La ciberguerra y sus generaciones: un enfoque para comprender la incidencia de las tic en la guerra regular

ANDRÉS GAITÁN RODRÍGUEZ

Politólogo de la Pontificia Universidad Javeriana. Magister en Defesa y Seguridad Nacional de la Escuela Superior de Guerra. Jefe de la Línea de Investigación en Desarrollo Científico, Tecnológico e Innovación del Centro de Estudios Estratégicos en Seguridad y Defensa Nacional del CEESEDEN, de la Escuela Superior de Guerra.

Correo: garo@hotmail.com

Recibido:
20 de Mayo de 2012

Evaluado:
21 de mayo- 5 junio 2012

Aprobado:
8 de junio 2012

Tipología:
Artículo de reflexión resultado de investigación ya terminada.

El presente documento pretende presentar un enfoque para comprender el fenómeno de la ciberguerra. Se pone a consideración del lector la posibilidad de interpretar tres momentos característicos en los cuales los computadores, la Internet y el ciberespacio como una dimensión de interacción humana, se han prestado como medios para atacar a un enemigo o contendiente al interior de la categoría de los conflictos regulares. Se plantea este enfoque partiendo del principio de la cibernética como forma de control; acción que ha determinado tres elementos en la guerra: el control del factor psicológico, el control de la infraestructura crítica y finalmente, el control del armamento del enemigo.

Palabras clave:
computadores, Internet, ciberespacio, factor psicológico, infraestructura crítica estatal, armamento no tripulado.

Introducción

La Línea de Investigación en Desarrollo Científico, Tecnológico e Innovación del ESDEGUE-SIIA-CEESEDEN[1], desde su conformación se ha interesado por analizar cuál ha sido, y será en el futuro, la incidencia de la evolución industrial del *hombre* en la guerra. No se puede desconocer, que sumado a elementos como la estrategia, la moral, el entrenamiento, logística y doctrina, el factor tecnológico ha sido determinante en el desarrollo de los conflictos armados; incluso, si se elabora un barrido histórico se puede llegar a establecer la pauta de que todas las guerras han consistido en la tecnología (como lo expone Van Creveld en su obra *Technology and War: From 2000 B.C. to the Present*).

A razón de esto, se convirtió en un objetivo de alto valor para la Línea de Investigación expugnar uno de los fenómenos contemporáneos y relevantes para la disciplina de la seguridad y la defensa nacional: la transformación del ciberespacio como un campo de batalla. Con la inscripción "El Ciberespacio: un nuevo teatro de batalla para los conflictos

1 El ESDEGUE-SIIA-CEESEDEN hace referencia al Sistema Integrado de Investigación Académica (SIIA) de la Escuela Superior de Guerra (ESDEGUE), y el cual es administrado por el Centro de Estudios Estratégicos en Seguridad y Defensa Nacional (CEESEDEN).

armados del siglo XXI", la ESDEGUE estableció en 2011 un proceso de investigación en donde ya se ha logrado obtener un importante conocimiento acerca de las dinámicas que practican los Gobiernos, Fuerzas Militares, Agencias de Inteligencia, y del lado ilegal de esta atmósfera los actores terroristas, en función de las capacidades ofrecidas por las tecnologías informáticas.

Uno de los asuntos analizados bajo la égida de esta exploración, ha sido la ciberguerra. Este fenómeno, se ha caracterizado como el ejercicio de emplear los computadores, la Internet y la dimensión ciberespacial por parte de un Estado (mediante sus fuerzas de defensa y seguridad) con el objetivo de causar daños suntuarios sobre otro (Estado), mediante el desarrollo de ataques cibernéticos que van dirigidos hacia su infraestructura crítica. Desde el plano pragmático, la ciberguerra es una maniobra que la comunidad científica, académica y gubernamental ha establecido como propia del siglo XXI, en tanto que es en esta época en donde han acaecido sucesos representativos como; la Operación *Titan Rain* de China (2002), los ciberataques a Estonia (2007), Georgia (2008) e Irán (2010), entre otros casos semejantes.

Por otra parte, partiendo de los hallazgos señalados, se han podido establecer dos antecedentes fundamentales para trastocar el enfoque de análisis que se le ha otorgado a la ciberguerra. Primero, los computadores y la Internet fueron tecnologías introducidas a la guerra desde el esbozo de los años noventa del siglo XX. Y segundo, cuando se apela a la etimología del concepto ciberguerra ,y se denota su prefijo *ciber*, claramente se está haciendo alusión a la teoría y práctica de la cibernética (kybernetyké)[2]; la cual se fundamenta desde siglos atrás en las **técnicas de control** que puede emplear un ser humano para dominar los seres vivos y dispositivos de su entorno.

La armonización de estos preceptos ,y las últimas maniobras desarrolladas en este "nuevo" campo de batalla, permite en el presente caracterizar tres momentos o como se propone en este *paper*, tres generaciones para comprender la ciberguerra. La *primera generación*, establecida en los 90's a partir de la Guerra del Golfo Pérsico y en donde el elemento a controlar mediante estas tecnologías fue el **factor psicológico del enemigo**. La *segunda generación*, que hace referencia a la noción de operaciones para **controlar la infraestructura crítica del Estado contrario** como se indicó. Y finalmente, la *tercera generación*, sustentada en acontecimientos ocurridos en el presente año (2012), y en la cual, ya se ha revelado que **el armamento del enemigo también puede ser controlado**.

> Primera Generación de la ciberguerra: el control psicológico

La información nunca había cobrado más relevancia en el campo de batalla como lo hizo a partir de la década de los años noventa. Esto fue el producto de la introducción de los computadores y la transmisión de datos a través de Internet en la Guerra del Golfo Pérsico durante 1990 y 1991. La estructura militar comenzó a contar con una red comunicacional eficiente; los soldados en el campo de batalla fueron dotados de procesadores de datos portables para la recepción de información estratégica; aparecieron plataformas móviles cargadas con tecnologías informáticas (aviones J-STAR y AWACS) que sustentaron con radiografías del terreno en tiempo real el desarrollo de la operación y la táctica; e incidió en el armamento inteligente gracias a su integración con la informática (misiles Tomahawk).

Alan D. Campen, Director de la Política de Mando y Control en el Departamento de Defensa de Estados Unidos a principios de los noventa, ofrece su concepto de esta coyuntura histórica.

2 Se encuentra la raíz de cibernética en el griego antiguo, en la medida en que para dicha época este concepto ya denotaba el arte que poseían los timoneles de navíos para comandar y dirigir con éxito por las aguas sus embarcaciones. Fue un concepto que también fue trasladado por el ejército Nazi en la Segunda Guerra Mundial al campo de batalla, producto del control que maniobras como la *blitzkrieg* y las telecomunicaciones de la época otorgaron; de esto el nacimiento de la *leitenkrieg*. SAMPAIO, Fernando G. *Ciberguerra, Guerra Eletrônica e Informacional Um novo desafio estratégico*. Escola Superior de Geopolítica e Estratégia, Porto Alegre; 2001. [En línea]. Disponible en: httpwww.defesanet.com.bra.

"El conocimiento llegó a rivalizar en importancia con las armas y la táctica, presentando crédito a la idea de que es posible doblegar a un enemigo principalmente a través de la destrucción y el quebrantamiento de los medios de mando y control [...] virtualmente cualquier aspecto bélico se halla ahora automatizado y exige la capacidad de transmitir grandes cantidades de datos en formas muy diferentes"[3].

Las Tecnologías informáticas y por ende la información, cobraron su espacio en el campo de batalla. El Comandante T. J. Gibson (especialista informático militar) evidencia que al interior de la conflagración "los ordenadores determinan y analizan las formaciones y fuerzas del enemigo, se simulan las acciones posibles con programas que emplean la inteligencia artificial, y la información, logística y personal queda compilada y precisada"[4]. No en vano, como lo enuncian Alvin y Heidi Toffler, cuando culminó la campaña aliada en Kuwait, se registró que había en la zona de guerra un residuo de más de tres mil ordenadores (computadores) conectados con otros en Estados Unidos"[5]

No fue aleatorio el hecho de que en el ambiente militar del periodo naciera la doctrina de Guerra de la Información (*Information war*). Como marco de acción en tiempo de conflagración, este "nuevo" modelo de guerra conllevó a una actualización del entendimiento del concepto de *centro de gravedad*. Adicionalmente a concebir a los centros de poder del Estado como los objetivos para desarticular al enemigo; el factor sicológico del contendiente se convirtió en un elemento de victoria al que se podía acceder de manera más fácil bajo estas circunstancias.

Revisando la concepción de estrategia que el Departamento de Defensa de EE.UU. difundía sobre la tropa durante la Tormenta del Desierto, es posible precisar la inclusión de esta dimensión humana en el desarrollo de la guerra. Para entonces, estrategia significó "el arte y ciencia del desarrollo y empleo del poder político, económico, **psicológico** y militar tanto en tiempo de paz como de guerra, para asegurar el apoyo a las políticas que buscan incrementar las probabilidades y factores de victoria, así como reducir las opciones de derrota"[6]

En consecución, bajo el marco de la Guerra de la Información, el factor psicológico se desarrolló mediante las Operaciones de Información (o las OI). Estas tácticas se fundamentaron en el análisis de la tecnología, los procesos y los factores humanos que afectan la mente de quien toma las decisiones. Las OI se diseñaron para ser dirigidas contra líderes o tomadores de decisiones de alto nivel, pero también pueden afectar a cada escalón de la estructura militar, industrial e incluso de la población en general[7]. En concreto, las Operaciones de este tipo instauradas fueron: las *operaciones psicológicas*, *operaciones de engaño*, las *operaciones de seguridad*, las *operaciones de computadores en red* y las *operaciones electromagnéticas*.

Trayendo a acotación el principio de la cibernética, sobre el cual se sustenta el planteamiento del enfoque presentado en el documento, se puede establecer la primera premisa acerca del *control* a través de las tecnologías informáticas en el campo de batalla. Fueron las *operaciones psicológicas* y de *engaño* aquellas que permitieron a las fuerzas militares (de países desarrollados en los primeros años del fenómeno) obtener métodos para controlar el elemento característico de la primera generación de la ciberguerra.

Por una parte, las operaciones psicológicas se desarrollan sobre una estrategia de envío de in-

3 CAMPEN, Alan D. Citado en: TOFFLER, Alvin y TOFFLER, Heidi. *Las Guerras del futuro: la supervivencia en el alba del siglo XXI*. Plaza y Janes Editores, S.A. Barcelona, 1994. Pp. 104-105.

4 GIBSON, T.J. Citado en: Ibíd. p. 105.

5 Ibíd. p. 105.

6 DEPARTMENT OF DEFENSE. *Dictionary of Military and Associated Terms*. US Government Printing Office; Joint Publication 1-02; Washington DC. 1989.

7 BRADLEY K. Ashley. *Anatomy Of Cyberterrorism Is America Vulnerable*. Air War College. Air University, Maxwell Field; 2003, p. 4

formación seleccionada para influir las emociones, motivaciones, razonamientos objetivos, en última instancia, el comportamiento de gobiernos extranjeros, organizaciones, grupos e individuos. Y las operaciones de engaño, consisten en diseñar la información necesaria para guiar al enemigo a la toma de decisiones erróneas mediante la presentación de datos, imágenes y declaraciones falsas[8]. De manera aglutinante, para George Stein estas son operaciones enfocadas en influir las emociones, motivos, el razonamiento objetivo y finalmente el comportamiento de otros"[9].

Las operaciones psicológicas presentaron una alta correlación con la estrategia de la negación, contenida en la lógica del empleo del *poder*. Su objetivo se fundamentó en el principio de buscar la desarticulación parcial o total de los sistemas de comunicación del enemigo, o bien, lo que se denomina como la estructura de comando y control. Desde otro matiz, al impedir la comunicación se planeó la negación de la información; y como fin último, un efecto psicológico sobre el contrario.

Como lo ilustran los Toffler:

> "Al mismo tiempo que las fuerzas de coalición se afanaban por recoger, analizar y distribuir información, se ocupaban también activamente en destruir la capacidad de información y comunicación del enemigo. El último documento enviado por el Pentágono al Congreso sobre el desarrollo de la guerra del Golfo, el llamado Informe COW (de conducción de la contienda), señala que los primeros ataques se concentraron contra torres repetidoras de microondas, centrales telefónicas, salas de control, nódulos de fibra óptica y puentes portadores de cables coaxiales"[10]

Esta clase de guerra supuso éxitos operacionales para las Fuerzas de la Coalición de manera determinante. Stuart Slade, haciendo referencia a los sistemas informáticos iraquíes del momento argumenta: "Las sociedades que congelan el flujo de comunicaciones, el libre curso de ideas y datos, no serán por definición capaces de sacar un gran partido de estos medios [computadores y redes]... El sistema iraquí es un árbol. Tenemos a Saddam Hussein en la copa. Si rompemos en cualquier punto este tipo de sistema, puede ser catastrófico, sobre todo cuando el jefe de una división, aislado de la copa del árbol, sabe que el premio a su empleo de la iniciativa puede ser una -bala- 357 en la nuca"[11].

Ahora bien, las operaciones de engaño, como lo presenta George Stein se constituyeron con la misión de:

> Penetrar sistemas informáticos y ordenadores con el fin de enviar al adversario información engañosa, y que al ser disfrazada como elementos propios de la cadena de mando y control, lograban producir una acción en el campo de batalla que va en detrimento de la estrategia aplicada. No obstante, también es efecto de este tipo de operaciones, que el enemigo vea interrumpida su habilidad de orientar las operaciones eficientemente debido a la imposibilidad de generar un razonamiento objetivo. En consecuencia, se produce un condicionamiento en el proceso de toma de decisiones del enemigo al someterlo a responder a un universo virtual o ficticio de hechos, que a su vez se traduce en

8 WEILSON, Clai. Information Operations, Electronic Warfare, and Cyberwar Capabilities and Related Policy Issues. CRS Report for Cogress, Washington, 2007. P. 3

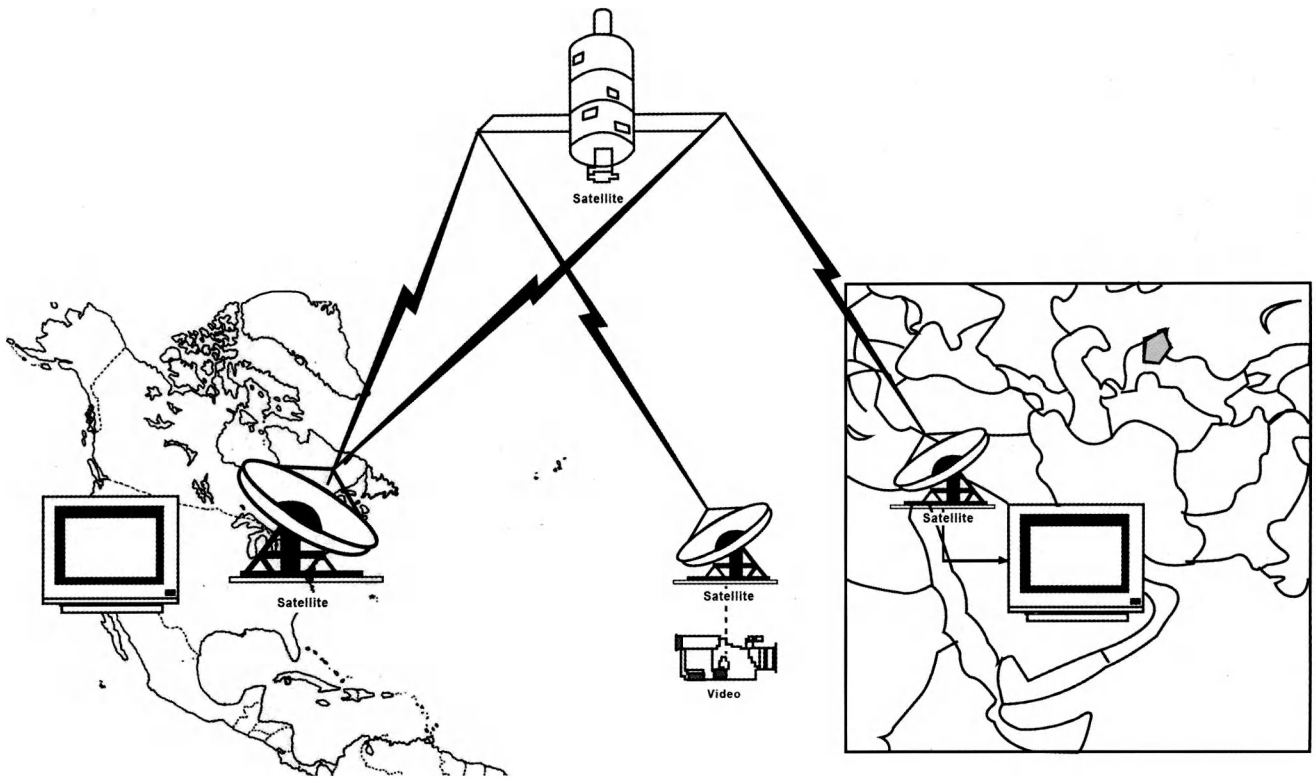
9 STEIN, George. *InformationWar-Cyberwar-Netwar*. En: SCHENEIDER, Barry y GRINTER, Lawrence (ed.). *Battelfield of the Future: 21st Century Warfare Issues*. University Press of the Pacific, Honolulu, 1998.p.157

10 TOFFLER. Op Cit. p.106

11 Ibíd. p. 208

> acciones caóticas, aleatorias, constantes e impredecibles; en síntesis, conductas que no son racionales en una balanza entre fines y medios[12]

Stein, paralelamente permite señalar que las operaciones psicológicas también se tradujeron en prácticas que llevaron a los contendientes a construir y difundir las denominadas "noticias virtuales". Partiendo del principio, de que las tecnologías informáticas se convirtieron en eficientes dispositivos que dieron paso a técnicas de combinar actores reales con gráficas e imágenes digitales, comenzó a ser posible el proceso de creación de noticias, conferencias, cumbres o incluso una batalla. "Ya no se trata de propaganda tradicional en donde el blanco es desacreditado mediante una fuente confiable de información. Más bien, la verdadera posibilidad de la "verdad" está siendo reemplazada por una "realidad virtual"; esto es, "información" que produce efectos independientemente de su realidad física. Lo que está siendo atacado en este nivel estratégico no es sólo las emociones, motivaciones o creencias del objetivo, esto constituye una amenaza muy posible de controlar un Estado"[13].



(Ejemplo de enlaces de comunicación de propaganda de Saddam Hussein. Extraído del documento "Beyond Security: A Data Quality Perspective on

Defensive Information Warfare" del Navy Command Control and Ocean Surveillance Center. [En línea]. Disponible en: http://web.mit.edu/tdqm/papers/other/kaomea.html)

12 STEIN. Op Cit. P.206.

13 Ibíd. p. 158

Segunda Generación de la ciberguerra: el control de la infraestructura crítica del Estado

Para comprender la segunda generación de la ciberguerra, es necesario partir de un principio fundamental e intrínseco en este proceso; la conformación del ciberespacio. Y por ende, cuál fue su diferencia con el escenario en donde se llevaron a cabo las primeras operaciones de control informático vistas precedentemente.

El control o cibernética aplicada al aspecto psicológico del enemigo, fue posible en tanto se extendió sobre el teatro de guerra una red de comunicaciones que integró a nivel estratégico, operacional y táctico las capacidades y esfuerzos militares (de las Fuerzas Aliadas en Kuwait en 1990), para poder desarrollar una nueva tipología de acciones sustentadas en el valor inmaterial de la información y las tecnologías que permiten su flujo exponencial. Pese a esto, para entonces no era posible aun hablar de ciberespacio, puesto que esta dimensión sólo surge en el momento en que las tecnologías citadas sufren una inserción categórica en los ámbitos del Estado Nación.

Estupiñan, analista de la globalización, ha establecido que entre los dispositivos informáticos y este proceso, se estableció un fenómeno de *"causa-efecto"* correlativo que[14], bajo esta explanación, compartida también por Manuel Castells, la globalización (como modelo) comenzó a ser exportada por el mundo con el fin de integrar a los Estados Nacionales a una comunidad global soportada en la Internet. Así, la propia globalización acarreó, gracias a su dinamismo, que las Naciones demandaran el usufructo de la informática para acomodarse a circunstancias en dónde la comunicación en tiempo real y sin límites geográficos fue el patrón establecido. En síntesis, la globalización disemina por el mundo las TIC, pero a su vez, son los computadores e Internet los que dan vida a este modelo económico; que posteriormente trasciende al ámbito político, cultural y social[15].

Como corolario, se originó una transformación en la cual los gobiernos (y sus diversos ministerios e instituciones), sistemas financieros, bancarios y bolsas de valores, empresas y compañías del sector privado, sistemas de control de tránsito (aéreo y terrestre), sistemas de funcionamiento (fuentes de energía, acueductos, gaseoductos, redes de comunicación, etc.), las Fuerzas y Sistemas de defensa y seguridad, y finalmente, la misma sociedad,[16] comenzaron a propugnar sus actividades, procedimientos y articulación en las capacidades de la informática y la *red mundial*[17].

Este proceso evolutivo (que continúa en la actualidad) ha sido determinante para la concatenación del ciberespacio, el cual se ha interpretado como una dimensión que permitió a las diversas sociedades del mundo poseer una nueva dimensión a la cual traspalar sus prácticas y desarrollo; así cómo se ha efectuado en la geografía terrestre, los océanos y mares, el cielo y el espacio.

Lo determinante de esta coyuntura fue la reciprocidad que se fundó entre la dimensión real o física de los Estados Nación y la dimensión virtual del ciberespacio. Según Gibson, las computadoras y su interconexión generaron una red artificial de terminales que dominaban exorbitantes canti-

14 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 [Citado el 5 de mayo de 2012]

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

16 A la conjunción de estos elementos se le denomina infraestructura crítica estatal. Los sistemas y los activos, ya sean físicos o virtuales, que son sumamente vitales para los Estados Unidos y que en caso de ser incapacitados o destruidos, los activos tendrían un impacto debilitante en la seguridad, la seguridad económica nacional, la salud o la seguridad pública, o cualquier combinación de dichos asuntos.

17 BHATTACHARJEE, Subimal. The Strategic Dimensions of Cyber Security in the Indian Context. Strategic Analysis, 33 2: 2009,pp. 196-201

dades de información que podían ser empleadas para diversos fines. Adicionalmente, y más importante aún, 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[18].

Desde el plano de la guerra, esta coyuntura se refleja en el hecho de que al generar un ataque propio de la ciberguerra de la segunda generación, un actor determinado puede crear información maliciosa (virus, *malware*, etc) que está destinada a viajar por el ciberespacio hasta alojarse en el sistema informático deseado y ejecutar la acción para la que fue diseñada.

Si bien es entonces el objetivo la infraestructura crítica estatal, el concepto de Gibson se traduce al proyectar escenarios en donde: reactores nucleares pueden ser saboteados para que funcionen erróneamente; que hidroeléctricas abran sus compuertas sin control produciendo inundaciones a su paso; que un controlador aéreo deje de ver en su monitor el mapa real de vuelo de los aviones a su cargo; que los sistemas bancarios queden inservibles y las personas queden sin la posibilidad de acceder a sus recursos y apagar redes eléctricas dejando a poblaciones sin el funcionamiento que esta fuente de energía sustenta, serían algunas de las formas de comprender este vinculo *interdimensional*.

Otra perspectiva de distinción, es el concepto de Centro de Gravedad (CG) desarrollado por Karl Von Clausewitz. Partiendo del principio, de que es el punto en donde confluyen las fuerzas de gravedad de un elemento determinado, el CG para un Estado, o visto desde la polemología, es aquel núcleo determinante para el correcto funcionamiento y subsistencia de una Nación, y que en caso de ser golpeado con la mayor energía puede producirse su invalidación como actor de un conflicto interestatal.

La naturaleza de esta práctica, también se encuentra sustentada en la teoría de los cinco anillos John Warden. Bajo esta doctrina, Warden evidencia que no sólo existe un único CG para el Estado Nación, sino que éste se compone de cinco instancias de soporte cuando se plantea un estado de guerra. A razón, emerge la concepción de que son, las Fuerzas (militares) desplegadas, la población, la infraestructura crítica, los sistemas esenciales y el liderazgo (gobierno), los pilares que declaran esta realidad.

La cada vez más creciente dependencia no solo de los países sino también de las personas, abre una ventana de riesgo para todas las actividades desarrolladas en la sociedad digital[19]. En consecuencia, entre mayor dependencia exista sobre la interconexión de estos procesos, mayor será la capacidad de las tecnologías informáticas para afectar la vida de los individuos, lo que hace del ciberespacio un escenario propicio para la ciberguerra en esta dimensión.

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 de alto valor estratégico[20]; esto es lo que habitualmente se ha conceptualizado como guerra, pero presentando la disconformidad de que el medio empleado no es el armamento convencional, sino un ataque informático que le permita a uno de los bandos obtener una ventaja sobre el

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

19 Por ejemplo, los Estados Unidos de Norteamérica al establecer sus operaciones en el contexto transnacional, ha entendido que se encuentra actuando en un medio ambiente globalizado, caracterizado por la interdependencia, la incertidumbre, la complejidad y los continuos cambios. Como se ha establecido en la Estrategia de Operaciones Militares en el Ciberespacio, la seguridad y el desarrollo de la Nación en el mundo interconectado dependen claramente de las Tecnologías Informáticas (TI) y la internet como elementos estratégicos para fortalecer y desarrollar los instrumentos del poder nacional. USAF Commander; CHILTON, Kevin. Cyberspace Leadership: Towards New Culture, Conduct, and Capabilities. En: Air & Space Power Journal, Fall 2009, p. 7.

20 Se entiende como información secreta y ultrasecreta que sea manejada por un Estado y que en un mediano o largo plazo, la utilización de esa información puede ser empleada para generar en el mundo real alguna clase de ataque programado. Es decir, el robo de un proyecto secreto de armamento militar aeroespacial que permita a una industria foránea replicar el modelo y posteriormente emplearlo sobre su iniciador original.

enemigo para situarse en superioridad o incluso derrocar el gobierno contrario[21].

Diversos casos han sustentado la existencia y desarrollo de la ciberguerra en su segunda generación. En primera instancia, se puede observar la Operación "Titan Rain". Esta iniciativa fue puesta en práctica por el Gobierno Chino y el Ejército Popular de Liberación a partir del año 2002, con el fin de *hackear* los sistemas informáticos gubernamentales y de industria nacional de países como Estados Unidos de Norteamérica y Alemania, entre otros. Esto, con el fin de extraer o desarrollar operaciones para controlar los centros de almacenamiento de información clasificada gubernamental, estratégica e industrial de los Estados afectados[22]. Estudios realizados al respecto (2007), evidenciaron que mediante esta Operación, China ya había logrado *hackear* (piratear) más de veinte terabytes (1.024.000.000'000.000 Gigabytes equivalen a 1 Terabyte) de información prioritaria[23].

Casos más críticos fueron los suscitados en países de los Balcanes. A partir de un altercado diplomático con el Gobierno ruso, Estonia en el mes de abril del año 2007 recibió (durante aproximadamente tres semanas) un ciberataque a su red nacional informática, en donde fueron deshabilitados los servicios bancarios y financieros paralizando así la economía del país, en tanto que los ciudadanos se vieron imposibilitados para desarrollar transacciones, compras y retiro de dinero a través de cualquier medio digital o virtual (incluso por cajeros automáticos); el sector gubernamental también fue seriamente golpeado. Paginas gubernamentales y redes de comunicación, principalmente del aparato Ejecutivo y el sector de defensa fueron saboteadas y revocadas, generando, tanto una incomunicación a nivel gubernamental, así como de la Administración con los ciudadanos y los servicios *on-line* existentes; cabe resaltar, que los índices mundiales de medición de integración estatal al ciberespacio, posicionan a Estonia como uno de los países que soporta más actividades en estas tecnologías[24].

El ataque perpetrado en Georgia un año después (2008) presentó similitudes destacables, a diferencia de que su duración fue menor. No obstante, los canales de comunicación gubernamentales fueron puestos a disposición del atacante con el fin de controlar los flujos de información que este manejaba con el exterior, así como también los sistemas de defensa del país. Es preciso connotar, que esta situación se enmarca en el desarrollo del conflicto fronterizo que ha mantenido Rusia con este país por la región de Osetia[25].

Los dos casos se vieron inmersos en coyunturas en donde Rusia presentaba claros intereses políticos y regionales tanto con Estonia así como con Georgia. No obstante, una vez la OTAN efectuó las investigaciones pertinentes para detectar a al agresor de estos hechos, los resultados dictaron que la información maliciosa sí había provenido de las redes informáticas del vecino país (Rusia), no obstante la fuente concreta de la acción no fue detectada; esto, gracias al empleo de herramientas propias de este ambiente, que permiten borrar la trazabilidad de los actos, que en este caso podría considerarse *de guerra*.

En el año 2010 (al igual que los trascurridos hasta el presente) la problemática del desarrollo del programa nuclear de Irán para los países

21 SÁNCHEZ MADERO, Gema. Internet: una herramienta para las guerras en el siglo XXI. En: Military Review, julio-agosto, 2010.

22 KREKEL, Bryan. Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation. The US-China Economic and Security Review Commission. Northrop Grumman Corporation, Virginia;2009.

23 IISS. China's cyber attacks. En Strategic Comments, 13 7; 2007. Págs. 1-3

24 BLANK, Stephen. Web War I Is Europe's First Information War a New Kind of War. Comparative Strategy, 27 3; 2008. Págs 227-247

25 KORNS, Stephen W. y KASTENBERG, Joshua E. Georgia's Cyber Left Hook. En Parameters, winter 2008-2009. Págs. 60-76

occidentales y principalmente para Israel se recrudeció. Esto propició el desarrollo del ciberataque denominado por la comunidad científica como Etuxnet, el cual ha sido el arma virtual más compleja desarrollada hasta el momento para atacar la infraestructura crítica del Estado. Este viajó por el ciberespacio hasta llegar a los sistemas informáticos que controlan el reactor nuclear de Bushehr, emplazamiento en dónde los servicios de inteligencia de otros Estados han denunciado se encuentra el centro de operaciones del Gobierno de Mahmoud Ahmadinejad para la posible construcción de armamento nuclear[26].

Al igual que los casos europeos, las investigaciones efectuadas plantean a Estados Unidos e Israel como los posibles ejecutores del Etuxnet, no obstante, los dictámenes no son fiables y concretos en la actualidad.

Una vez el virus llegó a controlar el sistema de operaciones de la instalación, asumió el control de este y lo llevó a operar bajo comandos erróneos y desestabilizadores que ultimaron un daño tal, que el reactor no pudo ser puesto en actividad ;meses después los ingenieros informáticos del país restituyeron la normalidad del sistema[27].

La ciberguerra en esta generación ya no es una cuestión del futuro para diversos países; aunque debe reconocerse que principalmente para aquellos actores con mayores capacidades tecnológicas informáticas. No es coincidencia por consiguiente, que los estadounidenses hayan revelado a la comunidad internacional la creación de su primer Cibercomando en el año 2010.

Army Cyber Command (Ejército), Fleet Cyber Command (Armada), 24th Air Force (Fuerza Aérea), Marines Corps Cyberspace Command (Marines).

(Extraído del sitio web del U.S. Army Cyber Command. [En línea]. Disponible en: http://www.arcyber.army.mil/org-arcyber.html)

> Tercera Generación: el control del armamento contrario

Esta generación de la ciberguerra parte claramente de los principios del ciberespacio expuestos precedentemente, no obstante, su connotación al interior de este ámbito posee una lógica diferencial.

Si se planteara la ciberguerra en su concepción más simple y natural, la tercera generación de esta nueva clase de conflagración es la que mejor simboliza el carácter de la cibernética. Ahora, la técnica trasciende de gobernar sistemas informáticos controladores de procesos fundamentales de un Estado Nación, al dominio directo de artefactos bélicos que hacen parte de las fuerzas militares u otras instancias del sector defensa y seguridad de las Naciones. Bajo la tipificación otorgada por el matemático y físico alemán Norbert Wiener, se

26 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 [Citado el 10 de mayo de 2012]

27 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 [10 de mayo de 2012]

podría esgrimir que ahora si se está haciendo alusión a la más pura ciencia del control y la comunicación de animales y máquinas[28].

El escenario propicio para esta generación de la ciberguerra comenzó a incubarse en al año 2004. Este fue un momento en el cual la guerra que libraba los EE.UU. en países como Afganistán y Pakistán para desarticular a Al Qaeda (como represalia al 11 de septiembre) llevó a los organismos de inteligencia, tanto militares como civiles, a dar un salto estratégico en materia tecnológica. Mediante la denominación de UAV (Unmanned Aerial Vehicle) se introdujeron al teatro de guerra,máquinas con la capacidad de ser dirigidas a través de controles remotos, y por ende , como su nombre los expresa, sin la necesidad de que exista un piloto en su interior[29]. Por supuesto, los sistemas de control y los canales de transmisión de las señales mediante los cuales se soporta el funcionamiento de estos vehículos aéreos se soporta en tecnología que se encuentra integrada a la red mundial de comunicaciones, la Internet y de esa atmósfera descrita como el ciberespacio.

EE.UU e Israel comenzaron a emplear los *drones* a partir del año 2010, con el fin de operar de manera secreta para la obtención de material de inteligencia acerca del programa nuclear del gobierno Ahmadinejad. No obstante, debe destacarse que algunos de los modelos empleados en estas operaciones poseen la capacidad de transportar material de ataque y bombardeo; como es el caso del Heron TP fabricado por la hata'asiya ha'avirit (Industria Aeroespacial Israelí)[30].

El hecho, de que en días pasados la Fuerza Aérea de la Guardia Revolucionaria de Irán haya logrado forzar al UAV estadounidense RQ-170 *sentinel* a aterrizar de forma asertiva en suelo nacional para su captura, es prueba fehaciente de esto.

Las fuerzas militares que detentan la posesión y empleo de esta clase de aeronaves ya no son los únicos actores con la capacidad de ejercer la cibernética en el teatro de operaciones. Ahora, el contrario se encuentra en la capacidad de hacerse al control del armamento hostil; lo que se corrobora en la realidad ,,y en el caso concreto, en que éste sea el cuarto *dron* que Irán le arrebata a EE.UU y ya posea tres del Ejército judío[31].

El Gobierno en Teherán, no ha negado hasta el momento la relación que se ha establecido con países como China[32] y Rusia[33] a partir de la captura de la aeronave no tripulada estadounidense. A pesar de que las fuerzas iraníes han alcanzado la tecnología para controlar los *drones* que operan en su espacio aéreo, no poseen la tecnología electrónica ni industrial para replicar, tanto el cascarón aerodinámico y furtivo, así como los componentes de inteligencia de la aeronave. Por lo cual y más por iniciativa rusa y china, los gobiernos ya han empezado a negociar los mecanismos de aplicación de ingeniería inversa, en tanto que el conocimiento adquirido y la duplicación de los dispositivos pueda ser compartida[34].

28 WIENER, Norbert. Cybernetics Or Control and Communication in the Animal and the Machine. MIT Press, Massachusetts; 1965.

29 GLYN WILLIAMS, Brian. The CIA's Covert Predator Drone War in Pakistan, 2004-2010: the history of an assassination campaing. Taylor and Francis Group, Brighton; 2010.

30 El País. Irán acusa a Israel de implicación en la guerra secreta de los 'drones'. [En línea]. Disponible en:http://internacional.elpais.com/internacional/2011/12/16/actualidad/1324058793_657762.html. (Consultada 15 de mayo de 2012).

31 Csmonitor. Did Iran Jijack the Beast US Experts Cautious about Bold Claims. [En línea]. Disponible en:http://www.csmonitor.com/USA/Military/2011/1216/Did-Iran-hijack-the-beast-US-experts-cautious-about-bold-claims.-Video. (Consultada 15 de mayo de 2012).

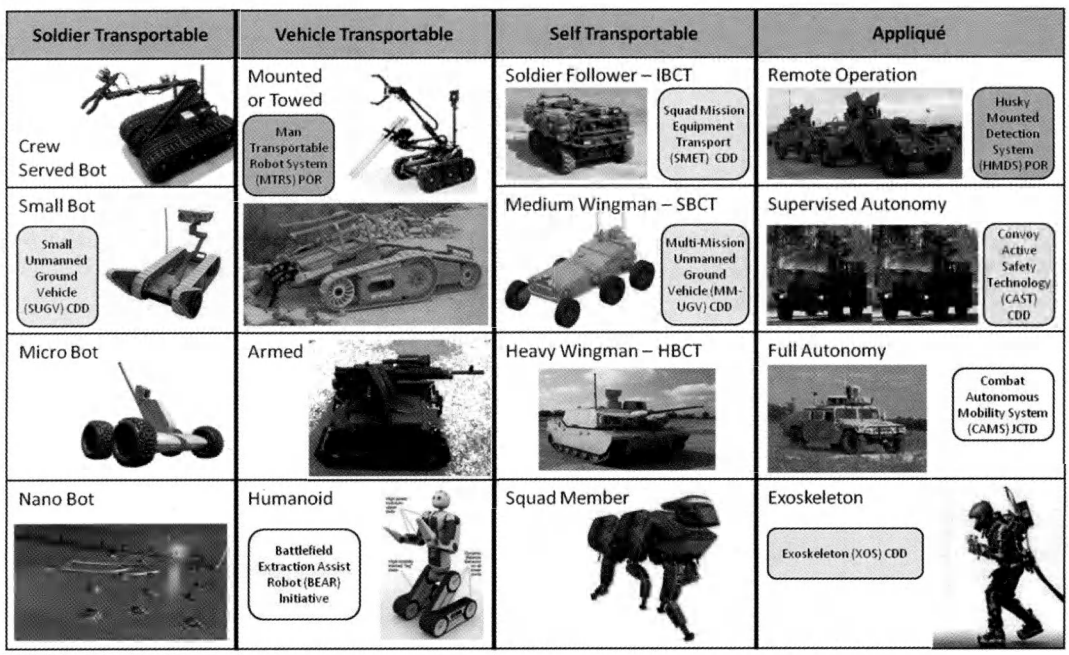
32 CBS. Iran Could Seek Chinas Help on U.S Drone [En línea]. Disponible en: http://www.cbsnews.com/8301-18563_162-57342628/iran-could-seek-chinas-help-on-u.s-drone/. (Consultada 15 de mayo de 2012).

33 ABC News. Covert War US Iran. [En línea]. Disponible en: http://abcnews.go.com/Blotter/covert-war-us-iran/story?id=15174919#.Tu1wddQoSHc. (Consultada 15 de mayo de 2012)

34 Payvand. U.S. worried China, Russia will gain access to RQ-170 drone. [En línea]. Disponible en: http://www.payvand.com/news/11/dec/1167.html. (Consultada el 15 de mayo de 2012).

Ahora, si bien es cierto que hasta el presente el único caso que se ha puesto en evidencia ha sido el de Irán, no se puede desestimar el crecimiento que está presentando la industria militar en el desarrollo de vehículos *sin hombres*. El terreno y los mares también se han visto provistos de nuevos dispositivos para actuar en sus condiciones naturales y cumplir con objetivos operacionales y tácticos determinados (no obstante las imágenes televisivas y de prensa han ilustrados el ya empleado método de desplegar *robots* en la desactivación de artefactos explosivos). Esto, si bien no ha conllevado a nuevos episodios de ciberguerra, si pone de manifiesto que un "enemigo" con la capacidad evidenciada por Irán para ejercer control sobre esta tecnología, cada vez más tendrá una probabilidad mayor de poder despojar a sus contrarios de su armamento; o bien, como no se debería descartar al momento de instaurar medidas de seguridad, de ponerlo incluso en su contra (al momento de emplear estas máquinas con potencial de ataque).

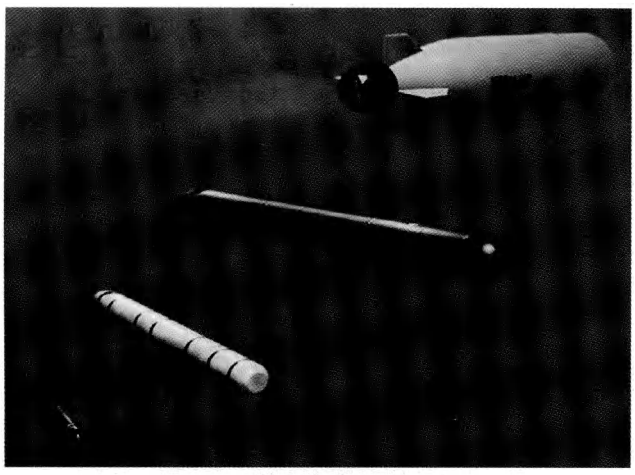
El documento desclasificado de la Robotic Systems Joint Project Office, bautizado como "Unmanned Ground Systems Roadmap" revela esta realidad para el ejercicio de la ciberguerra en su tercera generación. Allí se establece como el Ejército de los Estados Unidos ha proyectado hasta el año 2020 la inclusión en el campo de batalla de los Unmanned Ground Vehicle (UGV), los cuales, al igual que el armamento diseñado para el aire (UAV), están diseñados para cumplir con misiones de reconocimiento, así como operaciones que demandan el empleo de artillería. Cabe denotar, que incluso las categorías más avanzadas de los UGV se bosquejan para adoptar formas humanoides; estructuras que tal vez se encuentren mayormente capacitadas para emplear armamento convencional al igual que el soldado clásico[35].



(Imagen extraida del documento "Unmanned Ground Systems Roadmap 2011", de la Robotic Systems Joint Project Office.p-41. [En línea]. Disponible en: http://contracting.tacom.army.mil/FUTURE_BUYS/FY11/UGS%20Roadmap_Jul11.pdf)

35 ROBOTIC SYSTEMS JOINT PROJECT OFFICE. Unmanned Ground Systems Roadmap. Department of the Army (Doa); 2011.

Los océanos y mares no se quedan excluidos de un posible escenario de ataque en la tercera generación de la ciberguerra. Bajo la categoría de Unmanned Undersea Vehicle (UUV), las Armadas de países industrializados ya han proyectado escenarios estratégicos, en donde el empleo de artefactos sin tripulación cumplan los objetivos operacionales, tácticos e incluso como se aprecia en la imagen subsecuente, también efectúen misiones de apoyo logístico[36].



(Extraído del documento "The Navy Unmanned Undersea Vehicle (UUV) Master Plan 2004" del Department of the Navy. [En línea]. Disponible en: http://www.navy.mil/navydata/technology/uuvmp.pdf)

Conclusiones

En páginas precedentes se buscó formular un enfoque que permitiera comprender el fenómeno de la ciberguerra de una manera más sencilla. Si bien, como concepto la guerra cibernética comenzó a ser abordada a profundidad en ámbitos académicos, científicos y estatales en lo transcurrido ya del siglo XXI, cuando se parte del concepto connatural de la cibernética, y de que este tipo de conflagración se sustenta en los computadores, la Internet y el ciberespacio, se proyectan tres momentos cronológicos donde el *objeto* a ser controlado se ha transformado exponencialmente; y por ende la amenaza de recibir un ciberataque.

La ciberguerra que se inició en la década de los noventas del siglo XX, se estableció sobre la base del control de aspectos psicológicos. Es decir, como llevar al enemigo a frustrar su proceso de toma de decisiones y comunicación, y por ende, esto cómo podría impactar en la organización, moral, seguridad de un ejército. Pero también, no se puede dejar de lado el empleo de *falsa propaganda,* que buscaba influir de manera decisiva en la percepción que se tuviera del conflicto y la confianza sobre el gobierno o régimen contrario dentro de la población. De igual manera, el impacto estratégico, operacional y táctico que presentó el empleo de estas tecnologías en el campo de batalla por parte de Fuerzas como las de EE.UU en Kuwait, de igual manera generó un efecto moral devastador en los comandos de Hussein.

Esto coloca en evidencia, que el empleo de estas herramientas aun no se había concebido como el arma en si misma, como sí ocurrió en las generaciones ulteriores. Los computadores y la Internet fueron empleados para truncar los sistemas de comunicación de la estructura de comando, control, y comunicaciones (C3) del enemigo, para desestabilizar su accionar en el campo de batalla. Y de igual manera, para generar unas estrategias comunicacionales que confundiera tanto a las tropas como a la población del contendiente. Es decir, se dio un empleo de medios eficiente, de envío de información para dañar procesos basados analógicamente en información; lo cual, mediante un cálculo esperado, impactaría en instancias inherentes al ser humano.

36 The Unmanned Undersea Vehicle (UUV) Master Plan 2004. Deputy Assistant Secretary of the Navy and OPNAV N77 (Submarine Warfare Division). [En línea]. Disponible en: http://www.navy.mil/navydata/technology/uuvmp.pdf

Ahora bien, la ciberguerra en su segunda generación sí presentó la característica de emplear la información como una nueva tipificación de arma. Aunque el factor psicológico no se ha desvinculado en ningún sentido en este escenario, el objetivo en esta oportunidad son los sistemas informáticos que sustentan el funcionamiento, control y comunicaciones de la infraestructura crítica de un Estado. Mediante la consumación del ciberespacio, instancias gubernamentales, públicas, del sector defensa y seguridad, privadas, comerciales, financieras y sociales vieron la necesidad de integrarse a esta dimensión ,para poder ejecutar procesos bajo las demandas de tiempo y espacio de un mundo globalizado e interconectado. Esto, abrió la caja de pandora para aquellos con el conocimiento en informática requerido para crear información maliciosa en un computador.

Esta información, denominada comúnmente como virus, puede ser escrita para generar diversos propósitos en un objetivo seleccionado. Una vez ésta se envía a través del ciberespacio hasta el sistema informático que se seleccionó para ser atacado, efectos como el robo de información clasificada estatal, el control de los sistemas de un reactor nuclear o la red bancaria y financiera de un país, puede verse destruida causando daños adversos en su población; situación, que puede ser aprovechada como recurso estratégico dentro del marco de una *guerra preventiva* como se expresó en el caso de Bushehr en Irán, o bien como operación paralela a la movilización de tropas en el teatro de operaciones. En esta generación, queda de manifiesto que aquellos sectores de un Estado que convivan con tecnologías informáticas integradas al ciberespacio, sí no poseen las capacidades defensivas requeridas para evadir la información maliciosa que busca desestabilizar su funcionamiento, tienen una alta probabilidad de alterarse en origen de graves daños para una Nación.

Finalmente, aunque tan sólo se ha logrado registrar un episodio que certifique que las máquinas *no tripuladas* de un Estado pueden ser expuestas a operaciones de ciberguerra, no es causal de desmerecimiento de que es un escenario y por ende una tercera generación, tan real como sus precedentes.

Aunque desde la perspectiva de la amenaza, el caso de Irán y el UAV estadounidense *hackeado* y robado gira en torno a un dispositivo de inteligencia, el principio es el mismo para un dispositivo con capacidad de transportar armamento y la aviónica para ubicar blancos estratégicos y dirigir ataques inteligentes (como es la característica de diversos de estos modelos de aviones controlados). Por supuesto, sigue siendo una generación de la ciberguerra neonata, pero como se expresó en páginas precedentes, existen proyecciones estratégicas a nivel militar donde los elementos a desplegar en el campo de batalla cumplen con estas características y para los diversos terrenos de una conflagración; tierra, mar y aire.

Los Estados deben tener en cuenta en la actualidad, que cada instancia organizacional, funcional y de defensa y seguridad nacional que se integre a la dimensión comunicacional del ciberespacio puede estar en riesgo de ser vulnerada. Personal militar y civil que hoy en día poseen el conocimiento y experiencia para generar ataques cibernéticos, se encuentran capacitados para controlar dichos elementos y generar caos o efectos devastadores en una Nación. Si bien el control y la comunicación efectiva que trasciende fronteras espaciales y temporales es parte de las potencialidades del sistema globalizado y de los estándares en eficiencia y eficacia contemporáneos para el desarrollo de procesos, los gobiernos tienen que construir modelos y sistemas de ciberdefensa, que al igual que en la dimensión física, busquen proteger los centros de gravedad y la soberanía del Estado.

Comprender bajo un marco de *distinción el* fenómeno de la ciberguerra, permite avizorar y preparar a los Estados y sus sociedades de los posibles y distintos efectos que podría representar para una Nación este fenómeno.

Bibliografía

1 ABC News. Covert War US Iran. [En línea]. Disponible en: http://abcnews.go.com/Blotter/covert-war-us-iran/story?id=15174919#.Tu1wddQoSHc. (Consultada 15 de mayo de 2012).

2 BHATTACHARJEE, Subimal. The Strategic Dimensions of Cyber Security in the Indian Context. Strategic Analysis, 33 2; 2009,pp. 196-201

3 BLANK, Stephen. Web War I Is Europe's First Information War a New Kind of War. Comparative Strategy, 27 3; 2008. Págs 227-247

4 BRADLEY K. Ashley. Anatomy Of Cyberterrorism Is America Vulnerable. Air War College. Air University, Maxwell Field; 2003, p. 4

5 CAMPEN, Alan D. Citado en: TOFFLER, Alvin y TOFFLER, Heidi. Las Guerras del futuro: la supervivencia en el alba del siglo XXI. Plaza y Janes Editores, S.A. Barcelona, 1994. Pp. 104-105.

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

7 CBS. Iran Could Seek Chinas Help on U.S Drone [En línea]. Disponible en: http://www.cbsnews.com/8301-18563_162-57342628/iran-could-seek-chinas-help-on-u.s-drone/. (Consultada 15 de mayo de 2012).

8 CHILTON, Kevin. Cyberspace Leadership: Towards New Culture, Conduct, and Capabilities. En: Air & Space Power Journal, Fall 2009, p. 7.

9 Csmonitor. Did Iran Jijack the Beast US Experts Cautious about Bold Claims. [En línea]. Disponible en: http://www.csmonitor.com/USA/Military/2011/1216/Did-Iran-hijack-the-beast-US-experts-cautious-about-bold-claims.-Video. (Consultada 15 de mayo de 2012).

10 DEPARTMENT OF DEFENSE. Dictionary of Military and Associated Terms. US Government Printing Office; Joint Publication 1-02; Washington DC. 1989.

11 El País. Irán acusa a Israel de implicación en la guerra secreta de los 'drones'. [En línea]. Disponible en: http://internacional.elpais.com/internacional/2011/12/16/actualidad/1324058793_657762.html. (Consultada 15 de mayo de 2012).

12 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 [Citado el 5 de mayo de 2012]

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

14 GLYN WILLIAMS, Brian. The CIA's Covert Predator Drone War in Pakistan, 2004-2010: the history of an assassination campaing. Taylor and Francis Group, Brighton; 2010.

15 IISS. China's cyber attacks. En Strategic Comments, 13 7; 2007. Págs. 1-3

16 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 [Citado el 10 de mayo de 2012]

17 KORNS, Stephen W. y KASTENBERG, Joshua E. Georgia's Cyber Left Hook. En Parameters, winter 2008-2009. Págs. 60-76

18 KREKEL, Bryan. Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation. The US-China Economic and Security Review Commission. Northrop Grumman Corporation, Virginia;2009.

19 Payvand. U.S. worried China, Russia will gain access to RQ-170 drone. [En línea]. Disponible en: http://www.payvand.com/news/11/dec/1167.html. (Consultada el 15 de mayo de 2012).

20 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 [10 de mayo de 2012]

21 ROBOTIC SYSTEMS JOINT PROJECT OFFICE. Unmanned Ground Systems Roadmap. Department of the Army (Doa); 2011.

22 SAMPAIO, Fernando G. Ciberguerra, Guerra Eletrônica e Informacional Um novo desafio estratégico. Escola Superior de Geopolítica e Estratégia, Porto Alegre; 2001. [En línea]. Disponible en: httpwww.defesanet.com.bra.

23 SÁNCHEZ MADERO, Gema. Internet: una herramienta para las guerras en el siglo XXI. En: Military Review, julio-agosto, 2010.

24 STEIN, George. InformationWar-Cyberwar-Netwar. En: SCHENEIDER, Barry y GRINTER, Lawrence (ed.). Battelfield of the Future: 21st Century Warfare Issues. University Press of the Pacific, Honolulu, 1998.p.157

25 The Unmanned Undersea Vehicle (UUV) Master Plan 2004. Deputy Assistant Secretary of the Navy and OPNAV N77 (Submarine Warfare Division). [En línea]. Disponible en: http://www.navy.mil/navydata/technology/uuvmp.pdf

26 WEILSON, Clai. Information Operations, Electronic Warfare, and Cyberwar Capabilities and Related Policy Issues. CRS Report for Cogress, Washington, 2007. P. 3

27 WIENER, Norbert. Cybernetics Or Control and Communication in the Animal and the Machine. MIT Press, Massachusetts; 1965.