el espacio cibernético, un campo

virtual donde las fronteras tradicionales desaparecen y se origina un campo de batalla global, puesto que un ataque puede producirse desde países alejados geográficamente o desde el interior del mismo.

Los países que no tienen una gran capacidad económica que les permita adquirir sistemas militares para la guerra convencional, deberían desarrollar capacidades para dominar y explotar los sistemas cibernéticos, de tal forma que se puedan formar profesionales con conocimientos multidisciplinarios para enfrentar las nuevas amenazas de este teatro de guerra global y contribuir a la seguridad nacional.

Referencias Bibliográficas

Impresos

Dan, K, (2006). From Cyberspace to Cyberpower: Defining the Problem, Information Resources Management, College/National Defense University, Washington

Chairman of the Joint Chiefs of Staff, (2006). The National Military Strategy for Cyberspace Operations, Washington

Rattray, G, (2001). Strategic Warfare in Cyberspace, Cambridge, Mass.: MIT Press, UK

Páginas WEB.

Artículo las Guerras Informáticas, Documentos varios, Estudio sobre Ciber Guerra Informática tomado en línea, septiembre 2014, http://www.gitsinformatica.com/descargas.html

Huerta Pablo, Ciberguerras: Las Batallas del Futuro, Hoy, Investigation Discovery, tomado en línea septiembre 2014, http://id.tudiscovery.com/ciberguerras-las-batallas-del-futuro-hoy/.

Vergara, Evergisto de, Los Niveles de la Guerra o del Conflicto, Instituto de Estudios Estratégicos de Buenos Aires, Sep-2003, tomado en línea, http://www.ieeba.com.ar/docu/ Los niveles de la guerra y del_conflicto.pdf.