El ciberespacio : un nuevo campo de batalla

Andrés Gaitán Rodríguez

Trabajo de grado para optar al título profesional:
Maestría en Seguridad y Defensa Nacionales

Escuela Superior de Guerra "General Rafael Reyes Prieto"
Bogotá D.C., Colombia

2011

FUERZAS MILITARES DE COLOMBIA

ESCUELA SUPERIOR DE GUERRA

MAESTRÍA EN DEFENSA Y SEGURIDAD NACIONAL

El CIBERESPACIO: UN NUEVO CAMPO DE BATALLA

ANDRÉS GAITÁN RODRÍGUEZ

BOGOTÁ D.C.

Índice

INTRODUCCIÓN

La historia militar ha estado descrita por importantes periodos de transformación como producto de la incidencia de los procesos científicos y tecnológicos de la humanidad sobre las capacidades de los ejércitos.

Producto de lo anterior, y bajo la concepción del *poder militar*, se observó en una primera instancia, y gracias al desarrollo de la artillería de tierra cómo surgió el *poder terrestre*. Posteriormente, cuando el ingenió humano llevó la tecnología marítima a un nuevo nivel para hacer la guerra, se dio origen al *poder marítimo*. Luego, alcanzando el cielo y más tarde el espacio, los ejércitos lograron constituir su *poder aéreo* y espacial.

Introducirse en la naturaleza de estas capacidades, evidencia de manera clara que la concepción de ese elemento que se ha denominado como *poder* depende claramente de la concatenación de dos elementos; la *tecnología* y el *escenario* o *espacio* de acción en donde dichos avances se pueden emplear de manera estratégica.

Por ésto, ha sido posible evidenciar el uso de la geografía terrestre para desplegar una gran diversidad de carros blindados, armamento para las tropas, dispositivos explosivos de alto poder destructivo, artillería, tecnología de guerra electrónica y vehículos de transporte entre otros. De igual manera, la aparición de los submarinos, barcos portaaviones, y la modernización de las naves artilladas se convirtieron en la punta de lanza en los mares y océanos del mundo. Finalmente, en concordancia con lo anterior, la llegada de aviones caza, satélites, bombarderos, y en la actualidad las furtivas aeronaves no tripuladas (UAV), ha dado origen a las batallas aéreas, y del espacio en el caso de los países que han logrado desarrollar una carrera espacial.

Ahora bien, en la actualidad con el sorprendente desarrollo que se le ha impreso al perfeccionamiento y evolución de las *tecnologías informáticas* y el *ciberespacio*, se ha venido presenciando un fenómeno, que si bien se encuentra en etapa de gestación aun, ya ha evidenciado que nuevamente hay un elemento tecnológico y un espacio o dimensión que se están conjugando para ofrecerle nuevas capacidades de para *hacer la guerra* a los Estados en el siglo XXI.

Parte de esto, es que ya ha sido posible observar cómo países como China llevan haciendo espionaje en el ciberespacio (ciberespionaje) desde el año 2002 a EE.UU. y Alemania (entre otros) a nivel gubernamental y comercial, cómo el Estado de Rusia ya ha ejecutado ataques informáticos (ciberataques) a Estonia (2007) y Georgia (2008), o bien cómo la infraestructura crítica de un Estado puede verse gravemente afectada por un arma cibernética, tal y como se constató con la intrusión de la ciberarma *stutnex* al sistema informático del reactor nuclear de Bushehr en Irán; ataque que en la actualidad se le atribuye a Israel.

Partiendo de los ejemplos tomados precedentemente, y adicionalmente de que de igual manera los Estados Unidos de Norteamérica ya hayan conformado su primer Comando Cibernético, o CYBERCOM, o que dentro de las agendas de defensa y seguridad de Organismos Internacionales Gubernamentales (OIG) como la OTAN o la ONU ya se estén adoptando políticas concretas para generar capacidades militares para responder a las agresiones en el ciberespacio (entre diversas accionas más a resaltar), ha puesto de manifiesto que un número importante de países ya se han percatado de la realidad del ciberespacio como un nuevo campo de batalla; y que al interior del mismo, ya existe un tipo de conflicto entre Estados que se puede denominar como la ciberguerra .

Esta nueva forma de enfrentamiento, a diferencia de las que se pueden llevar a cabo en los escenarios de guerra tradicionales (tierra, mar, aire y espacio), gracias al armamento con el que se hace, y la dimensión en la cual se desarrolla, variables como tiempo, espacio, clima, arsenal, número de tropas, movilización,

perdida de vidas humanas y costo de la guerra, dejan de ser relevantes; solo se requiere un computador conectado a internet y un objetivo que de igual manera lo este para hacer la ciberguerra.

El factor álgido de la ciberguerra radica en la organización del sistema mundial que la humanidad ha optado por construir para sí misma. En la medida en que los Estados han inclinado su desarrollo mediante su inclusión a un mundo globalizado e interconectado en sus procesos políticos, económicos y culturales, el ciberespacio ha sido el canal para conseguirlo.

Por esto, es claro observar cómo: los Gobiernos han integrado su imagen, información pública y servicios a este escenario; los sistemas informáticos de mando y control de la infraestructura crítica (pública y privada) se integran a la Internet; los sistemas de control de tránsito vehicular y aéreo dependen de la informática y las redes; o bien, cómo los sistemas de defensa y militares también dependen de los computadores.

En este sentido, al consolidar un mundo bajo un sistema informático global denominado como ciberespacio, todo aquello que podría denominarse como *centro de gravedad* en un Estado, en la actualidad se encuentra integrado a esta dimensión; y por ende, al partir de este precepto, todo actor con el conocimiento necesario en cibernética, y acceso a un computador que se encuentre conectado a la Internet, tiene la posibilidad de acceder a los centros neurálgicos de funcionamiento de una Nación, ya sea con intenciones hostiles, o bien con el objeto de espiar información gubernamental en todos sus ámbitos.

En otro orden de ideas, no se puede perder de vista la naturaleza de la guerra contemporánea. Como se ha evidenciado históricamente, posterior a la guerra de Corea en 1951, los conflictos comenzaron a caracterizarse por la parición de los actores armados irregulares, y por originarse al interior del territorio del Estado Nación, en un primer momento, y contemporáneamente por operar de manera

transnacional. Al interior de esta categorización se ha visto el surgimiento de movimientos de subversión, grupos rebeldes y por supuesto, las agrupaciones terroristas; o todas aquellas que se pueden denominar como tal por el emplear el terrorismo como una de sus diversas formas de lucha.

Al igual que las Fuerzas Militares de los Estados, el terrorismo, tanto doméstico como trasnacional, también ha encontrado en el ciberespacio y las tecnologías que lo controlan, importantes instrumentos para llevar a cabo sus luchas irrestrictas contra la institucionalidad y los ciudadanos de sus propios países, o de aquellos a los cuales les han declarado la guerra; como es el caso de la FARC actuando al interior de Colombia, o bien, Hezbolá y Hamás haciendo su guerra contra Israel, igual que Al Qaeda a los Estados Unidos.

Cabe resaltar, que una vez que el ciberespacio comenzó a cobrar vida en la década de los años noventa, como producto de constituirse como causa y efecto de la Globalización, los grupos terroristas encontraron en el ciberespacio un importante escenario para potenciar sus acciones tradicionales, y generar nuevas capacidades simultáneamente.

Parte de lo anterior, se puede observar claramente cómo ha haber desarrollado una clara capacidad de ataque cibernético, los terroristas han sabido desarrollar una diversidad de apoyos y capacidades que claramente están aportando a la realización de los objetivos que estos grupos han establecido en sus conflictos.

El hecho de que este tipo de actores ya no depende de que el medio de comunicación decida capturar y difundir su acción perpetrada, para que el objetivo psicológico del terrorismo se cumpla, pues la Internet es de libre acceso y se puede difundir globalmente el comunicado deseado. De igual manera, el terrorista también ha consolidado medios de reclutamiento, financiación, de guerra política, de comunicación y coordinación, de entrenamiento y adoctrinamiento en el ciberespacio; elementos que vistos individualmente aportan de manera alguna a la

consumación de los actos de estas organizaciones en el escenario físico del conflicto que libran.

Este fenómeno, al igual a como sucedió con los enfrentamientos informáticos entre Estados, ha sido conceptualizado mediante la prelación del medio en el que se desarrolla, por lo que de igual manera se puede hablar de ciberterrorismo para este propósito.

El ciberterrorismo, si bien se representa como el fenómeno mediante el cual un actor propio de esta categoría podría desarrollar un ataque cibernético a un estado enemigo, al traducirse de igual manera como una forma en la cual el terrorista emplea el ciberespacio para mejorar sus capacidades de organización, claramente se han encontrado a través de esta dimensión una forma de sopesar la asimetría que los describe frente a las fuerzas oficiales que los combaten.

Ahora bien, el hecho de que tanto la ciberguerra, como representación de la guerra interestatal o regular en el ciberespacio, y el ciberterrorismo como expresión de la asimetría de los conflictos irregulares, hayan adquirido un importante dominio del ciberespacio para llevar a cabo acciones furtivas y hostiles, ha puesto de manifiesto la necesidad de consolidar medidas y contramedidas de respuesta a estos fenómenos del siglo XXI, y así extender sobre el ciberespacio el manto de la defensa y seguridad estatal.

Tanto para aquellos Estados que han desarrollado importantes capacidades para hacer la ciberguerra, así como para los que se han visto alejados de dicha práctica, la necesidad de poner en marcha políticas de ciberdefensa para contrarrestar las amenazas que en este nuevo escenario emergen, es un punto de discusión irrestricto en la agenda gubernamental de la mayoría de países del mundo.

Partiendo de este recorrido sinóptico acerca del ciberespacio como un campo de batalla, ha surgido el interrogante en esta investigación, de sí es posible interpretar el empleo de las tecnologías informáticas (computadores e Internet) en este escenario de interacción humana como un nuevo *poder* militar que los Estados pueden emplear para alcanzar sus objetivos nacionales, o bien defenderse de los posibles enemigos que pretendan agredirlo a través de estos mismos medios.

No obstante, en tanto que el terrorismo es un elemento de la presente investigación, será el objetivo principal de la misma, evidenciar cómo el ciberespacio, además de convertirse en una dimensión que ha aportando al desarrollo humano, también se ha convertido en un escenario de batalla en el siglo XXI.

De tal forma, con el fin último de poder expugnar los elementos y acontecimientos que han descrito el objeto de estudio seleccionado, este documento de investigación se ha diseñado con base en cuatro ejes temáticos.

En primera instancia, se desarrollará un capítulo inicial en el cual se observará el cómo y el porqué el ciberespacio se ha transformado en una dimensión a la cual ya se han traspalado aspectos propios de la *guerra*. Para esto, se expondrá en primera medida los elementos que configuran a los procesadores y la Internet como una clase de armamento útil para esta dimensión virtual. Y en segunda medida, y al emplear las tecnologías informáticas de esta manera, se expondrán los hallazgos que permiten evidenciar la naturaleza del ciberespacio como un campo de batalla; y más importante aún, evidenciar las características que evidenciar que los Estados pueden verse sumamente perjudicados, en todas sus dimensiones reales o físicas (ya no sólo informáticas) cuando se combinan las ciberarmas y el espacio cibernético.

El segundo capítulo de la investigación, asumirá por su parte una postura analítica en torno al fenómeno del ciberterrorismo. Este acápite, permitirá como inicio

observar la lógica que ha determinado el comportamiento terrorista sobre los medios de comunicación, y cómo al consolidarse el ciberespacio, y que las tecnologías informáticas sean de libre acceso para estos actores, ha potenciado el desarrollo de sus causas de forma determinante. Como un segundo elemento, se pondrá en consideración las nuevas capacidades que los grupos terroristas han logrado adquirir en el ciberespacio para sopesar su asimetría característica al interior de los conflictos armados que detentan; por lo anterior, acciones relacionadas con la *guerra política*, el financiamiento, los ataques cibernéticos y la coordinación de acciones, entre otras acciones más, serán los puntos a observar.

Cabe resaltar, que si bien la prioridad de esta exploración es el ámbito militar en el escenario ya propuesto, con el fin de no interrumpir este propósito, se ha considerado pertinente en primera instancia analizar los elementos de la guerra asimétrica; o bien, el ciberterrorismo. En este sentido, cuando la investigación llegue a su momento de entender los modelos de defensa y seguridad cibernética estatales y de Organismos Gubernamentales Internacionales, ya se tenga como precedente las amenazas de este fenómeno, y por ende la prioridad de lo que se podría denominar como ciberdefensa (capítulo 4).

Conexo a lo anterior, debe tenerse en cuenta de igual manera, que si bien el objeto de investigación contenido en este documento se ha diseñado para evidenciar sí el ciberespacio es un campo de batalla, conforme la naturaleza de la guerra contemporánea (guerra de cuarta generación, guerra irregular, guerras de la *tercera ola* o *nuevas guerras*) es de mayor valor poder circunscribir cuales son las dinámicas propias de los actores que desarrollan batallas ilegítimas contra los Estados.

Ahora bien, entrando al marco analítico del ámbito castrense y gubernamental, será objetivo del capítulo tercero el estudio de la ciberguerra. Este espacio se ha diseñado con el fin de poder brindar un punto de vista holístico acerca de este fenómeno, por lo que involucrará en primera instancia un acercamiento conceptual

y teórico con el fin de entender en qué consiste esta nueva forma de ataque. Paralelamente se pondrá a consideración los casos o hechos más representativos que han ocurrido en los últimos años sobre ciberguerra en el mundo; esto, con el objetivo de ver que este escenario que se considera todavía más en el plano de la ficción, sea aterrizado a una realidad que revela que ya existen Estados que han sido altamente afectados por ataques de esta naturaleza.

1. CAPITULO PRIMERO

EL CIBERESPACIO: LA CONSOLIDACIÓN DE UN NUEVO CAMPO DE BATALLA

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

1.1 *Las Tecnologías Informáticas: la consolidación de nuevas capacidades para trasgredir la defensa y seguridad estatal en el siglo XXI*

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"[1].

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 personas y organizaciones privadas y públicas. Al tener como objetivo la conexión de procesos políticos, económicos, culturales, religiosos y sociales, los sistemas y redes informáticas fueron demandados precipitadamente a lo largo del planeta. Pero de igual manera, al posicionar un mundo transnacional, con movimientos y flujos de información

---

[1] 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

constantes y transgrediendo las barreras espaciales y temporales a las que se encuentra sujeto el hombre, el mismo sistema mundial ligó, sin retorno alguno a un estadio anterior, a las organizaciones y personas al mundo virtual del ciberespacio[2].

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 herramientas como dispositivos y medios para hacer la guerra.

Al partir de que todo cálculo militar estratégico siempre se 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 (con las Red mundial, o World Wide Web)[3].

Este principio se entiende claramente al comenzar a 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 éstos se depende de una terminal (computador), y por consiguiente, para alcanzar los contenidos desde los terminales son necesarias las redes de comunicaciones (intranet y la Internet)[4]; componentes que

---

[2] CASTELLS, Manuel. Galaxia Internet. Plaza & Janés. Barcelona, 2001.

[3] 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.

[4] 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.

en síntesis, sí se encuentran difundidos en lo mas intrínseco del Estado y su sociedad por las razones ya esgrimidas.

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 conceptos sencillos de asimilar, 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 computadores se encuentran compuestos de tres 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 *chips*, disco duro, memoria RAM, exoesqueleto y salida al exterior de la máquina (cable de conexión a la red)[5].

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[6].

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

---

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

[6] Ibíd.

una acción específica; caso concreto, la digitación de una dirección electrónica en el buscador de Internet[7].

La consecución de estas capas, según el analista de RAND, permite que, bajo el control y dominio por parte de un experto de las tecnologías informáticas, la capa semántica pueda repercutir claramente sobre la capa sintáctica y física del sistema. Es decir, sí el sistema es controlado por un actor que posee la habilidad de generar y difundir la información correcta, tiene la completa capacidad de generar que la capa semántica del sistema sólo lo sea en su nombre, pues ésta se hace netamente sintáctica en su propósito bajo este escenario; el actor en mención, con la información maliciosa que puede generar la convierte en términos sintácticos en la medida en que adquiere la capacidad de establecer comportamientos determinados en el sistema que invade. De igual manera, en consecuencia esta lógica permite que el efecto de la información se traduzca de una forma u otra en la capa física del sistema; lo que lleva el impacto de la acción al mundo real[8].

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. Con base en los principios que se han establecido a partir de esta perspectiva, es posible entender lo Libicki conceptualiza como información maliciosa y su construcción.

A partir del análisis realizado por María Fernanda Gutiérrez, es preciso detectar cómo los procesadores personales se describen y comportan como seres orgánicos cuando son infiltrados e invadidos por agentes externos que poseen la naturaleza para afectar sus sistemas.

---

[7] Ibíd.
[8] Ibíd.

Al igual que un sistema vivo cuando es atacado por un virus biológico, un sistema informático también recibe información dañina para sí mismo. No obstante, a diferencia de la primera amenaza, la cual se crea por condiciones naturales, y posee una información traducida en un código genético, lo que ya se ha denominado como virus informático, es creado por un actor determinado, y a diferencia de basarse en una cadena de ADN, este posee información cibernética; información constituida sobre las leyes del lenguaje informático (*bits* y *bytes*)[9].

A partir de entonces, el virus informático, a diferencia de transmitirse con las condiciones y elementos del ambiente, se propaga por el ciberespacio. Por ende, cuando el código maligno llega al huésped, el daño afecta los componentes del sistema, como el virus biológico puede dañar órganos en un ser humano[10].

Ahora bien, lo que desde el enfoque anteriormente empleado se denomina como virus informático, al interior de las fronteras de las ciencias militares, en donde el concepto de arma o armamento es natural, este nuevo tipo de capacidades se ha denominado como las *ciber-armas*; término que por conjugarse al interior del ciberespacio ha recibido dicho prefijo.

Ahora bien, partiendo del estudio que Peter Lorents y Rain Ottis han desarrollado en torno a los casos que se han registrado sobre ataques concretos en el ciberespacio, se logrado establecer la existencia de diversas formulas para la construcción códigos informáticos o formas para causar efectos calculados en los sistemas del enemigo. Como lo describen directamente los investigadores del NATO Cooperative Cyber Defense Center of Excellence (CCD COE), los tipos de ataque cibernético "son una tecnología informática basada en sistemas del mismo

---

[9] 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

[10] Ibíd.

orden (software, hardware y medio de comunicación) que ha sido diseñada para perjudicar y dañar la estructura y funcionamiento de algún otro sistema"[11].

En primera instancia, el ataque de negación de servicio consiste en la generación de un código que se envía en forma imperceptible, a través de herramientas como los *virus troyanos* o los *BotNet*, a un gran número de computadores a través de la Internet[12]. Este código, posteriormente a esconderse en los diversos sistemas interconectados, espera la fecha con la cual fue programado para ejecutar su ataque, el cual consiste en transformar dicha información en una petición de acceso a una página web establecida por el agresor con el fin de que al momento de multiplicarse la misma solicitud por el número de computares infectados el sitio virtual quede deshabilitado ara el uso de su administración hasta el punto de imposibilitarlo de seguir prestando sus servicio[13].

Otra forma de ataque, es la denominada como *weapon of mass distracción* o arma de distracción masiva, las cuales buscan a través del empleo de las tecnologías informáticas manipular a la población civil de forma sicológica. Como lo describe Susan W. Brenner, las armas de distracción masiva "a través de su manipulación busca derrumbar la moral civil con el sofocación de la fe ciudadana en la eficacia de sus gobiernos. Dependiendo del tipo de ataque de manipulación, puede resultar como efecto desde la imposición de un perjuicio o la destrucción de la propiedad"[14].

Por su parte, 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

---

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

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

[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] BRENER, Susan W. Cyberthreats: the emerging fault lines of the Nation State. OXFORD University Press. New York, 2009. Pág. 45

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[15]. 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[16].

Partiendo de operaciones furtivas, también existen formas de atacar a un Estado a través de la sustracción o robo de información confidencial acerca de su armamento y sistemas de defensa nacionales, planes de guerra, estrategias militares y planeamiento de operaciones, en lo que podría considerarse como una forma de acción que proporciona su resultados por medio del ciberespacio, pero posiblemente, en la medida en que se ejecute una acción, presentará su impacto en la dimensión física aprovechando en la táctica el recurso obtenido[17].

En última instancia, se encuentran los ataques cibernéticos en contra de la infraestructura crítica del Estado, la cual en caso de verse afectada como resultado de la alteración de sus sistemas informáticos de control con un código malicioso de comando o la generación de un vinculo de control remoto, podrían representar la parálisis de un Estado trayendo consigo efectos devastadores en la vida de sus ciudadanos[18]. Tan sólo en necesario imaginar lo que pasaría si se inhabilitara la red eléctrica de una ciudad, y por ende no hubiera forma de poner en marcha las bombas de gasolina que proveen de combustible a sistemas de transporte y medios de abastecimiento de *elementos esenciales*, o bien que en

---

[15] K. ROSENFIELD, Daniel. Rethinking Cyber War. George Washington University, Elliott School of International Affairs, Washington, DC, 2010.
[16] Op. Cit. GLEBOCK
[17] CARR, Jeffrey. Inside Cyber Warfare. O' Really Media. United Sstates, 2010. Pág. 4
[18] SIERRA CABALLERO, Francisco. Guerra informacional y sociedad-red. La potencia inmaterial de los ejércitos. En: Signo y Pensamiento, Vol. XXI, Núm. 40. 2002.

determinado momento las plantas generadoras de electricidad de los hospitales agotaran de igual manera su fuente trabajo[19].

1.2 *El Ciberespacio como un nuevo campo de batalla*

Partiendo de la existencia y validez que han presentado los *poderes* en la historia militar, ha sido evidente que su aparición se debió a la tendencia del hombre por extender el empleo de la *fuerza* a nuevos escenarios de enfrentamiento con el fin de desarrollar nuevos tipos de estrategias para ganar la guerra. Consecuentemente, en una primera instancia el conflicto se desenvolvió en los teatros terrestres. Consecutivamente, la conflagración se trasladó al mar y al océano. Y finalmente, los conflictos alcanzaron la altura de la atmosfera y la estratosfera[20].

Ha sido cierto de igual manera, que la extensión de los enfrentamientos armados a nuevos escenarios del planeta Tierra, ha sido el producto directo de los procesos de desarrollo científico propio de las Naciones y por ende de sus ejércitos. No hubiera sido posible, posteriormente a constituirse el *poder terrestre*, que surgiera el *marítimo*, el *aéreo* y *espacial* si la tecnología no lo forjara como posible; es decir, sin que los barcos y submarinos alcanzaran las grandes masas de agua, y las aeronaves y dispositivos espaciales ascendieran a las alturas y a la *gravedad cero*[21].

En la actualidad, con el advenimiento y globalización de las Tecnologías de la Informáticas (computadores y las Internet) y su consecuente configuración del ciberespacio, como ya se ha observado, se ha venido configurando nuevamente, en primera instancia un escenario en el cual se ha hecho posible librar un nuevo

---

[19] GLOSH, Sumit. The Nature of Cyber-attacks in the Future: A Position Paper. En: Information Security Journal: A Global Perspective. New Jersey, 2010.
[20] LIANG, Qiao y XIANGSUI, Wang. Unrestricted Warfare. PLA Literature and Arts Publishing House. Beijing, 1999. Págs. 1-9
[21] Ibíd. Págs. 11-20.

tipo batallas desde la perspectiva regular e irregular de los conflictos armados. Y de igual manera, novedosas formas para atacar al contrario; lo cual, ha generado posturas académicas, gubernamentales y militares que apoyan la representación de esta dimensión como un quinto *dominio* de batalla[22].

El Ciberespacio se ha configurado como el entramado de tecnologías informáticas que se constituye como el pilar sobre el que se erige y sustenta un medio ambiente virtual de información y de continua interacción humana y artificial trasgrediendo el espacio geográfico del mundo y las barreras temporales de comunicación sobre éste, por lo que forma parte de todas las actividades diarias del mundo[23].

Es por lo anterior, que este nuevo escenario se ha descrito como una red interdependiente de sistemas de tecnologías informáticas, entre las que se denotan los computadores o procesadores, la Internet, y los sistemas de control de la infraestructura crítica del Estado[24].

Desde un punto de análisis mas cercanos al impacto sociológico de esta dimensión, William Gibson, autor de la obra *Neuromancer*, recreó el concepto de ciberespacio para describir cómo las computadoras y su interconexión estaba generando una red artificial de terminales que dominaba exorbitantes cantidades de información que podía ser empleada en diversos fines. Adicionalmente, y más importante aun, 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 semejantes en el otro[25].

---

[22] War in the fifth domain. The Economist, Volume 396 Number 8689, 2010. en línea], disponible en: http://www.economist.com/node/16478792

[23] TRIAS, Eric y BELL, Bryan. Ciber Esto, Ciber Aquello... ¿Y Qué? En: Air and Space Power Journal en Español, Volumen XXII, No. 3. Universidad del Aire. Alabama, 2010.

[24] UK OFFICE OF CYBER SECURITY y UK CYBER SECURITY OPERATIONS CENTRE. Cyber Security Strategy Of The United Kingdom: Safety, Security and Resilience in Cyber Space. Crown Copyright. Londres, 2009.

[25] GIBSON, William. Neuromancer. Ace Books. Nueva York, 1984

Evidenciando lo anterior, y entregando una caracterización mucho más pragmática acerca del Ciberespacio, el General y Comandante del Comando Estratégico EUA, Kevin Chilton, describe este escenario indicando que:

> Los Estados Unidos de Norteamérica al establecer sus operaciones en el contexto transnacional, ha entendido que se encuentra actuando al interior de un medio ambiente globalizado, caracterizado por la interdependencia, la incertidumbre, la complejidad y los continuos cambios. Como se ha establecido en su Estrategia de Operaciones Militares en el Ciberespacio, la seguridad y el desarrollo de la Nación en el mundo interconectado ha dependido claramente de las Tecnologías Informáticas (TI) y la Internet como elemento estratégico para fortalecer y desarrollar los instrumentos del poder nacional. Por esto, y no sólo desde la perspectiva gubernamental norteamericana, el ciberespacio logra trascender los límites geopolíticos y es bastante acertado al momento de integrar las operaciones de la infraestructura crítica, de gobernabilidad, de comercio y de seguridad nacional por supuesto[26].

A nivel general, una clara representación de lo anterior es, que los gobiernos se preocupen constantemente por invertir en la construcción de *E-Goverment* para generar una cercanía con la ciudadanía y alcanzar estándares óptimos de gestión, que los flujos de valores y capital circulen por el globo gracias a la interconexión de las *bolsas* y mercados nacionales, que los sistemas informáticos de control de infraestructuras criticas del Estado y privadas se puedan controlar y monitorear a distancia, que los controladores de tráfico terrestre y aéreo funcionen en la Internet y que el sector privado y las personas apoyen sus actividades rutinarias en las capacidades de las TIC, entre otros casos que se pueden destacar.

Ahora bien, pero qué es lo que describe al ciberespacio como una dimensión en la cual la defensa y seguridad estatal, y por ende su soberanía se vea amenazada.

---

[26] USAF Commander, CHILTON, Kevin. Cyberspace Leadership: Towards New Culture, Conduct, and Capabilities. En: Air & Space Power Journal, Fall 2009. Pág. 7

Fernando Sampaio, logra hacer un acercamiento a la respuesta del interrogante, formulando 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 vulnerabilidad de su defensa y seguridad, en tanto que este factor puede ser explotado perfectamente por el enemigo con el fin de poder atacar las redes de comando y control de un sin número de servicios públicos, 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 materialmente[27]

La cuestión es, que 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 entendidas como tal.

Entonces resulta que, la superioridad tecnológica, reproducción, posicionamiento y empleo estratégico de armamento convencional asegura, con mayor probabilidad, que los ejércitos y Estados posean una superioridad al momento de interponer sus modelos de defensa y seguridad ante las amenazas que los aquejan. No obstante, cuando se posee un volumen cada vez mayor de tecnologías informáticas al nivel gubernamental y militar, y además se parte de que la sociedad y la infraestructura crítica se encuentran estrechamente vinculadas al mismo sistema, se traduce en que el Ciberespacio es contundentemente un punto de vulnerabilidad para un país[28].

Tomando como referencia la Teoría delos Cinco Anillos de John Warden, el panorama se clarifica aun más. Warden concentra su planteamiento en la idea de que el Estado se encuentra compuesto por cinco anillos que representan cada uno una parte vital del mismo; las cuales se traducen en, *los mecanismos de combate*,

---

[27] 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.

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

la población, *la infraestructura crítica*, *los elementos orgánicos y sintéticos esenciales* y *los líderes gubernamentales*.

De esta manera, cuando se aterriza sobre el escenario descrito, en donde los nódulos de subsistencia de una Nación se encuentran integrados al ciberespacio, y sabiendo ya que se pueden desarrollar ciberataques con las tecnolgías informáticas, se esclarece, cómo desde la teoría Warden la estructura del Estado se encuentra en gran riesgo; ya no por las capacidades del poder aéreo como fue construido el postulado originalmente, sino con las capacidades que ofrecen los computadores y el ciberespacio, y que los anillos se encuentran vinculados a estos.

Una clara representación de esta clase de riesgo exponencial se observa en como los Estados Unidos, tan sólo en la esfera de la defensa: aproximadamente el 97% de las comunicaciones militares son transmitidas por redes y servicios comerciales; EE.UU adquiere la mayoría de los microchips que implementa en los sistemas informáticos de sus milicias en Estados que fácilmente podrían estar o ser permeados por sus enemigos; y de igual forma, no se puede obviar el hecho de que los planos de desarrollo del armamento convencional, los cuales son evidentemente fuente de defensa en el mundo físico, se encuentran almacenados magnéticamente en los sistemas de la industria civil[29].

Entender la naturaleza del ciberespacio desde una óptica militar, implica, para obtener una mejor perspectiva, analizar el concepto desde la lógica del actor vulnerado, es decir, posicionándose a partir de la mirada del objetivo. De esta manera, se entiende con mayor claridad el significado de atacar a un Estado Nación mediante las tecnologías informáticas y a través de la virtualidad.

---

[29] BISHOP, Matt y O. GOLDMAN, EMILY. The Strategy and Tactics of Information Warfare. En: Contemporary Security Policy, 24. California, 2010.

En concordancia, es posible hacer una aproximación al hecho de que si bien es el ciberespacio el medio a través del cual se lleva a cabo la agresión, el perpetrador de éste, ya sea un actor estatal o terrorista, no diseña su ataque para afectar concretamente los sistemas informáticos de su enemigo.

Al emplear un ciberataque, el fin buscado es que la agresión se traslape de forma contundente al mundo real, ya sea generando efectos sicológicos, caos organizacional y civil, o bien un ataque dirigido a la infraestructura crítica, y por ende, sobre la población si se llegara a poner en riesgo el funcionamiento adecuado de la misma[30].

Por lo anterior, teóricos de la materia han establecido que si bien esta dimensión puede catalogarse como un escenario en donde el Estado puede ver amenazada su soberanía, es gracias a que de manera similar a como se constata en los poderes militares preexistentes, al utilizar las tecnologías informáticas como armas en el ciberespacio, se está recreando el tradicional empleo de un dispositivo bélico en un escenario geográfico o físico de conflicto con el fin propiciar un efecto en el enemigo[31].

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 tiene efectos devastadores en aquellos escenarios donde son implementadas, lo que se busca con las tecnologías informáticas y el ciberespacio también radica en destruir o desarticular los centros de gravedad del contrario con el objeto de deshabilitarlo como contendiente en el conflicto[32]

---

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

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

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

De esta manera, cómo no anticipar parálisis o catástrofe de un Estado Nación cuando el enemigo puede hacerse bajo el control de sus reactores nucleares, o de sus sistemas controladores de tráfico aéreo, de sus redes de comunicación, de la información estratégica de bases y sistemas de defensa militares, de los flujos de capital de las bolsas de valores, o bien, de los sistemas de transporte[33].

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

2. CAPÍTULO SEGUNDO

EL CIBERTERRORISMO: UNA AMENAZA LATENTE PARA LOS ESTADOS EN EL SIGLO XXI

"As we approach the 21st century, our foes have extended the fields of battle from physical space to cyberspace, from the world's vast bodies of water to the complex workings of our own human body. Rather than invading our beaches or launching bombers, these adversaries may attempt cyber attacks against our critical military systems and our economic base,"

Bill Clinton

Annapolis, mayo 22 de 1998

La guerra se ha transformado. El enfrentamiento de los ejércitos de los Estados-Nación en teatros de guerra simétrica es cosa del pasado. Desde hace ya unas décadas atrás, en especial desde el mundo bipolar de la Guerra Fría, los ejércitos y organismos de seguridad nacionales se enfrentan en contra de enemigos clandestinos que enmarcan sus luchas en las desigualdades socio-económicas, en las disparidades étnicas o religiosas, en las luchas de liberación nacional o anti-ocupación, en el sustento de la economía de guerra, o simplemente, y en mayor medida, en el terror[34].

Por supuesto, uno de los actores predominantes al interior de este, han sido las agrupaciones terroristas. Si bien el terror como táctica y estratagema en los teatros de operación se ha empleado como elemento a lo largo de la historia, es a partir de la mitad del siglo XX que este elemento se comienza a emplear como forma de acción política, y como medio de lucha de agrupaciones organizacionalmente establecidas.

---

[34] FOJÓN, José Enrique. "Vigencia y limitaciones de la guerra de cuarta generación" Real Instituto Alcano de Estudios Internacionales y Estratégicos. 2005. [en línea], Disponible en: http://www.realinstitutoelcano.org/analisis/916/916_Fojon.pdf. [consultado: 10 de febrero de 2010]. Págs. 2-4

El Ciberterrorismo es un fenómeno que ha hecho presencia al interior de los conflictos armados contemporáneos. Con la globalización de las Tecnologías Informáticas a partir de la década de los noventas del siglo pasado, y sus bajos costos y fácil acceso en los mercados comerciales han permitido que las organizaciones terroristas se valgan del ciberespacio para sopesar las desventajas propias de la asimetría del conflicto.

Las agrupaciones terroristas, o bien, subversivas que han empleado el uso del terrorismo como estrategia para apoyar sus guerras y alcanzar sus objetivos políticos, han detectado como una herramienta fundamental para su accionar a los medios de comunicación masiva a través de la historia.

Si bien los grupos terroristas, actúan bajo la determinación de acciones de destrucción masiva mediante el empleo de armamento convencional, y no convencional, sobre la infraestructura crítica y la sociedad, el fin último es sembrar el caos y terror en la mente de las personas.

Ahora, cabria cuestionarse, sí el terrorismo es un arma sicológica en su expresión máxima, que sería de las organizaciones ilegales que lo emplean sí los medios de comunicación no estuvieran allí para difundir la perpetración de sus atentados sobre toda la sociedad; por supuesto, en la era de la información y la Globalización, sobre la sociedad mundial.

En consecuencia, siguiendo el recorrido del terrorismo a través de los años, es posible observar como este fenómeno se ha valido de medios como la radio, la prensa escrita y la televisión para difundir la consumación de hechos fastuosos, en *pro* de radicar el miedo en distintas sociedades como mecanismo de presión política hacia las instancias gubernamentales que pueden cumplir sus demandas.

Ahora bien, el escenario y lógica que ha traído consigo la implementación de las tecnologías informáticas y el ciberespacio, ha logrado dar un giro importante en el *modus operandi* de estos actores.

En primera instancia, porque a diferencia de los medios de comunicación precedentes, el terrorista ya no depende de que las cadenas de noticias decidan captar los actos de agresión llevados a cabo, y de igual manera, qué de todo lo que sucede en su transcurso es divulgado. Ahora las organizaciones de este orden, gracias a que pueden adquirir computadores y conexiones a Internet de manera factible en el mercado comercial, y a que la internet gracias a su naturaleza democrática permite a cualquier persona publicar todo tipo de contenidos, poseen el control del medio de comunicación *más* masivo que ha poseído la humanidad; el terrorista puede, bajo estas condiciones, tener el control de uno de los elementos principales de terrorismo, el acceso a la mente de las masas.

Por otra parte, este no ha sido el único rédito que los terroristas han logrado obtener del ciberespacio. Gracias las bondades ya expresadas de esta dimensión, estos actores de los conflictos asimétricos han podido establecer mecanismos de coordinación de sus operaciones de manera globalizada, han construido sitios en el ciberespacio en donde generan mecanismos de guerra política contra la institucionalidad, constituyen medios para que los partidarios de sus causas hagan donativos mediante dinero electrónico, reclutan y entrenan a sus integrantes. En síntesis, herramientas que permiten sopesar su asimetría frente a la contraparte.

En consecuencia, cuando se aborda teóricamente el fenómeno del ciberterrorismo, es posible establecer que esta cara del terrorismo se fundamenta, por una parte, como medio logístico para potenciar las practicas tradicionales de la agrupación al trasladarlas al ciberespacio mediante el empleo de las Tecnologías Informáticas. Y en segundo lugar, como un medio estratégico operacional y táctico

para llevar a cabo ataques directos a los Estados, sus infraestructuras criticas y su población.

En este sentido, el propósito del presente capítulo consistirá en tomar como referencia de análisis los elementos más significativos del fenómeno del ciberterrorismo. En primera medida, la incidencia comunicacional que trajo consigo el ciberespacio para los terroristas. Y posteriormente, las nuevas capacidades adquiridas por estos actores en esta misma dimensión; y claro está, mediante el empleo de las tecnologías informáticas.

2.1 *La lógica del terrorismo y medios de comunicación: el control del ciberespacio para fines sicológicos*

Rafael Guarín en su artículo, *Medios de comunicación, terrorismo y antiterrorismo*, menciona el principio, de que "la acción política, cualquiera que sea su signo ideológico, busca la captación de los ciudadanos para acceder al poder, influenciarlo o ejercerlo [...] Acudiendo a mensajes, símbolos y actos con contenido político se consigue el consentimiento ciudadano, o bien la coacción, amabas caras del poder político"[35]

La lógica del terrorismo, y tal vez con más rigor que otras formas de expresión política, se ha tenido que acoplar a este canon. Tomando como referencia la completa definición del terrorismo que ha recreado el experto en la materia, Andrés Molano Rojas, se puede percibir esta realidad:

> El terrorismo es un método de acción política violenta que tiende a articularse en procesos de larga duración para compensar asimetrías en el contexto de un conflicto y que opera provocando una destrucción o caos suntuario, según un modelo eminentemente transitivo y cuyo efecto psicológico es superior a sus efectos materiales (por cuanto elige objetivos con alto valor histórico), a efectos

[35] GUARÍN, Rafael. Medios de comunicación, terrorismo y antiterrorismo. Editorial, Escuela de Inteligencia y C/I "BG Ricardo Charry". Bogotá. 2009. Pág. 118

> de transmitir un mensaje para afectar grandes audiencias, y cuyos agentes impulsan principalmente determinadas pretensiones políticas[36]

Realizando un recorrido histórico a partir del inicio del siglo XX, es posible observar como, en lo que entonces todavía seguía siendo la Rusia zarista, los registro denotaron que las acciones terroristas que llevó a cabo el partido político bolchevique en contra de la dinastía Romanov y el sistema político, no hubieran tenido el mismo impacto en el pueblo si el colectivo revolucionario no hubiera empelado la prensa escrita y la radio para difundir la perpetración de los mismos.

De la misma manera, no se puede olvidar como, y aun sin aterrizar en el escenario del mundo globalizado contemporáneo, las transmisiones en directo, y la posterior divulgación de las imágenes televisivas del atentado terroristas consumado por el Al Fatah (Movimiento Nacional de Liberación de Palestina) en los Juegos Olímpicos de Munich en 1972, y por supuesto su trágico desenlace, causaron conmoción en diversas sociedades.

Ahora, trasladándonos al esbozo del siglo XXI donde confluyen mundialmente comunicaciones de prensa, radio, televisión y por supuesto se cuenta con el ciberespacio (canal único pero aglutinador de los anteriores *–multimedia-*), los terroristas de la red internacional de Al Qaeda dejaron anonadado al mundo entero al colisionar los aviones comerciales en las *tweens towers* del World Trade Center de Nueva York, y una posterior aeronave en el Pentágono de los EE.UU.

Los anteriores hechos se sustentan, como lo expresa Guarín, en que la relación específica entre los grupos terroristas y los medios de comunicación ha sido connatural a su nacimiento y su naturaleza. Como se expresa a continuación:

> La prioridad del terrorista está en el pensamiento y este se crea a partir de la información que los ciudadanos reciben de parte de los medios de

[36] MOLANO ROJAS, Andrés. El nombre y la cosa: aportes al debate definicional sobre el terrorismo. Editorial, Escuela de Inteligencia y C/I "BG Ricardo Charry". Bogotá. 2009.

> comunicación" [...] "Si se examina con cuidado se identifica que la comunicación es el hilo conductor de la lógica terrorista. No sirve de nada cometer el atentado y mucho menos amenazar con su realización si la población no llega a conocer ni lo uno, ni lo otro. La eficacia del empleo de la violencia en este caso depende de que el mayor número de personas conozca el hecho, así, sin medios de comunicación no existe la cadena de consecuencias buscada por los terroristas[37]

Claramente, cuando se analiza el escenario en el cual los grupos de esta naturaleza han trascendido a emplear medios de comunicaciones mucho más poderosos que la radio, la prensa y televisión, como lo es evidentemente el ciberespacio, los resultados propios de la interacción entre el *fenómeno* y el *canal* ha logrado sobrepasar sus propias fronteras[38].

Retomando a Ortiz, las características que hicieron del ciberespacio una verdadera revolución para los conflictos armados, y en especial para actores propios como los grupos terroristas, han sido: por una parte, a que las Tecnologías Informáticas poseen bajos costos y se adquieren fácilmente en el comercio civil o los mercados *on-line*; y en segundo lugar, por que los usuarios de estas tecnologías tienen la potestad de crear contenidos o alterar el ciberespacio con base en sus criterios[39].

Por ende, a partir de la conformación del ciberespacio, la tecnología que permite acceder a él no ha dejado de potencializar sus herramientas, y por supuesto, crear constantemente nuevas aplicaciones. Sumado a este factor, la modernización de los equipos informáticos, les han permitido a los usuarios del ciberespacio

---

[37] GUARÍN, Rafael. *Medios de Comunicación, Terrorismo y Antiterrorismo*. Perspectivas de Inteligencia. Colección Centro de Investigación en Guerra Asimétrica (CIGA). Número 3. Editorial, Escuela de Inteligencia y CI "BG Ricardo Charry Solano". Bogotá-Colombia. Octubre de 2009. Pág. 120

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

[39] ORTIZ, Román. "Amenazas transnacionales a la seguridad, tecnología e ingobernabilidad: el caso de Colombia" [en línea], disponible en: http://cooperacioninternacional.com/descargas/prueba.pdf [consultado: 9 de febrero de 2010]

establecer sus labores y estrategias propias en las nuevas formas de uso y potencialidades de la Internet; por supuesto, lógica bajo la cual se suscribe las agrupaciones terroristas, y así dar paso al fenómeno terrorismo ciberespacial[40].

A diferencia de las dinámicas mediáticas del siglo precedente, donde los terroristas dependían de que los medios llevaran a cabo la trasmisión televisiva de su atentado para cumplir el objetivo, ahora los terroristas tienen el control de la Internet, y por ende pueden modificar el ciberespacio convenientemente[41].

Por esto, grupos terroristas peruanos, como el Sendero Luminoso y el Movimiento Revolucionario Tupac Amaru, emplean este espacio virtual para generar terrorismo a través de la divulgación de contenidos alusivos a la violencia, como imágenes y videos con argumentación política de odio y terror, con el fin de construir mecanismos de ataque psicológico que desvirtúen la mentalidad de la comunidad global frente a su verdadero *modus operandi*[42].

De la misma manera, explorando las abismales posibilidades del ciberespacio, las redes del terrorismo del Yihad islámico han llegado a consolidar efectivas herramientas para su causa. De la mano de partidarios o militantes "civiles" a nivel mundial, las células yihadistas que coexisten en África, el Medio Oriente, y Asia han logrado concretar mecanismos complejos para "externalizar" su trabajo propagandístico a través de la divulgación de videos acerca de sus ejecuciones y ataques terroristas consumados, los cuales son "colgados" y administrados [por sus colaboradores] en foros y páginas de la red que hoy en día ya han alcanzado

---

[40] TORRES, Manuel. "Terrorismo yihadista y nuevos usos de Internet: la distribución de propaganda (ARI)" [en línea], disponible en: http://www.realinstitutoelcano.org/wps/portal/rielcano/contenido?WCM_GLOBAL_CONTEXT=/elcano/elcano_es/zonas_es/terrorismo+internacional/ari110-2009, [consultado: 9 de febrero de 2010]

[41] NAGPAL, Rohas. Cyber Terrorism in the Context of Globalization. II World Congress on Informatics and Law. Madrid-España, septiembre de 2002.

[42] BOYD, Cristina. "Internet: el refugio de grupos terroristas" [en línea], disponible en: http://intelligenceservicechile.blogspot.com/2009/08/internet-el-refugio-de-grupos.html [consultado: 10 de febrero de 2010]

una estabilidad, reconocimiento, y eficacia sin precedente; lo cual no es nada más que la divulgación del terror y los alcances violentos de dichos actores, a través del ciberespacio [43].

Igualmente, de la mano de partidarios o militantes a nivel mundial, las células yihadistas en África, el Medio Oriente, y Asia han establecido mecanismos para "externalizar" su trabajo propagandístico a través de la divulgación de videos acerca de sus ataques terroristas, los cuales son administrados por estos colaboradores en foros y páginas de la red[44].

Ejemplo fehaciente de este tipo de uso del ciberespacio, entre otros tantos[45], fue el lamentable caso de ejecución tortuosa que se le dio al periodista del 'The Wall Street Journal', Daniel Pearl, por parte de una célula terrorista paquistaní en la ciudad de Karachi en 2002, en la cual se documentó en un video, que rápidamente fue difundido por la red, como este personaje fue decapitado por integrantes de la misma, con el fin de transmitir un mensaje de terror al pueblo norteamericano por la incursión armada que llevaba a cabo su gobierno en este país del Medio Oriente[46].

2.2 Las nuevas capacidades de los grupos terroristas en el ciberespacio

A partir de diversas perspectivas, el Ciberterrorismo es el elemento que ha otorgado a los terroristas la posibilidad de existir en un mundo globalizado y con objetivos globalizados (en algunos casos). Partiendo de las asimetrías connaturales de los conflictos irregulares, el ciberespacio le ha permitido a agrupaciones terroristas como Al Qaeda funcionar en red a lo largo del mundo, o

---

[43] TORRES. Óp. Cit.,

[44] ECHAVARRÍA, Carlos. La innovación yihadista: propaganda, ciberterrorismo, armas y tácticas. Grupo de Estudios Estratégicos GEES. Análisis No. 7416, 2009

[45] Al igual que la ejecuciones de Nicholas Berg, Eugene Armstrong, y Jack Hensley.

[46] AGENCIAS. "Musharraf ordena la detención de todos los miembros del grupo que degolló al periodista Daniel Pearl" .El mundo. [en línea], disponible en: http://www.elmundo.es/elmundo/2002/02/21/internacional/1014327615.html

bien organizaciones de carácter más regional como las FARC, conectarse con el mundo entero e intercambiar elementos con organizaciones del mismo tipo[47].

Entrando a una perspectiva mucho más profunda en materia cibernética en torno al terrorismo, se puede anticipar que ya no sólo se trata del empleo de un medio de comunicación, sino de la consolidación eficiente y efectiva de herramientas a través del ciberespacio que aportan importantes elementos de subsistencia y éxito a la causa de estos actores; en consecuencia, elementos que de una forma u otra acercan al terrorista un paso más a sus objetivos en los escenarios reales de los conflictos, es decir, la perpetración de acciones propias de esta doctrina.

Como lo formuló Barry Collin, del Institute for Security and Intelligence in California, partiendo del hecho de que los grupos terroristas han sabido explotar a cabalidad las cualidades del mundo informático, y concretamente el ciberespacio como un escenario al cual se pueden traslapar diversas formas de lucha, el Ciberterrorismo debe entenderse como la sinergia entre cibernética y terrorismo[48].

Dan Verton, aterrizando un poco más el concepto, ha evidenciado que el Ciberterrorismo es "un juego de inteligencia que aplica las tácticas violentas y pragmáticas del viejo mundo a las realidades y vulnerabilidades de la nueva era tecnológica. [...] El terrorismo ahora implica atacar de forma indirecta, inteligente y bien planeada los tendones de una nación."[49]

Finalmente y de forma complementaria, Mark Pollitt dice, que "el Ciberterrorismo es el ataque premeditado, sobre una base política y en contra de la información, los sistemas de los procesadores, los programas de los procesadores y datos el

---

[47] WILSON, Clay. Computer Attack and Cyberterrorism: Vulnerabilities and Policy Issues for Congress. CRS Report for Congress. Congressional Research Service. The Library of Congress. Washington, 2005.

[48] KUSHNER, Havey. Encyclopedia of Terrorism. Sage Publication. Londres, 2003.

[49] VERTON, Dan. La Amenaza invisible del ciberterrorismo. McGraw Hill. 2004

cual se traduce en violencia en contra de objetivos no combatientes, por acción de grupos sub-nacionales o grupos clandestinos"[50]

Bajo ésta lógica, se está haciendo alusión a cómo prácticas como la obtención de información estratégica, la guerra sicológica, el reclutamiento, el financiamiento y el adoctrinamiento al ser trasladadas al ciberespacio, le permite a los actores en mención potenciar estas mismas gracias a las características de este escenario virtual de alcance global, que rompe las barreras del tiempo y el espacio, y que maneja uno de los bienes más preciados en la actualidad; la información[51].

Por supuesto, una de esas potencialidades que han podido obtener los grupos terroristas en el ciberespacio ha sido la coordinación de acciones a nivel global.

Para la organización terrorista de las Farc, la cual para desarrollar sus operaciones de ataque a la institucionalidad, FF.MM y población civil colombiana se ha organizado prioritariamente en estructuras móviles, y posee milicias urbanas, la internet se ha presentado como medio facilitador para la coordinación de sus atentados terroristas. Adicionalmente, el uso que esta agrupación le ha dado a su red de comunicación en el ciberespacio, ha contribuido a diversas actividades como su cobro de impuesto revolucionario, la compra de armamento en el mercado negro, y ciertas actividades del orden diario que facilita sus métodos administrativos[52].

Otro caso que refuerza la especialización y estructuración que llevan a cabo los terroristas en Internet, es la creación del *comité de comunicación y publicidad* que la organización Al Qaeda ha conformado para manejar específicamente sus

---

[50] POLLITT, Mark. Cyberterrorism - Fact Or Fancy?. FBI Laboratory and George Washington University. Computer Fraud & Security, Volume 1998, Number 2, 1998

[51] MATUSITZ, Jonathan. Cyberterrorism: how can american foreign policy be strengthened in the information age?. American Foreign Policy Interests, 27: 2, 2005.

[52] SÁNCHEZ MADERO, Gema. Internet: una herramienta para las guerras en el siglo XXI. Military Review (edición hispanoamericana). Centro de Armas Combinadas. Fuerte Leavenworth, Kansas. Julio-agosto 2010.

operaciones en este espacio; cabe mencionar que es tal la importancia que ésta le han otorgado a dicha comisión, que se encuentra jerárquicamente un escalón abajo del Emir-General y de la asamblea consultiva[53].

Haciendo alusión de nuevo a Al Qaeda, no podía eximirse el acontecimiento que de forma más concreta y representativa ha atentado contra la seguridad y defensa de un Estado; el ataque al World Trade Center de los Estados Unidos de Norteamérica el 11 de septiembre de 2001. Este acontecimiento ha sido la muestra más representativa de cómo una agrupación terrorista ha hecho empleo del ciberespacio para coordinar un atentado a gran escala[54].

Bajo esta egida, la búsqueda de las escuelas de aviación que entrenarían a los suicidas islámicos, la reserva y compra de los pasajes de avión de la compañía American Airlines y United Airlines en su sitio web, y sobretodo, la coordinación de toda la estratagema y faces del atentado fueron planeadas a través de cuentas de correo electrónico del dominio de *Yahoo* y *Hotmail*, y chats[55]; claro está, haciendo uso de métodos de encriptación de la información implementados por la organización para nos ser detectados por los organismos de seguridad del país norteamericano[56].

La coordinación y comunicación al nivel mundial, también ha permitido que importantes líderes terroristas ya no tengan que tomar el riesgo de ser capturados o eliminados al programar reuniones presenciales en algún lugar del mundo. Por lo anterior, los mensajes cifrados a través de cuentas de correo electrónico se han convertido en el pilar de dicha práctica. Ha sido tan importante este factor para las organizaciones terroristas, que sus encargados y expertos en tecnologías informáticas han dedicado grandes esfuerzos por implementar intrínsecos

---

[53] Guarín. Óp. Cit., Pág. 123

[54] VERTON, Dan.. *La Amenaza Invisible del Ciberterrorismo*, McGraw Hill, 2004, p. 16-17

[55] L. THOMAS, Thimoty. Al Qaeda and the Internet: the Danger of "Cyberplanning". Parameters No. 33, ProQuest Military Collection, 2003

[56] CARRILLO PAYÁ, Pedro. *Terrorismo y Ciberespacio*. [en línea], disponible en: http://www.assessorit.com/web/images/stories/prensa/pcarrillo-paper.pdf

sistemas para evitar la interceptación de sus mensajes; como lo es la encriptación, el empleo de páginas web privadas donde se infiltran mensajes y por último, técnicas como la estenografía[57]

El Ciberterrorismo, en su rol de reclutamiento y adoctrinamiento, también se ha enfocado proporcionar la información necesaria a sus militantes y componentes armados para que no pierdan el valor militar y los valores políticos y simbólicos de su causa. Desde esta línea, se busca poder difundir canciones y documentos de carácter político que enaltecen el movimiento, revistas on-line, programas de radio e imágenes[58]. Adicionalmente estos elementos, en la mayoría de casos reseñados van acompañados de una estrategia lingüística que busca traducir dichos contenidos a idiomas foráneos al que emplea la organización, y así, poder generar una captación y aceptación social al nivel mundial[59].

Partiendo de que las Farc llevan un arduo recorrido de explotación del ciberespacio, se puede esgrimir que en el sitio web ANNCOL se ha conformado como su página oficial, permitiéndole así divulgar a este grupo, videos, música, documentos e información que tergiversa las acciones del Estado y las Fuerzas Armadas, y comunicados de prensa que buscan enaltecer en la sociedad no solo su causa subversiva, sino gobiernos y movimientos políticos internacionales que han demostrado estar en contravía de la soberanía e intereses nacionales de Colombia[60].

---

[57] L. THOMAS, Thimoty. Al Qaeda and the Internet: the Danger of "Cyberplanning". Parameters No. 33, ProQuest Military Collection, 2003

[58] S. TIBBETTS, Patrick. Terrorist use of the internet and related information technologies. Fort Leavenworth, KS: US Army Command and General Staff College. 2002. http://cgsc.cdmhost.com/u?/p4013coll3,213

[59] JOSHI, Akshay. The Scourge of Cyber-Terrorism. Strategic Analysis, 24: 4, 2000.

[60] COHEN-ALMAGOR, Raphael. The Terrorists' Best Ally. Simon Fraser University. Canadian Journal of Communication, Volumen 25 No. 2. Vancouver-Canada, 2000.

Otra de las expresiones del ciberterrorismo se ha configurado en torno a la facilidad de obtención de información de *inteligencia* (guardadas las diferencias naturales del concepto por supuesto), y métodos de entrenamiento.

Cualquier usuario de internet puede testificar que dentro de la información que se encuentra en la red, mucha de esta ofrece contenido personal de los objetivos humanos de estas redes, también fotografías, mapas y planos de lugares y estructuras que podrían se punto de ataque[61]. De igual manera, programación y ubicación de actividades políticas de alto impacto; lo cual para los terroristas se ha traducido como un sistema que nutre de una gran cantidad de información al momento de planear sus operaciones[62].

Paralelamente, no se puede obviar que en cuanto a canales de entrenamiento, el ciberterrorismo se ha valido de complejos y eficientes canales de comunicación, entre la organización y sus militantes, como lo son foros secretos y encriptados, con el fin de estar informando a su estructura organizacional las directrices políticas y operativas de la organización, la difusión de manuales para la construcción de artefactos explosivos, información referente a como se debe escapar de un teatro de operaciones después de realizado el atentado, cómo realizar secuestros efectivos, o procedimientos específicos en caso de detención policiaca, entre otras formas de acción[63]

Ahora bien, partiendo del principio de que dimensiones como el ciberespacio difícilmente pueden controlarse respecto a la información que los usuarios

---

[61] S. TIBBETTS, Patrick. Terrorist use of the internet and related information technologies. Fort Leavenworth, KS: US Army Command and General Staff College. 2002

[62] CONWAY, Maura. Reality Bytes: Cyberterrorism and Terrorist 'Use' of the Internet. Department of Political Science of Trinity College. Dublin, 2002

[63] WEIMANN, Gabriel. Cyberterrorism How Real Is the Threat? Especial Report. United States Institute of Peace (USIP). Washington D.C, 2004

difunden a través de ésta, los grupos ciberterroristas no han encontrado ningún obstáculo para establecer mecanismos de guerra política[64].

A través de la guerra política en la red, el terrorismo está ganado una importante ventaja frente a los Estados y fuerzas institucionales que los combaten. Los grupos terroristas están consiguiendo difundir una imagen de impunidad y fortaleza en el mundo entero, lo que en términos concretos, ha significado más una deslegitimación institucional frente a sus campañas antiterroristas y la consolidación del temor permanente en las personas[65]

Otro factor merecedor de ser resaltado para comprender la inmersión del terrorismo en el ciberespacio es la consolidación de fuentes de financiamiento de causas. Se ha logrado establecer que agrupaciones como el IRA (Irish Republican Army) han puesto en práctica mecanismos, a través de sus páginas de internet, para que los visitantes de las mismas pudieran hacer donaciones mediante el uso de sus tarjetas de crédito. Otras como Hamás, por su parte, ha recaudado fondos de financiamiento por medio del sitio web diseñado para su organización benéfica, la *Fundación Tierra Santa para la Ayuda*. Por ultimo, en el caso de los terroristas chechenos se empleo el método de la publicación en el ciberespacio de los números de diversas cuentas bancarias para que sus colaboradores depositaran sus donativos en ellas[66].

En última instancia, cuando partimos del escenario de las capacidades adquiridas por los grupos terroristas, no se podría dejar de lado la más importante de todas; los ataques cibernéticos. Adicionalmente a que estos actores han logrado construir importantes mecanismos a través del ciberespacio con el fin de ajustarse a los

---

[64] PEREŠIN, Anita. Mass Media and Terrorism. Media Research: revista científica para el periodismo y los medios de comunicación de Croacia. Zagreb, 2007.

[65] VÁZQUEZ LIÑÁN, Miguel. La propaganda de guerra en Internet. En: Historia y Comunicación Social, número 5, 2000.

[66] P. TRACHTMAN, Joel. Global Cyberterrorism, Jurisdiction, and International Organization. Conference on the Law and Economics of Cybersecurity. George Mason University School of Law. 2004

parámetros y características del mundo globalizado, y sopesar la asimetría que poseen frente a las Fuerzas Militares y de seguridad que los combaten, el elemento determinante del ciberterrorismo radica en su capacidad de generar ciberataque a los Estados con los que mantienen su lucha[67].

Bajo esta perspectiva, ya no se involucra en el análisis prácticas terroristas tradicionales de tipo logísticas o de inteligencia, sino que se atiende a la concepción más pura de terrorismo desarrollándose en el ciberespacio. Como ha establecido Sumit Glosh, si bien en la Internet la mayoría del tiempo se está interactuando con información visible, es la información que pasa desapercibida al usuario la que le permite a los ciberterroristas acceder a sistemas informáticos que pueden contener información que al ser empleada flagrantemente puede ocasionar graves daños y perdidas humanas[68].

Desde esta concepción pura de terrorismo actuando en el ciberespacio, se maneja las hipótesis de amenaza de destrucción o caos masivo del Estado y su ciudadanía. Como lo expresa Berkowitz, el echo de que las tecnologías informáticas se hayan presentado como *causa* y *efecto* de la globalización, mientras que, y como medio de comunicación unieron al mundo, de igual manera generaron que estas tecnologías tuvieran que ser implementadas paulatinamente en todos los procesos llevados a cabo por la sociedad, el Estado y el sector privado[69].

Esto ha permitido, que actualmente la mayoría de procesadores que pertenecen al sector gubernamental, militar, de defensa y seguridad, de la infraestructura crítica y la sociedad de los Estados estén conectados al ciberespacio, canal por el cual

---

[67] WOLTHUSEN D., STEPHEN. Asymmetric Information Warfare: Cyberterrorism Critical Infrastructures. Security Technology Department. Fraunhofer-IGD. Darmstadt-Alemania, 2002

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

[69] 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

alguna de estas instancias podría tener un alto riesgo de ser ciberatacada por alguna organización terrorista. Enviar la información adecuada a través del ciberespacio hasta un objetivo seleccionado podría tener diversas consecuencias. Perfectamente se podrían violar los mecanismos de seguridad que protegen archivos con información estratégica ultra-secreta, o se podría dañar páginas gubernamentales para inhabilitar su uso y cambiar información[70].

Desarrollando un análisis del accionar terrorista, es posible percibir que bajo las posibilidades que ofrece el ciberespacio y la naturaleza informática del mismo sistema, la teoría que se maneja con mayor fuerza al momento de generar modelos y políticas de Ciberdefensa, es aquella en la cual el Ciberterrorismo logra atacar directamente los sistemas informáticos de la infraestructura crítica del Estado, por lo cual se produciría, entre otros ejemplo, el recalentamiento de un reactor nuclear, la apertura de compuertas de una hidroeléctrica, el sabotaje del tráfico aéreo y la parálisis de la bolsa de valores[71].

Como lo relata Bishop y Goldman, ya han sido varios, aunque no demasiados los casos en los cuales un grupo terrorista ha estado implicado en un ciberataque. En primera medida se registró en 1998 como los extintos *tigres tamiles* bombardearon con códigos malignos las páginas gubernamentales de Sri Lanka, imposibilitando a los web máster de estos sitios controlarlas y repararlas. De igual manera, también se registró que durante la guerra de Kosovo, diversos grupos terroristas del conflicto atacaron en varias ocasiones las páginas en Internet de la OTAN[72].

Finalmente como último punto a resaltar, iniciando el año 2000, un grupo de jóvenes israelís expertos en informática, presuntamente vinculados al Gobierno, o bien profesando el nacionalismo propio de la sociedad sionista frente a la *causa*

---

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

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

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

palestina, construyeron una página web programada para interferir u obstruir sitios en el ciberespacio que le pertenecieran entonces a las organizaciones terroristas islamistas, nacionalistas, y yihadistas de Hizbolá y Hamás[73].

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 afectados por los ataques palestinos[74].

---

[73] 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.
[74] Ibíd.

CAPÍTULO TERCERO
LA CIBERGUERRA: ¿LA REPRESENTACIÓN DE UN NUEVO *PODER* DE ATAQUE MILITAR?

"El supremo Arte de la Guerra es someter al enemigo sin luchar"
Sun Tzu, año 512 A.C.

Al igual a como los actores no estatales, protagonistas de las guerras catalogadas como de *cuarta generación*, *nuevas guerras* o de la *tercera ola* se han inmerso en el ciberespacio para incidir y generar control sobre éste con fines terroristas, los Estados, y para este caso concreto sus fuerzas militares, no se han rezagado del proceso.

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* o *reglas de 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"[75]

---

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

Hilado a 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*.

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

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. La aparición de los procesadores personales y la Internet como producto del adelanto informático de la Tercera Revolución

Industrial, la posterior recreación de lo que se ha denominado como el Ciberespacio[76] y que las FF.MM actúen ofensiva y defensivamente a través y gracias a los anteriores, permiten entrever la posibilidad de evidenciar la configuración de un nuevo *poder militar*: el *poder cibernético*.

Partiendo de esta premisa, la presente investigación se ha planteado el objetivo de analizar 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 las tecnológicas informáticas como armamento para las 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.

3.1 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 maquinas[77].

En el estudio *Cyberwar is Coming*, realizado por John Arquilla y David Ronfeldt se parte de que si el prefijo ciber, o bien cibernetica, conyeva a la accion de controlar, conceptos como el de Leitenkrieg, o *guerra de control* al ser traducido del alamán,

---

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

[77] Op Cit SAMPAIO

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 de su enemigo con el fin de proporcionar un ataque que trascienda, en diversas representaciones, al plano físico del Estado objetivo[78].

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 hemos entendido 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"[79].

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 israelís expertos en cibernética informática, presuntamente vinculados al Gobierno, o bien profesando el nacionalismo propio de la sociedad sionista, construyeron una página web

---

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

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

programada para interferir u obstruir sitios en el ciberespacio que pertenecían a las organizaciones terroristas libanesas de Hizbolá y Hamás[80].

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 afectados por los ataques palestinos[81].

También se encuentra presente el caso de la Operación con nombre código "Titan Rain", en la cual, durante el año 2002 un grupo gubernamental de hacker chinos entrenados en el ciberespionaje, lograron descargar aproximadamente entre 10 y 20 terabytes de información sensitiva (pero no confidencial) del Departamento de Defensa de Estados Unidos a través del Non-secure Internet Protocol Router Network (NIPRNet), y específicamente del Army Information System Engineering Command, del Naval Ocean Systems Center, y de la Missile Defense Agensy[82].

Unos años más tarde, 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 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

---

[80] 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.
[81] Ibíd.
[82] Opcít. CARR.

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[83].

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 nueve 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 paginas web ministeriales se transformaron en sitios inservibles, y los ciudadanos no pudieron hacer compras on-line durante varios días, lo que perjudicó severamente la economía estonia que se dinamiza en gran medida a través del ciberespacio[84].

Posteriormente, de forma consecutiva, en el mes de julio de 2008 una firma georgiana de seguridad de la Internet registro 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 así como militares quedaran imposibilitados para comunicarse a través de la Internet[85].

Según las investigaciones de los analistas del ciberataque, paralelamente al advenimiento del segundo ataque, se desarrolló una movilización de tropas del

---

[83] 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

[84] Ibíd.

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

Ejército ruso hacia la región del sur de Georgia denominada como Osetia, un día después de 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[86].

Cabe resaltar, y como se establece en los documentos de investigación, 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 ves, 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 iranís, 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 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

---

[86] 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

a la ejecución del ataque programado con el que fue diseñado para afectar la infraestructura del Estado[87].

Posteriormente, al llegar el mes de junio del 2010, el estuxnet se activó, y con base en las características que describen este tipo de ciber-arma, 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. Después a este 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 reactor todavía no ha podido ser inaugurado por el gobierno de Ahmadinejad[88]..

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, deicidio emplear al ciberespacio y la ciberguerra para alcanzar un objetivo estratégico que de forma convencional hubiera sido bastante costos 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[89].

---

[87] Ibíd.

[88] 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.

[89] 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

Conclusiones

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 aun, gracias a las evidencias presentadas en el presente 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.

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, mas 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 planteo 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 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.

Ha sido evidente como el ciberespacio se ha transformado en una nueva dimensión, que si bien rompe con toda la lógica de los escenarios precedentes de desarrollo y evolución de la guerra, en la actualidad está siendo empleado activamente por los actores que protagonizan los complejos conflictos armados contemporáneos. Se constató como los Estados, grupos terroristas y activistas políticos (hackers políticos) emplean los computadores y la interconexión e

interdependencia de las redes informáticas, y de los gobiernos, infraestructura crítica y sociedad a estás.

Por lo tanto, no ha sido contradictorio observar a aquellos que se han convertido en blanco concreto de esta nueva clase de amenaza, diseñando y construyendo mecanismos apropiados para consolidar una salvaguarda de los niveles y esferas del Estado Nación en su conjunto. Gracias a esto, hoy en día los países que han logrado iniciar el camino en la salvaguarda del ciberespacio ven como prioridad integrar todos los actores que hacen parte de la Nación en la política y modelo de Ciberdefensa.

Por supuesto, este interés no se ha minimizado al ámbito domestico únicamente. Paralelamente a interpretarse al ciberespacio como un escenario en el cual el Estado debe propender en primera medida por su seguridad, no se puede perder de vista, que a diferencia de los espacios en los cuales el ser humano ha solido interactuar socialmente, ahora, las relaciones se gestan bajo una dinámica en la cual no existen las fronteras físicas ni temporales; evidenciando así que este nuevo dominio debe defenderse de mejor manera bajo modelos de defensa colectiva y trasnacional.

La disuasión, se ha convertido en un elemento principal al momento de pensar los modelos de Ciberdefensa. Si bien, en un principio se logró fundar la idea de que las características del *deterrance* propio de la Guerra Fría serían apropiadas para ser aplicadas a las capacidades de los computadores y el ciberespacio, la complejidad de los fenómenos y amenazas que han surgido a través de la virtualidad han demandado una mayor complejidad al momento de repensar la defensa estatal en el entorno cibernético.

En este nuevo escenario, las dinámicas de la guerra y la defensa se han transformado abismalmente hasta el punto tal que las lógicas a las cuales los gobiernos, fuerzas militares y organismos de seguridad estaban acostumbrados a

promover y sortear, distan en gran medida de los nuevos retos que impone el ciberespacio. Sin lugar a dudas, las variables que permiten este escenario tan voluble son diversas. La naturaleza de las tecnologías informáticas que otorgan capacidades sin parangón a los actores que las emplean, ya que logran desligar sus acciones de un territorio, una temporalidad, y en la mayoría de casos desligarse así mismos de ser reprendidos por el cato son algunas de éstas.

Si bien es cierto, que en la mayoría del tiempo el ciberespacio y las tecnologías informáticas se configuran como herramientas que interconectan al mundo y le permiten un mejor desarrollo a las sociedades, gobiernos, empresas y comercio (entre otros) en la medida en que la información se ha transformado en la materia prima de muchos de sus procesos, no se puede ocultar que paralelamente el ciberespacio también se ha configurado como un escenario para que la defensa, seguridad y soberanía estatal se ponga en detrimento: motivado en gran parte, en que el ataque es económico; ya no se necesita movilizar tropas ni maquinaria bélica, sólo se necesita un procesador con óptimas capacidades, una conexión a la red y un controlador con las habilidades suficientes para transformar los sistemas informáticos del enemigo.

La Ciberdefensa no puede seguir siendo un tema fuera de la agenda pública y los esfuerzos militares por preservar la defensa y seguridad del Estado. Aunque no es erróneo establecer que los países con mayor desarrollo tecnológico y científico, y por ende, mayormente dependientes del ciberespacio son los más vulnerables en este contexto, el considerable registro de acciones hostiles en la dimensión cibernética involucran a países de todo el globo; ya no hay razón que imposibilite llegar hasta a los niveles céntricos de un Estado a través de las autopistas informáticas.

Ahora bien, debe comprenderse de igual manera cómo bajo la construcción de la ciberdefensa, el concepto de *guerra total* cobra vida, si bien no destinado hacia la ofensiva en la guerra, sí para la defensa permanente de Estado. El resguardo de

la seguridad y soberanía de la Nación demanda que se integre al sector gubernamental, sector militar, organismos de seguridad, sector privado, ciudadanos y aliados externos. Por ende, la ciberdefensa no sólo es una acción ineludible, sino que perfectamente se adecua al tipo de respuestas que exigen las *nuevas amenazas* o *amenazas trasnacionales*, donde la defensa del Estado no es el único elemento que debe guiar el proceso, sino el desarrollo de un enfoque colectivo.

BIBLIOGRAFÍA

- AGENCIAS. "Musharraf ordena la detención de todos los miembros del grupo que degolló al periodista Daniel Pearl" .El mundo. [en línea], disponible en: http://www.elmundo.es/elmundo/2002/02/21/internacional/1014327615.html

- ANDRESS, Jason y WINTERFELD, Steve. Cyber Warfare: techniques, tactics and tools for security practitioners. ELSEVIER, Waltham-Massachusetts, 2011.

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

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

- BISHOP, Matt y O. GOLDMAN, EMILY. The Strategy and Tactics of Information Warfare. En: Contemporary Security Policy, 24. California, 2010.

- BOYD, Cristina. "Internet: el refugio de grupos terroristas" [en línea], disponible en: http://intelligenceservicechile.blogspot.com/2009/08/internet-el-refugio-de-grupos.html [consultado: 10 de febrero de 2010]

- BRENER, Susan W. Cyberthreats: the emerging fault lines of the Nation State. OXFORD University Press. New York, 2009.

- CARR, Jeffrey. Inside Cyber Warfare. O' Really Media. United Sstates, 2010.

- CARRILLO PAYÁ, Pedro. *Terrorismo y Ciberespacio*. [en línea], disponible en: http://www.assessorit.com/web/images/stories/prensa/pcarrillo-paper.pdf

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

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

- COHEN-ALMAGOR, Raphael. The Terrorists' Best Ally. Simon Fraser University. Canadian Journal of Communication, Volumen 25 No. 2. Vancouver-Canada, 2000.

- 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.

- COMMISSION OF THE EUROPEAN COMMUNITIES. Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience. Bruselas, 2009.
- CONWAY, Maura. Reality Bytes: Cyberterrorism and Terrorist 'Use' of the Internet. Department of Political Science of Trinity College. Dublin, 2002

- CORNISH, Paul. HUGHES, Rex. y LIVINGSTONE, David. Cyberspace and the National Security of the United Kingdom: Threats and Responses. Chatham House, marzo 2009. [en línea], disponible en: http:// www.chathamhouse.org.uk/publications/papers/view/-/id/726/

- 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.

- 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

- DOWNING, Emma. Cyber Security: a new national programme. Library of House of Commons. Londres, 2011.

- ECHAVARRÍA, Carlos. La innovación yihadista: propaganda, ciberterrorismo, armas y tácticas. Grupo de Estudios Estratégicos GEES. Análisis No. 7416, 2009

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

- 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

- FEDERAL MINISTRY OF THE INTERIOR. Cyber Security Strategy for Germany. Págs. 6-12 [en línea], http://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/OED_Verwaltung/Informationsgesellschaft/cyber_eng.pdf?__blob=publicationFile.

- FOJÓN, José Enrique. "Vigencia y limitaciones de la guerra de cuarta generación" Real Instituto Alcano de Estudios Internacionales y

Estratégicos. 2005. [en línea], Disponible en: http://www.realinstitutoelcano.org/analisis/916/916_Fojon.pdf. [consultado: 10 de febrero de 2010]. Págs. 2-4

- 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.

- GARDHAM, Duncan. MI6 attacks al-Qaeda in 'Operation Cupcake'. En: The Tlegraph, 2 de junio de 2011. [en línea], disponible en: http://www.telegraph.co.uk/news/uknews/terrorism-in-the-uk/8553366/MI6-attacks-al-Qaeda-in-Operation-Cupcake.html

- GEERS, Kenneth. The Challenge of Cyber Attack Deterrence. Naval Criminal Investigative Service (NCIS) y Cooperative Cyber Defence Centre of Excellence (CCD COE). Tallin-Estonia, 2009

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

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

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

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

- GUARÍN, Rafael. *Medios de Comunicación, Terrorismo y Antiterrorismo*. Perspectivas de Inteligencia. Colección Centro de Investigación en Guerra Asimétrica (CIGA). Número 3. Editorial, Escuela de Inteligencia y CI "BG Ricardo Charry Solano". Bogotá-Colombia. Octubre de 2009.

- 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

- HUGES, Rex B. NATO and Cyber Defence: Mission Accomplished?. En: Atlantisch Perspectief No. 8, Volume 32. Netherlands Atlantic Association, Bezuidenhoutseweg, 2008.

- 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.

- JOSHI, Akshay. The Scourge of Cyber-Terrorism. Strategic Analysis, 24: 4, 2000.
- K. ROSENFIELD, Daniel. Rethinking Cyber War. George Washington University, Elliott School of International Affairs, Washington, DC, 2010.

- 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.

- KESAN, Jay P. y HAYES, Carol M. Thinking Through Active Defense in Cyberspace. Workshop on Deterring CyberAttacks: Informing Strategies and Developing Options for U.S. Policy. Committee on Deterring

Cyberattacks: Informing Strategies and Developing Options; National Research Council.

- KRAMER, Franklin D. Cyberpower and National Security: policy recommendations for a strategic framework. En: Power and National Security. National Defense University Press y Potomac Books, Virginia, 2009.

- KUSHNER, Havey. Encyclopedia of Terrorism. Sage Publication. Londres, 2003.

- L. THOMAS, Thimoty. Al Qaeda and the Internet: the Danger of "Cyberplanning". Parameters No. 33, ProQuest Military Collection, 2003

- LIANG, Qiao y XIANGSUI, Wang. Unrestricted Warfare. PLA Literature and Arts Publishing House. Beijing, 1999.

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

- LORD, Kristian M. y SHARP, Travis. America 's cyber future : securit y and prosperit y in the information age. Center for a New American Security, junio de 2011. Págs. 7-9. Descarga disponible en: http:// http://www.cnas.org/node/6405

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

- LYNN, William J. Defendiendo un Nuevo Ámbito: la Ciberestrategia del Pentágono. En: Foreign Affairs Magazine, Septiembre/Octubre 2010

- MATUSITZ, Jonathan. Cyberterrorism: how can american foreign policy be strengthened in the information age?. American Foreign Policy Interests, 27: 2, 2005.

- MINISTRY OF DEFENCE. Cyber Security Strategy. Tallin-Estonia, 2008. [en línea], disponible en: http: http://www.mod.gov.ee/files/kmin/img/files/Kuberjulgeoleku_strateegia_2008-2013_ENG.pdf

- MOLANO ROJAS, Andrés. El nombre y la cosa: aportes al debate definicional sobre el terrorismo. Editorial, Escuela de Inteligencia y C/I "BG Ricardo Charry". Bogotá. 2009.

- MOLANO, Andrés. Terrorismo camaleónico: evolución, tendencias y desafíos inminentes del terrorismo global. Revista Fuerzas Armadas. VOL LXXXI. Edición 211. Septiembre, 2009.

- NAGPAL, Rohas. Cyber Terrorism in the Context of Globalization. II World Congress on Informatics and Law. Madrid-España, septiembre de 2002.

- ORTIZ, Román. "Amenazas transnacionales a la seguridad, tecnología e ingobernabilidad: el caso de Colombia" [en línea], disponible en: http://cooperacioninternacional.com/descargas/prueba.pdf [consultado: 9 de febrero de 2010]

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

- P. TRACHTMAN, Joel. Global Cyberterrorism, Jurisdiction, and International Organization. Conference on the Law and Economics of Cybersecurity. George Mason University School of Law. 2004

- PARLAMENTO EUROPEO. Directorado General de Política Exterior de la Unión. Política del Departamento de Política Exterior. "Cyber Security and Politically, Socially and Religiously Motivated Cyber Attacks" European Community, 2009. Pág.7 [en línea], disponible en: http://www.europarl.europa.eu/activities/committees/studies.do?language=EN

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

- PEREŠIN, Anita. Mass Media and Terrorism. Media Research: revista científica para el periodismo y los medios de comunicación de Croacia. Zagreb, 2007.
- POLLITT, Mark. Cyberterrorism - Fact Or Fancy?. FBI Laboratory and George Washington University. Computer Fraud & Security, Volume 1998, Number 2, 1998

- 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

- S. TIBBETTS, Patrick. Terrorist use of the internet and related information technologies. Fort Leavenworth, KS: US Army Command and General Staff College. 2002

- SÁNCHEZ MADERO, Gema. *Ciberguerra y ciberterrorismo ¿realidad o ficción? Una nueva forma de guerra asimétrica*. Dos décadas de Posguerra Fría. Actas de las I Jornadas de Estudios de Seguridad de la Comunidad de Estudios de Seguridad "General Gutiérrez Mellado", Tomo 1. [en línea],

disponible en: http://www.iugm.es/publicaciones/libros2008/ADEFAL/ADEFAL%20tomo%20I.pdf. Pág. 230

- SÁNCHEZ MADERO, Gema. Internet: una herramienta para las guerras en el siglo XXI. Military Review (edición hispanoamericana). Centro de Armas Combinadas. Fuerte Leavenworth, Kansas. Julio-agosto 2010.

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

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

- SOFAER, Abraham D., CLARK, David y DIFFIE, Whitfield. Cyber Security and International Agreements. Workshop on Deterring CyberAttacks: Informing Strategies and Developing Options for U.S. Policy. Committee on Deterring Cyberattacks: Informing Strategies and Developing Options; National Research Council.

- 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

- THE ECONOMIST. War in the fifth domain. En: The Economist, Volume 396 Number 8689, 2010. en línea], disponible en: http://www.economist.com/node/16478792

- TIRENIN, Walt y FAATZ, Don. A Concept for Strategic Cyber Defense. En: MILCOM: IEEE Military Communications Conference Proceedings. Atlantic City, 2009. Págs. 3-5

- TORRES, Manuel. "Terrorismo yihadista y nuevos usos de Internet: la distribución de propaganda (ARI)" [en línea], disponible en: http://www.realinstitutoelcano.org/wps/portal/rielcano/contenido?WCM_GLOBAL_CONTEXT=/elcano/elcano_es/zonas_es/terrorismo+internacional/ari110-2009, [consultado: 9 de febrero de 2010]

- TRIAS, Eric y BELL, Bryan. Ciber Esto, Ciber Aquello... ¿Y Qué? En: Air and Space Power Journal en Español, Volumen XXII, No. 3. Universidad del Aire. Alabama, 2010.

- UK OFFICE OF CYBER SECURITY y UK CYBER SECURITY OPERATIONS CENTRE. Cyber Security Strategy Of The United Kingdom: Safety, Security and Resilience in Cyber Space. Crown Copyright. Londres, 2009.
- USAF Commander, CHILTON, Kevin. Cyberspace Leadership: Towards New Culture, Conduct, and Capabilities. En: Air & Space Power Journal, Fall 2009.

- VÁZQUEZ LIÑÁN, Miguel. La propaganda de guerra en Internet. En: Historia y Comunicación Social, número 5, 2000.

- VERTON, Dan. La Amenaza invisible del ciberterrorismo. McGraw Hill. 2004

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

- WEIMANN, Gabriel. Cyberterrorism How Real Is the Threat? Especial Report. United States Institute of Peace (USIP). Washington D.C, 2004

- WHITE HOUSE. The National Strategy to Secure Cyberspace. 2003. [en línea], disponible en: http://www.us-cert.gov/reading_room/cyberspace_strategy.pdf

- WILSON, Clay. Computer Attack and Cyberterrorism: Vulnerabilities and Policy Issues for Congress. CRS Report for Congress. Congressional Research Service. The Library of Congress. Washington, 2005.

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

- WOLTHUSEN D., STEPHEN. Asymmetric Information Warfare: Cyberterrorism Critical Infrastructures. Security Technology Department. Fraunhofer-IGD. Darmstadt-Alemania, 2002