Computadores e internet en la guerra interestatal: ¿La consolidación de un nuevo poder militar en el siglo XXI?

El presente documento hace parte de la investigación "El ciberespacio como campo de batalla en el siglo XXI", la cual se adscribe a la Línea de Investigación en Desarrollo Científico, Tecnológico y Políticas Ambientales de la Escuela Superior de Guerra.

El paulatino e histórico traslado de la guerra a nuevos teatros de conflagración como la tierra, el océano, el aire y espacio exterior como producto de los adelantos tecnológicos del hombre en materia militar, ha definido claramente el concepto polemológico del poder terrestre, marítimo, aéreo y espacial. Ahora, si los computadores se presentan como armamento para ser empleado en el ciberespacio (que se traduce como teatro de operaciones) por parte de los Estados (y sus Fuerzas Militares), será posible establecer la existencia de un poder ciberespacial en el presente.

"When we apply the principle of warfare to the cyber domain, as we do to sea, air, and land, we realize the defense of the nation is better served by capabilities enabling us to take the fight to our adversaries, when necessary, to deter actions detrimental to our interests".

General James Cartwright, Vice Chairman, U.S. Joint Chiefs of Staff, 2007

Cita Textual

ANDRÉS GAITÁN RODRÍGUEZ

Politólogo Pontificia Universidad Javeriana, Magister en Defensa y Seguridad Nacional de la Escuela Superior de Guerra, y Jefe de la Línea de Investigación en Desarrollo Científico, Tecnológico y Políticas Ambientales del ESDEGUE-SIIA-CEESEDEN

Correo: garo@hotmail.com

Recibido: 30 de octubre de 2011.
Evaluado: 1-15 de noviembre de 2011.
Aprobado: 20 de noviembre de 2011.

Tipología: Artículo de reflexión resultado de investigación ya terminada.

Palabras claves: Tecnologías Informáticas, Ciberespacio, Ciberguerra, Poder Ciberespacial.

Introducción

La guerra, tan sólo concentrándose en su trasegar a partir del inicio de la era moderna, ha evidenciado profundas transformaciones en su naturaleza. Estos cambios, han oscilado entre la evolución del pensamiento político y la consecución del Estado Nación, la construcción de marcos jurídicos como el derecho en la guerra y para la guerra (Ius In

Bello y Ius Ad Bellum), y por supuesto, y siendo el factor más significativo para la presente investigación, la evolución de los procesos de desarrollo científico y tecnológico de las sociedades.

Desde esta perspectiva temporal, la relación entre guerra y tecnología ha sido contundente. Como lo ha enfatizado Carlos Patiño en su obra *Religión, guerra y orden político: la ruta del siglo XXI*, "las actividades que poco a poco se fueron involucrando en la producción, mejoramiento e innovación de armas, sistemas de defensa y modelos de seguridad preventiva, hizo que los procesos de industrialización avanzaran en la medida en que el Estado hiciese la guerra y tuviera una fuerza permanente suficientemente preparada para ello"[1].

La concatenación de dichos elementos, no ha tenido una respuesta diferente a la materialización de lo que se concibe, al interior de las Ciencias Militares, como el *poder*. Cuando los alcances tecnológicos abarcaron el desarrollo de las armas de fuego y la artillería, el *poder* se concibió como terrestre. Al desarrollarse la industria de guerra naval, surgió el *poder* marítimo. Con la llegada de las aeronaves se instauró el *poder* aéreo. Finalmente, posterior al advenimiento del hombre al espacio exterior de la Tierra se determinó el *poder* espacial.

De acuerdo con lo anterior, al tomar como punto de partida que el consorcio guerra-tecnología se ha presentado como el catalizador de la extensión de la fuerza militar de los Estados a nuevos escenarios de conflagración, son precisamente estos nuevos teatros de guerra geográficos y espaciales (de alcance progresivo según el desarrollo tecnológico), otro elemento que debe ser tenido en consideración al momento de analizar los *poderes militares*.

De la misma manera, partiendo del principio de que el usufructo de armamento, medios y tecnología militar no determina directamente efectivos procesos de ofensiva si detrás de estos no existe el diseño de estrategias eficientes y eficaces a la hora de hacer la guerra. Por esto, de igual manera se pone de manifiesto que para conceptualizar un elemento tan complejo como el *poder*, no se puede esgrimir de la ecuación el diseño y la ejecución de tácticas y maniobras que sobrepasen y/o deshabiliten las capacidades enemigas; es decir, la estrategia como elemento fundamental de la conflagración.

Armamento y tecnología, escenarios geográficos y espaciales y estrategia, han sido elementos que se han presentado de forma sinérgica en diversos contextos de movilización castrense. Para evidenciar lo anterior, basta con traer a acotación puntos de referencia históricos como: infantería y artillería, campiñas y praderas europeas y líneas interiores de Jomini; carros blindados, bosques de las Ardenas y guerra de movimiento de Hans von Seeckt (Blitzkrieg) y la estrategia **Shlieffen**; acorazados y portaaviones, océano Pacífico y la concepción del dominio naval de Mahan; o bien, Bombarderos y cazas, espacio aéreo nacional y la teoría de los *cinco anillos* de Warden.

Ahora bien, en el contexto actual, los conflictos armados y políticos que se desatan alrededor del globo están contando con nuevas tecnologías, escenarios y estrategias para su consecución.

El desarrollo de la tecnología informática (procesadores y la Internet) como producto del avance científico de la Tercera Revolución Industrial, la posterior concatenación de lo que se ha denominado como el Ciberespacio, y como producto de esto, que las Fuerzas Militares de diversos países se encuentren generando estrategias, operaciones y tácticas por medio de estos ha permitido dilucidar la configuración (en etapa inicial) de un nuevo *poder* militar; el poder cibernético[2].

Partiendo de esta premisa, la presente investigación analiza concretamente los elementos que componen este nuevo entorno bélico. Conforme el enfoque tripartito que se ha esgrimido acerca del *poder* en párrafos preliminares, el estudio se concentrará en, el porqué se debe concebir a

1 PATIÑO, Carlos. Religión, guerra y orden político: la ruta del siglo XXI. Editorial Universidad Pontificia Bolivariana. Medellín, Colombia. 2006.

2 CASTELLS, Manuel. La era de la información: economía, sociedad y cultura en la sociedad red. (vol.1) Alianza editorial. Madrid, 2005.

las tecnológicas informáticas como armamento para los ejércitos, el porqué se puede esgrimir la existencia de un nuevo escenario donde se pueden desenvolver nuevas o complementarias formas de conflicto interestatal, y el porqué de la existencia de operaciones militares estratégicas en este escenario y por medio de tecnologías informáticas.

En concordancia con lo anterior, el presente documento se verá compuesto de tres espacios de desarrollo. El primero de estos, un análisis, desde diversas perspectivas, de por qué los procesadores, sistemas y redes informáticas son susceptibles de ser empleados como armas y como blancos de ataque. Posteriormente, y desde sus características principales y naturaleza, entender qué hace del ciberespacio un escenario donde también se puede atentar contra un Estado, su infraestructura y su población. Y en última instancia, analizar directamente qué es la ciberguerra, entendida ésta como la materialización de estrategias militares que se sustentan en las tecnologías y espacios cibernéticos para atacar a un enemigo.

Metodología de la investigación

El presente estudio se sustenta sobre un proceso de investigación de revisión literaria, que involucra documentos del ámbito académico, gubernamental y mediático que permiten abordar el tema en cuestión desde la teoría y los sucesos reales acaecidos en la materia.

El objetivo de estudio se enmarca con claridad en torno al fenómeno de la ciberguerra, que al haber tomado gran preponderancia en los últimos años como un fenómeno que describe los conflictos interestatales que se han sucintado en el ciberespacio, ha conducido a establecer si es posible posicionar al interior de la polemología y el desarrollo de la guerra el *poder cibernético*. Es claro por consiguiente, que al tratarse de un elemento que todavía se encuentra en discusión, el desarrollo del texto ofrecerá al lector herramientas que le permitirán construirse una concepción propia frente al tema.

En síntesis, la investigación se fundamenta en tres objetivos específicos. El primero, consiste en escrudiñar cómo las tecnologías informáticas se han convertido en una nueva clase de armamento para ser empleadas en los conflictos interestatales. En segunda medida, entender el por qué el ciberespacio se ha configurado como un escenario en el cual los ataques provenientes de los computadores ponen en grave riesgo la defensa y seguridad nacional. Y en última instancia, sumados estos factores, cómo ha surgido ya una nueva tipología de enfrentamiento interestatal denominada como ciberguerra.

Cabe resaltar, que la estructura temática establecida para la investigación responde al principio de que el poder terrestre, aéreo y del mar se concatenaron a la guerra como producto de la sinergia entre una tecnología especifica y un escenario particular en dónde aplicarla, y cómo esto a su vez llevó a la tipificación de nuevas forma de conflagración.

Tecnologías informáticas: armamento para los ejércitos modernos

La revolución de las Tecnologías de la Información y la Comunicación se ha materializado "como un fenómeno que se expande en la actualidad como la formulación de un nuevo paradigma social y económico que está generando el mito de una transformación sin precedentes en la vida de la humanidad, produciendo una comunicación instantánea de ámbito planetario, con efectos colectivos e individuales, que redundan en una generalización de acciones sin precedentes"[3].

Al proponerse como causa-efecto de la Globalización, las tecnologías informáticas, como lo establece Manuel Castells, se han inmerso en la mayoría de las actividades que llevan a cabo las

3 ESTUPIÑAN, Francisco. Mitos sobre la globalización y las nuevas tecnologías de la comunicación. Revista Latina de Comunicación Social, 2001. [en línea], disponible en: http://www.ull.es/publicaciones/latina

personas y organizaciones. Al tener como objetivo la conexión de procesos políticos, económicos, culturales, religiosos y sociales, los sistemas y redes informáticos fueron demandados precipitadamente a lo largo del planeta. Pero de igual manera, al posicionar un mundo transnacional, con movimientos y flujos de información constantes y transgrediendo las barreras espaciales y temporales a las que se encuentra sujeto el hombre, el mismo sistema mundial ligó, sin retorno, a las organizaciones y personas al mundo virtual de la Internet[4].

Esta diseminación de las tecnologías informáticas al interior de las estructuras y niveles del Estado Nación, permite dar el primer paso al entendimiento de éstas como dispositivos y medios para hacer la guerra. A partir de que todo cálculo militar estratégico siempre debe tener presente las capacidades propias al entrar al conflicto, cuando se deduce esta medida con base en los procesadores y redes, el resultado esgrime que existen tantas armas como número de dichos elementos. Es decir, en las manos correctas un procesador, y el efectivo envío de información a través de la red, hace de cada dispositivo un arma para atacar cualquier instancia de un país donde exista un nodo receptor alineado con el sistema[5].

Este principio se entiende claramente al aunar en las características técnicas de las tecnologías en estudio. Partiendo de la transmisión, almacenamiento y recolección de la información, la informática se ha catalogado en terminales, servidores y redes. En los servidores se encuentran los contenidos (información), para acceder a estos se depende de una terminal (ordenador), y por consiguiente, para alcanzar los contenidos desde los terminales son necesarias las redes de comunicaciones (Internet)[6]; componentes que en síntesis, sí se encuentran difundidos en lo mas intrínseco del Estado y su sociedad.

Martin C, Libicki, analista de la Organización RAND, ha llevado a cabo un estudio acerca de la implementación de las tecnologías informáticas en los ámbitos militares y de la defensa y seguridad nacional, en el cual ha evidenciado en simples palabras, cómo los procesadores y su conexión con el entorno pueden ser una potencial amenaza para los Estados que son victimas de aquellos que las emplean como estrategia de ofensiva.

Libicki ha identificado que los procesadores de información se encuentran compuestos de diversas capas estructurales según su función. En primera instancia, se reconoce la existencia de una capa física, la cual no es más que todos los componentes o aparatos tecnológicos sobre los cuales se construye el sistema en el mundo real; en otras palabras los órganos, exoesqueleto y salida al exterior de la máquina (cable de conexión a la red)[7].

En segundo lugar, se encuentra la capa sintáctica, la cual hace referencia a las instrucciones y comandos que los diseñadores y usuarios han otorgado al sistema para actuar y efectuar sus procedimientos, al igual que las órdenes para que estos interactúen con otras terminales; es decir, aquellos componentes que se describen como *hardware* y *controladores* del sistema[8].

Por último, la capa semántica es la encargada de contener y transmitir la información. Dicho insumo debe entenderse no únicamente como la información que crea y almacena el usuario o sistema que emplea el procesador, sino como un sinfín de nuevas directrices que pueden ser introducidas al sistema para buscar una acción específica; caso concreto, la digitación de una dirección electrónica en el buscador de Internet[9].

4 CASTELLS, Manuel. Galaxia Internet. Plaza & Janés. Barcelona, 2001.

5 J. STEIN, George. Information War, Cyberwar, Netwar. En: R. SCHENEIDER, Barry y E. GRINTER, Lawrence. Battelfield of the Future: 21st Century Warfare Issues. University Press of the Pacific. Honolulu, Hawaii, 2002.

6 CRIADO. Ignacio, RAMILO, María Carmen, SERNA, Miguel, La Necesidad de Teoría(s) sobre Gobierno Electrónico. Una Propuesta Integradora. 2002. [en línea], disponible en: http: www.cnti.gob.ve/cnti_docmgr/sharedfiles/gobiernoelectronico4.pdf.

7 LIBICKI, Marthin. Cyberdeterrence and cyberWar. RAND Corporation. U.S Air Force Power Proyect. Santa Monica, 2009.

8 Ibíd.

9 Ibíd.

La consecución de estas capas, según el analista de RAND, permite que, bajo el control y dominio parte de un experto de las tecnologías informáticas, la capa semántica pueda repercutir claramente sobre la capa sintáctica y física del sistema. Es decir, si el sistema es controlado por un actor que posee la habilidad de generar y difundir la información necesaria, quien tiene capacidad de generar que la capa semántica sólo lo sea en su forma, pues se hace netamente sintáctica en su propósito; lógica que permite que el efecto de la información se traduzca de una forma u otra en la capa física del sistema[10].

Reforzando de forma contundente el análisis esgrimido precedentemente, otra perspectiva que se ha venido formulando para comprender a los sistemas informáticos como medios para producir efectos en los sistemas del adversario, ha sido el enfoque biológico de la cibernética.

A partir del análisis realizado por María Fernanda Gutiérrez, es preciso detectar cómo los procesadores personales se describen y comportan como organismos cuando son infiltrados e invadidos por agentes externos que poseen la naturaleza para afectar sus sistemas. Al igual que un sistema vivo cuando es atacado por un virus, uno informático recibe información dañina, que a través de sus flujos circulatorios de información esparce o localiza el daño por el sistema o centros neurálgicos del mismo[11].

A partir de dicha etapa, el daño afecta los componentes físicos del sistema, como el virus biológico puede dañar órganos en un ser humano. No obstante, debe ponerse en consideración, que a diferencia de los virus creados en ambientes vivos, los cuales se configuran con base en información genética "aleatoria", los virus informáticos son el producto de una mente con conocimientos en cibernética que les otorga *bits* y *bytes* que determinan un daño programado; efecto que de alguna manera presentará síntomas en la dimensión física del sistema[12].

Ahora bien, partiendo de las consideraciones plasmadas anteriormente, lo que desde el enfoque biológico se denomina como virus informático, esta forma de información maligna es tan sólo una de las categorías, de lo que al interior de las fronteras de las Ciencias Militares, se ha denominado como las *ciber-armas*; término que por conjugarse al interior del ciberespacio (concepto que se revisará en el acápite siguiente del documento), ha recibido dicho calificativo.

Conceptualmente, Peter Lorents y Rain Ottis han establecido que las ciber-armas "son una tecnología informática basada en sistemas del mismo orden (software, hardware y medio de comunicación) que ha sido diseñada para perjudicar y dañar la estructura y funcionamiento de algún otro sistema"[13]. Dicho entendimiento, al presentar un horizonte tan amplio, ha permitido el diseño de diversas tipologías de armamento que responden a diferentes necesidades y objetivos del perpetrador del ataque (o ciberataque en este caso).

En la actualidad, existen tipos de ciber-armas, o formas de atacar un sistema informático enemigo si así se prefiere. Ataque a través de un virus cibernético, un ataque de distribución de negación del servicio (Distributed Denial of Service Attacks (DDoS) por sus siglas en inglés), ofensivas mediante gusanos cibernéticos, por medio de troyanos, y el ciberespionaje.

El virus informático (o *malware*), es un programa diseñado para infiltrarse de forma anónima en un sistema, y posteriormente copiarse y reproducirse reiteradamente en espacios específicos del sistema, como los archivos, con el fin de causar el daño que su programador le haya otorgado. A diferencia de otro tipo de armamento cibernético, el virus como máximo efecto tan sólo puede afectar el correcto funcionamiento de un sistema o la destrucción de cierta información de baja prioridad para el sistema[14].

10 Ibíd.

11 GURIÉRREZ, María Fernanda. Virus y Cibervirus: virus biologicos y virus informáticos llaman la tención de los virólogos. En: Revista Innovación y Ciencia, Volumen XVII, No. 1, 2010

12 Ibíd.

13 LORENTS, Peter y OTTIS, Rain. Knowledge Based Framework for Cyber Weapons and Conflicts. CCD COE Publications. Tallinn-Estonia, 2010.

14 K. ROSENFIELD, Daniel. Rethinking Cyber War. George Washington University, Elliott School of International Affairs, Washington, DC, 2010.

El ataque de distribución de negación del servicio, o DDoS, se diseña con el objetivo de atacar directamente un sitio web determinado con el fin de saturar y paralizar su servicio, mediante el progresivo aumento de solicitudes de acceso que en teoría son gestionadas por diversas terminales como orden de sus usuarios, cuando en realidad no es más que una herramienta que funciona por sí misma después de haber vulnerado la protección de dicho nodo. El sitio web, al comenzar a recibir con mayor frecuencia más solicitudes de ingreso y navegación, ve sobrepasada su capacidad de respuesta y entra en parálisis, lo que genera para su dueño o administrador, la imposibilidad de interactuar con ésta[15].

Los gusanos cibernéticos, tal vez el arma virtual más poderosa con la que se cuenta para realizar un ataque en el ciberespacio, se describe como una siguiente etapa de virus, que a diferencia de los tradicionales, no necesita ocultarse en el sistema, o correos electrónicos o descargas al momento de desplazarse por la Red. El gusano tiene la cualidad de reproducirse asimismo para infectar una inmensa masa de computadoras sin necesidad de afectar los sistemas para no ser detectado por los mecanismos de defensa. Gracias a esta característica, esta arma se programa, para que llegado el momento del ataque, éste se direccione hacia el objetivo desde todos los ordenadores que infectó desde tiempo atrás, haciendo de la agresión cibernética un poderoso ataque para deshabilitar el sistema vulnerado[16].

Por otra parte, el troyano también se encuentra relacionado con el ciberespionaje. El empleo de esta herramienta, que se infiltra en el sistema a través de su camuflaje en correos electrónicos o descarga de archivos y programas, por lo cual recibe su nombre, permite la construcción de *puertas traseras*, o entradas libres, para cualquier tipo de agresor que quiera apoderarse de información de acceso como las contraseñas. Esto con el fin, de hacerse posteriormente a información privilegiada de un actor determinado[17].

El Ciberespacio como un nuevo campo de batalla

William Gibson, reconocido escritor de la obra *Neuromancer*, recreó el concepto de ciberespacio para describir cómo las computadoras y su interconexión estaba generando una red ficticia de terminales que dominaba exorbitantes cantidades de información que podía ser empleada en diversos fines. Adicionalmente, el mundo virtual y físico a través del ciberespacio, según Gibson, logran converger de una forma tal que las acciones desarrolladas en cada uno de estos, tiene repercusiones en el otro. Si bien, el ciberespacio depende de los procesadores, su valor se determina por consiguiente en su profundidad; la existencia de una instancia inmaterial donde la información existe y confluye sin depender del tiempo o del espacio[18].

Entender la naturaleza del ciberespacio desde una óptica militar, implica para un mejor resultado analizar el concepto desde una lógica negativa, y posicionándose a partir de la mirada del objetivo, puesto que de esta manera se entiende el significado de atacar a un Estado Nación mediante las tecnologías informáticas y a través de dicho espacio.

Como lo establece Sampaio, se puede afirmar que las sociedades que se han erigido sobre la base de la dependencia de las redes de computadores y el ciberespacio para sus actividades estándares, han acrecentado los niveles de vulnerabilidades de su defensa y seguridad, en tanto que este factor puede ser explotado perfectamente por el enemigo con el fin de atacar las redes de comando y control de un sin número de servicios públicos,

15 GLEBOCKI, Joseph. DOD Computer Network Operations: time to hit the send button. Strategy Research Proyect. U.S. Army War College, Carlisle Barracks, 2008.

16 GLOSH, Sumit. The Nature of Cyber-attacks in the Future: A Position Paper. En: Information Security Journal: A Global Perspective. New Jersey, 2010.

17 SIERRA CABALLERO, Francisco. Guerra informacional y sociedad-red. La potencia inmaterial de los ejércitos. En: Signo y Pensamiento, Vol. XXI, Núm. 40. 2002.

18 GIBSON, William. Neuromancer. Ace Books. Nueva York, 1984.

hasta el punto de sembrar el caos e implantar un alto grado de desmoralización, y así mismo, que un país atacado, se desintegre sicológica y físicamente[19].

Cuando se analiza al ciberespacio como un nuevo campo de batalla, hay que partir de una diferencia básica entre el armamento regular o tradicional y las tecnologías informáticas. La tecnificación y proliferación de armamento convencional de última tecnología es evidente que asegura a los ejércitos y Estados, la superioridad en el campo de batalla, y permite una efectiva defensa y seguridad de las fronteras nacionales[20].

No obstante, cuando se es cada vez más dependiente de las tecnologías informáticas al nivel militar, y se parte de que la sociedad y la infraestructura crítica se encuentran estrechamente vinculadas al mismo sistema, la lógica no determina un avivamiento del concepto de *guerra total* de Clausewitz, sino transforma la fortaleza en la debilidad más contundente del Estado[21].

Si se toma como ejemplo a los Estados Unidos, es posible entender la lógica del ciberespacio como escenario de conflicto. Aproximadamente el 97% de las comunicaciones militares de este país son transmitidas por redes y servicios comerciales; Estados Unidos adquiere la mayoría de los microchips que implementa en sus sistemas informáticos militares y civiles en Estados que fácilmente podrían estar o ser permeados por sus enemigos; incluso, partiendo de que los planos de desarrollo del armamento convencional se encuentran almacenados magnéticamente en los sistemas de la industria civil, los sistemas de ofensiva y defensa convencionales también se ponen en riesgo[22].

Tomando como referente los *poderes* convencionales, es posible percibir de manera práctica cómo se determina el impacto de sus respectivos elementos en los escenarios en donde ejercen sus capacidades. No obstante, cuando el análisis se determina en torno al las ciber-armas y su conclusión en el ciberespacio, el panorama es más complejo de interpretar.

Si bien es en el ciberespacio en donde se lleva a cabo la totalidad de la batalla, y lo que podría considerarse como la *entrega de armas* por parte de un ejército contra un enemigo determinado, dicha fuerza armada, o Estado, no pretende que el alcance de su ataque solo afecte las instancias inmateriales o virtuales del teatro de guerra u operaciones cibernéticas. Se busca, al emplear las ciber-armas que su intrusión y ataque a los sistemas se traslape de forma contundente al mundo, determinando así un daño calculado en la infraestructura crítica del Estado; y por ende, en su población[23].

Teóricos de la materia, y partiendo del principio de Gibson acerca de la sinergia existente entre el ciberespacio y el mundo físico, han dejado en claro que si bien los escenarios informáticos pueden denominarse como teatros de conflagración, es gracias a que, y al igual que se evidenció en los *poderes* precedentes, el accionar estratégico y táctico en un escenario geográfico o espacial determinaba un efecto concreto en el enemigo; rival que se traducía en bases militares, edificios gubernamentales, industrias, suministros, energía y población, entre otros[24].

En tal sentido, cuando se analiza al ciberespacio desde una perspectiva bélica, a pesar de que sea un escenario todavía poco explorado, no debe considerarse como un espacio aislado del Estado y su defensa y seguridad. Al igual que la tecnología militar convencional, y su misma representación

19 G. SAMPAIO, Fernando. Ciberguerra: guerra eletrônica e informacional, um novo desafio estratégico. Organização para Estudos Científicos (OEC). Escola Superior de Geopolítica e Estratégia. Porto Alegre, 2001.

20 D. BERKOWITZ, Bruce. Warfare in the Information Age. En: Athena´s Camp: Preparing for Conflict in the Information Age. RAND Corporation. Santa Nonica,1997.

21 Ibíd.

22 BISHOP, Matt y O. GOLDMAN, EMILY. The Strategy and Tactics of Information Warfare. En: Contemporary Security Policy, 24. California, 2003.

23 ELINOR, Mills. Experts warn of catastrophe from cyberattacks. En: Cnet. InSecurity Complex, febrero 23 de 2010. [en línea], disponible en: http: http://news.cnet.com/8301-27080_3-10458759-245.html

24 WILSON, Clay. Congressional Research Project: report for congress. Information Operations, Electronic Warfare, and Cyberwar: Capabilities and Related Policy Issues. 2007.

como *poder*, tiene efectos devastadores en aquellos escenarios donde son implementadas estratégicamente, lo que se busca con las tecnologías informáticas y el ciberespacio también radica en destruir o desarticular los centros de gravedad del enemigo para deshabilitarlo como contendiente en el conflicto[25].

No en vano, y retomando las lecciones del acápite preliminar del documento, si se parte del hecho de que al enviar información que puede controlar y afectar los sistemas informáticos, es posible prever que tratándose de medios que controlan módulos de la infraestructura crítica del Estado, el daño, pérdidas y desconcierto puede ser igual de suntuario[26].

De esta manera, cómo no anticipar la parálisis o la catástrofe de un Estado Nación cuando el enemigo puede hacerse al control de sus reactores nucleares, o de sus sistemas controladores de tráfico aéreo, de sus redes de comunicación, de la información estratégica y ultra secreta de bases y sistemas de defensa militares, los flujos de capital de las bolsas de valores, e incluso controlar las compuertas de una hidroeléctrica conurbana a una población; es decir, todo sistema que esté alineado con el ciberespacio, se convierte en un canal por el cual se alcanza las vulnerabilidades del contrario[27].

Ahora, si bien es cierto que aunque después de haber desagregado y analizado tanto la materialización de las tecnologías informáticas como armamento, y al ciberespacio como aquel teatro de guerra y operaciones virtuales donde se emplean dichos instrumentos, todavía la configuración del *poder*, en este caso cibernético, se mantiene más cercano a un mundo de ficción; al introducir en el desarrollo temático el análisis de la ciberguerra, se podrá observar que esta nueva manifestación de las capacidades militares ya se ha desmitificado con hechos acaecidos que fueron dirigidos y sobrellevados por Estados.

La ciberguerra: una estrategia militar ofensiva en conflictos del siglo XXI

Para entender qué es la ciberguerra, es pertinente en primera instancia, hacer uso del análisis etimológico que se puede desligar del concepto. Si se toma como punto de atención el prefijo de la palabra, es decir *ciber*, se puede establecer su procedencia de la palabra cibernética. Ahora bien, y valga la redundancia, cibernética deviene del griego Κυβερνήτης (kybernetes), y representaba el arte del control o el arte de pilotar un navío en la antigüedad. Consecuentemente, el científico sueco Norbert Wiener, a mitad del siglo XX, describió la cibernética como medio para controlar animales y máquinas[28].

En el estudio *Cyberwar is Coming*, realizado por John Arquilla y David Ronfeldt se parte de que si el prefijo ciber, o bien cibernética, conyeva a la accion de controlar, conceptos como el de Leitenkrieg, o *guerra de control* al ser traducido del alemán, traducen el significado puro de lo que actualmente se concibe como ciberguerra. Si este tipo de guerra, como se ha evidenciado anteriormente, se basa en la información que circula por el ciberespacio, y generada y almacenada en procesadores informáticos, la guerra de control o ciberguerra busca el control de dicho insumo para modificar los sistemas del enemigo con el fin de proporcionar un ataque que trascienda, en diversas representaciones, al plano físico del Estado objetivo[29].

25 OTTIS, Rain. From Pitchforks to Laptops: volunteers in cyber conflicts. CCD COE Publications. Tallinn-Estonia, 2010.

26 SMITH, Stevenson. Recognizing and Preparing Loss Estimates from Cyber-Attacks. En: Information Security Journal: A Global Perspective, 12: 6. 2004

27 GEERS, Kenneth. The Cyber Threat to National Critical Infrastructures: Beyond Theory. Information Security Journal: A Global Perspective, 18: 1. 2009.

28 Op Cit SAMPAIO.

29 ARQUILA, John y RONDFELD, David. Cyberwar is Coming. En: Athena´s Camp: Preparing for Conflict in the Information Age. RAND Corporation. Santa Nonica,1997.

En este sentido, partiendo del principio en el cual la ciberguerra se traduce como una *guerra de control,* y que adicionalmente existe a través de diversas armas cibernéticas que se desenvuelven y generan sus impactos en un mundo virtual que trasciende a los escenarios físico, el fenómeno de la guerra cibernética en la actualidad hace referencia explícita a: "una agresión promovida por un Estado y dirigida a dañar gravemente las capacidades de otro para tratar de imponerle la aceptación de un objetivo propio o, simplemente, para sustraerle información, cortar o destruir sus sistemas de comunicación, alterar sus bases de datos, es decir, lo que habitualmente se entiende como guerra, pero con la diferencia de que el medio empleado no sería la violencia física, sino un ataque informático que le permita obtener una ventaja sobre el enemigo para situarse en superioridad, o incluso derrocarle"[30].

A lo largo del primer decenio del siglo XXI, ya han sido diversos los acontecimientos que se han suscitado en el mundo a nombre del fenómeno de la ciberguerra. Iniciando el año 2000, un grupo de jóvenes israelitas expertos en cibernética informática, presuntamente vinculados al Gobierno, o bien profesando el nacionalismo propio de la sociedad sionista, construyeron una página web programada para interferir u obstruir sitios en el ciberespacio que pertenecían a las organizaciones terroristas libanesas de Hizbolá y Hamás[31].

La agresión, que presentó una naturaleza propia de un ciberataque de tipo de *negación del servicio*, logró deshabilitar seis sitios cibernéticos de las organizaciones anteriormente mencionadas y un sitio web que pertenecía a la Autoridad Nacional Palestina. Como respuesta a esta acometida, los terroristas palestinos y organizaciones islámicas hicieron un llamado a una guerra santa cibernética; es decir, la *cyber-jihad* o la *e-jihad*. Días después, páginas pertenecientes a oficinas del Parlamento Israelí, del Ministerio del Exterior y del Ministerio de Defensa fueron afectadas por los ataques palestinos[32].

De igual manera, y encontrándose bastante ligados los casos, se puede resaltar los ataques cibernéticos sufridos por Estonia en el 2007 y por Georgia en el 2008, después de que ambos Estados atravesaran particularmente por coyunturas de crisis política y diplomática con su vecino país, Rusia.

En abril de 2007, el gobierno de Estonia anunció públicamente la remoción y reubicación que haría de un monumento Soviético que se encontraba en la capital del país, Tallin, para ser trasladada a un cementerio militar nacional. La decisión gubernamental generó de inmediato controversias entre los estonios de descendencia rusa que veneran la estatua, y los estonios naturales que ven en el monumento un símbolo del antiguo régimen de represión[33].

Los ataques que recibieron las páginas cibernéticas gubernamentales y comerciales estonias, a partir del mes de abril fueron decisivos. A través del ciberataque, el Gobierno ruso logró tomar control de los contenidos de los sitios públicos y sustituyó su información por propaganda política a favor de la causa rusa, y otros más fueron bloqueados para inhabilitar su funcionamiento y comunicación. En tanto que los ataques perduraron por semanas, para el 9 de mayo, día en el que los soviéticos conmemoran la derrota de Hitler, los ataques cibernéticos se intensificaron y recrudecieron significativamente; hasta el punto que las páginas web ministeriales se transformaron en sitios inservibles, y los ciudadanos no pudieron hacer compras on-line durante varios

30 SÁNCHEZ MADERO, Gema. Internet: una herramienta para las guerras en el siglo XXI. En: Military Review Julio-Agosto, 2010.

31 Colonel ALLEN, Patrick y Lieutenant Colonel DEMCHAK, Chris. La Guerra Cibernética Palestina-Israelí. En: Military Review March-April. Combined Arms Center, Fort Leavenworth, Kansas 2003.

32 Ibíd.

33 THE ECONOMIST. Estonia and Russia: a cyber-riot. En: The Economist on-line. 2007 [en línea], disponible en: http: http://www.economist.com/node/9163598.

34 Ibíd.

días, lo que perjudicó severamente la economía estonia que se dinamiza en gran medida a través del ciberespacio[34].

Posteriormente, de forma consecutiva, en el mes de julio de 2008 una firma georgiana de seguridad de la Internet registró un ataque del tipo DDoS contra las páginas gubernamentales del Estado. Un mes después, se registró un segundo ataque mucho más poderoso de la misma naturaleza que afectó contundentemente hasta llevar a la parálisis temporal las páginas del Gobierno de Georgia, impidiendo así que los servidores públicos, tanto políticos como militares, quedaran imposibilitados para comunicarse a través de la Internet[35].

Según las investigaciones de los analistas del ciberataque, paralelamente al advenimiento del segundo ataque, se desarrolló una movilización de tropas del Ejército ruso hacia la región del sur de Georgia denominada como Osetia, un día después que el gobierno local también movilizó algunas escuadras sobre su frontera. Desde esta perspectiva, el ataque DDoS se llevó a cabo con el fin de deshabilitar la comunicación gubernamental por medio de canales informáticos con el fin de deshabilitar las capacidades mando y control y por ende de respuesta, frente al acaecimiento de una agresión que se llevaba a cabo en el plano real o geográfico de la polémica[36].

Cabe resaltar, que las investigaciones que se llevaron a cabo posteriormente a los ataques de Estonia y Georgia de forma semejante apuntaron a las autoridades a rastrear, como fuente del ciberataque, a una gran cantidad de procesadores personales pertenecientes a civiles rusos y extranjeros que visitaban el país en los respectivos momentos, y por supuesto investigando sus áreas de desempeño profesional y sus conocimientos informáticos no presentaron relación alguna con la agresión; esto, gracias al funcionamiento propio de un ataque DDoS, como se observó en la primera parte del documento.

Tal vez, el caso de ciberguerra sin paragón alguno hasta el momento ha sido el ataque que sufrió Irán en el año 2010, cuando una ciber-arma denominada como *gusano estuxnet* invadió los sistemas informáticos que controlan específicamente la infraestructura crítica de este país.

Según los análisis de las autoridades y sectores de defensa e Inteligencia iraní, el gusano, con la capacidad de reproducirse rápidamente por el ciberespacio y terminales conectadas a ésta, entró a la red informática de Irán por medio de una flashdrive que fue conectada a un procesador con conexión a ésta. A partir de entonces, el arma se difundió por la *red mundial* hacia miles de procesadores, que incluso se encontraban en países como India, China y Paquistán, y así dar espera a la ejecución del ataque programado con el que fue diseñado para afectar la infraestructura del Estado[37].

Posteriormente, al llegar el mes de junio del 2010, el estuxnet se activó, y con base en las características que describen este tipo de ciberarma, desde cada una de las computadoras en las cuales se había alojado anónimamente, el ataque fue perpetrado. El gusano, una vez iniciara su ofensiva, fue programado para que buscara específicamente los sistemas informáticos que controlaban el comando y control del reactor nuclear de Bushehr. Posterior a esta etapa, y por reservas del Gobierno e Inteligencia iraní, no se sabe a ciencia cierta cuál fue el alcance del ataque cibernético con el gusano estuxnet. Lo único que se puede constatar, es que hasta el presente, el

35 W. KORNS, Stephen y KASTEMBERG, Joshua. Georgia's Cyber Left Hook. CCD COE Publications. Tallinn-Estonia, 2010.

36 Cyberspace and the 'First Battle' in 21st-century War. En: Defense Horizons, Number 68. National Defense University. Center For Technology And National Security Policy. Washington D.C., 2009.

37 Ibíd.

38 KERR, Paul, ROLLINS, John y THEOHARY, Catherine. The Stuxnet Computer Worm: Harbinger of an Emerging Warfare Capability. CRS Report for Congress, 2010. [en línea], disponible en: http://www.fas.org/sgp/crs/natsec/R41524.pdf.

reactor todavía no ha podido ser inaugurado por el Gobierno de Ahmadinejad[38].

Análisis paralelos al acontecimiento, concentrados en la fuente y motivación que giraron en torno al ataque al reactor nuclear en Irán, han detectado como el responsable directo al Estado de Israel, el cual, al detectar al país como una amenaza para la seguridad y defensa de la Nación en materia nuclear, decidió emplear al ciberespacio y la ciberguerra para alcanzar un objetivo estratégico que de forma convencional hubiera sido bastante costoso tanto a nivel político como militar. Anteriormente a este caso, no se había registrado una agresión cibernética de tal magnitud e impacto. El gusano estuxnet fue un arma con un desarrollo informático claro en sus objetivos, rutas y efectos al momento de diseñarse, por lo cual no ha existido cabida para el azar o desarrollo de un caso fortuito; en un principio mantuvo como objetivo la infraestructura crítica nuclear Iraní[39].

Conclusiones

Al finalizar la investigación, los resultados obtenidos han permitido concluir que si bien, al interior de la ciencia castrense o a nivel académico, el debate sobre la existencia de un nuevo *poder* militar, el *poder cibernético*, no se ha materializado aún. Tras el desarrollo de este documento, fue posible evidenciar que cuando la guerra se remite al empleo de tecnologías informáticas y las aplica en el ciberespacio con el fin de atacar a un enemigo, las semejanzas frente a la naturaleza de *poderes* precedentes como el terrestre, aéreo y marítimo son abismales.

Dos variables han trascendido en la historia de la guerra para poder considerar la existencia de los *poderes*. Por una parte la variable tecnológica, traducida en armamento, medios estratégicos, operativos y tácticos de los ejércitos y los Estados. Y por otra parte, un escenario o teatro de operaciones donde dichas capacidades puedan ser aprovechadas según su naturaleza. Es por esto, y a manera de contexto, que carros blindados han sido desarrollados para alcanzar objetivos en tierra, los aviones se han visto inmersos en grandes batallas en el aire aunque paralelamente demuestren una importancia estratégica en operaciones aire-tierra, y los buques y portaaviones se han empleado para el dominio de los océanos y mares.

Por lo tanto, (ahora en la actualidad) como se logró observar, existen conflictos que bien pueden apoyarse o suscitarse exclusivamente en el ciberespacio como medio para alcanzar y proteger los intereses nacionales. De igual manera, estas manifestaciones militares en la virtualidad también cuentan con el empleo de un sin número de tipos de armas, que otorgan al ejército ofensivo la capacidad de irrumpir en los sistemas informáticos de su rival en la guerra, y así causarle un daño calculado que se puede materializar desde la negación a la información, así como a la destrucción de la infraestructura física estatal; lo que afecta a la sociedad directamente.

Si se ha llegado a recrear, más que un concepto, el fenómeno de la ciberguerra como representación de los enfrentamientos cibernéticos interestatales, sin mencionar que las agrupaciones terroristas (actor fundamental de los conflictos irregulares contemporáneos) también ejercen una fuerte presencia y accionar en el ciberespacio, se pone de manifiesto que, y aunque no sea conceptualizado o teorizado como tal la existencia del *poder cibernético*, los Estados y sus Fuerzas Militares sí han detectado la coexistencia de su supervivencia, traducida en acciones de ataque y defensa, en un espacio virtual y cibernético.

En síntesis, y como se planteó al inicio de la investigación, no es objetivo de este espacio de reflexión imponer la existencia de la cibernética como un *poder* militar, que en orden consecutivo a sus predecesores ahora ocupe la potestad del ciberespacio. Tan sólo, aunque con el mayor rigor académico, se procuró evidenciar desde tres perspectivas -armamento, escenario de batalla, y naturaleza de la guerra (ciberguerra)-, que en

39 PORTEUS, Holly. The Stuxnet Worm: Just Another Computer Attack or a Game Changer? Parliament Information and Research Service of Canada. Publication No. 2010-81-E. [en línea], disponible en: http://www.parl.gc.ca/Content/LOP/ResearchPublications/2010-81-e.pdf.

los últimos años ya se viene gestando conflictos "armados" en este escenario tan poco explorado en comparación a los eventos que allí ocurren en materia de seguridad y defensa.

Las tecnologías informáticas como armamento cibernético, el ciberespacio como escenario de conflicto interestatal, y la ciberguerra como estrategia militar como fruto de la combinación de los elementos anteriores, dejaron de estar en el mundo del mito o la ciencia ficción desde años atrás. Ahora, y partiendo de la existencia de casos concretos de ciberguerra, es responsabilidad de los Gobiernos y Fuerzas Militares abordar este tema como la amenaza latente en la que se ha convertido.

Bibliografía

1 ARQUILA, John y RONDFELD, David. Cyberwar is Coming. En: Athena´s Camp: Preparing for Conflict in the Information Age. RAND Corporation. Santa Nonica,1997.

2 BISHOP, Matt y O. GOLDMAN, EMILY. The Strategy and Tactics of Information Warfare. En: Contemporary Security Policy, 24. California, 2003.

3 CASTELLS, Manuel. Galaxia Internet. Plaza & Janés. Barcelona, 2001.

4 _____. La era de la información: economía, sociedad y cultura en la sociedad red. (vol.1) Alianza editorial. Madrid, 2005.

5 Colonel ALLEN, Patrick y Lieutenant Colonel DEMCHAK, Chris. La Guerra Cibernética Palestina-Israelí. En: Military Review March-April. Combined Arms Center, Fort Leavenworth, Kansas 2003.

6 CRIADO. Ignacio, RAMILO, María Carmen, SERNA, Miguel, La Necesidad de Teoría(s) sobre Gobierno Electrónico. Una Propuesta Integradora. 2002. [en línea], disponible en: http: www.cnti.gob.ve/cnti_docmgr/sharedfiles/gobiernoelectronico4.pdf.

7 D. BERKOWITZ, Bruce. Warfare in the Information Age. En: Athena´s Camp: Preparing for Conflict in the Information Age. RAND Corporation. Santa Nonica,1997.

8 ELINOR, Mills. Experts warn of catastrophe from cyberattacks. En: Cnet. InSecurity Complex, febrero 23 de 2010. [en línea], disponible en: http: http://news.cnet.com/8301-27080_3-10458759-245.html

9 ESTUPIÑAN, Francisco. Mitos sobre la globalización y las nuevas tecnologías de la comunicación. Revista Latina de Comunicación Social, 2001. [en línea], disponible en: http://www.ull.es/publicaciones/latina

10 G. SAMPAIO, Fernando. Ciberguerra: guerra eletrônica e informacional, um novo desafio estratégico. Organização para Estudos Científicos (OEC). Escola Superior de Geopolítica e Estratégia. Porto Alegre, 2001.

11 GEERS, Kenneth. The Cyber Threat to National Critical Infrastructures: Beyond Theory. Information Security Journal: A Global Perspective, 18: 1. 2009.

12 GIBSON, William. Neuromancer. Ace Books. Nueva York, 1984.

13 GLEBOCKI, Joseph. DOD Computer Network Operations: time to hit the send button. Strategy Research Proyect. U.S. Army War College, Carlisle Barracks, 2008.

14 GLOSH, Sumit. The Nature of Cyber-attacks in the Future: A Position Paper. En: Information Security Journal: A Global Perspective. New Jersey, 2010.

15 GURIÉRREZ, María Fernanda. Virus y Cibervirus: virus biologicos y virus informáticos llaman la tención de los virólogos. En: Revista Innovación y Ciencia, Volumen XVII, No. 1, 2010.

16 J. STEIN, George. Information War, Cyberwar, Netwar. En: R. SCHENEIDER, Barry y E. GRINTER, Lawrence. Battelfield of the Future: 21st Century Warfare Issues. University Press of the Pacific. Honolulu, Hawaii, 2002.

17 K. ROSENFIELD, Daniel. Rethinking Cyber War. George Washington University, Elliott School of International Affairs, Washington, DC, 2010.

18 KERR, Paul, ROLLINS, John y THEOHARY, Catherine. The Stuxnet Computer Worm: Harbinger of an Emerging Warfare Capability. CRS Report for Congress, 2010. [en línea], disponible en: http://www.fas.org/sgp/crs/natsec/R41524.pdf.

19 LIBICKI, Marthin. Cyberdeterrence and cyberWar. RAND Corporation. U.S Air Force Power Proyect. Santa Monica, 2009.

20 LORENTS, Peter y OTTIS, Rain. Knowledge Based Framework for Cyber Weapons and Conflicts. CCD COE Publications. Tallinn-Estonia, 2010.

21 MILLER, Robert. Cyberspace and the 'First Battle' in 21st-century War. En: Defense Horizons, Number 68. National Defense University. Center For Technology And National Security Policy. Washington D.C., 2009.

22 OTTIS, Rain. From Pitchforks to Laptops: volunteers in cyber conflicts. CCD COE Publications. Tallinn-Estonia, 2010.

23 PATIÑO, Carlos. Religión, guerra y orden político: la ruta del siglo XXI. Editorial Universidad Pontificia Bolivariana. Medellín, Colombia. 2006.

24 PORTEUS, Holly. The Stuxnet Worm: Just Another Computer Attack or a Game Changer? Parliament Information and Research Service of Canada. Publication No. 2010-81-E. [en línea], disponible en: http://www.parl.gc.ca/Content/LOP/ResearchPublications/2010-81-e.pdf

25 SÁNCHEZ MADERO, Gema. Internet: una herramienta para las guerras en el siglo XXI. En: Military Review Julio-Agosto, 2010.

26 SIERRA CABALLERO, Francisco. Guerra informacional y sociedad-red. La potencia inmaterial de los ejércitos. En: Signo y Pensamiento, Vol. XXI, Núm. 40. 2002.

27 SMITH, Stevenson. Recognizing and Preparing Loss Estimates from Cyber-Attacks. En: Information Security Journal: A Global Perspective, 12: 6. 2004.

28 THE ECONOMIST. Estonia and Russia: a cyber-riot. En: The Economist on-line. 2007 [en línea], disponible en: http: http://www.economist.com/node/9163598.

29 W. KORNS, Stephen y KASTEMBERG, Joshua. Georgia's Cyber Left Hook. CCD COE Publications. Tallinn-Estonia, 2010.

30 WILSON, Clay. Congressional Research Project: report for congress. Information Operations, Electronic Warfare, and Cyberwar: Capabilities and Related Policy Issues. 2007.

CEESEDEN
Estudios en
SEGURIDAD y DEFENSA

Volumen 6 • N. 2 • *Edición Nº 12 • Noviembre de 2011*

Para solicitar un ejemplar en físico o en formato PDF o para confirmar el acuse de recibo de la revista, por favor escribir a:

Escuela Superior de Guerra
Centro de Estudios Estratégicos sobre Seguridad y Defensa Nacionales
-**CEESEDEN**-

Carrera 11 No. 102-50 • Teléfono: 6294928
e-mail: **revistaceeseden@esdegue.mil.co**
www.esdegue.mil.co

Bogotá - Colombia

En Colpatria nos encantan los productos exclusivos.

Vivimos lo mismo que **tú.**

TV SONY 40″

iMac Apple 21.5″

PSP SONY

Parlantes BOSE Soundtrack

MacBook Pro Apple 13.3″

Sabemos que quieres recibir lo mejor,
Rentabilidad y **Seguridad**.

Abre ya tu CDT

y llévate algo que nadie más te va a dar.

Pregunta AQUÍ

Depósito seguro de Fogafin
www.fogafin.gov.co

Hasta 20 millones, su dinero está asegurado

Aplican condiciones de acuerdo a montos, plazos y restricciones. Vigencia de la promoción de noviembre de 2011 a febrero de 2012. El Banco se reserva el derecho de reemplazar los obsequios por otras alternativas con características similares, previo aviso. Antes de hacer efectiva la promoción, consulta en www.colpatria.com/personas/cdt.

CDT

COLPATRIA MULTIBANCA

VIGILADO SUPERINTENDENCIA FINANCIERA DE COLOMBIA