Cómo citar este artículo:
Arreola García, A. (2016). Ciberespacio, el campo de batalla de la era tecnológica. *Estudios en Seguridad y Defensa, 11*(22),

Ciberespacio, el campo de batalla de la era tecnológica[1]

Cyberspace, the Battlefield of the Technological Age

Ciberespaço, o campo de batalha da era tecnológica

ADOLFO ARREOLA GARCIÍA[2]

Recibido:
25 de abril de 2016

Aprobado:
31 de octubre de 2016

Resumen

El progreso de los medios cibernéticos y su aplicación como medio de defensa – ataque por parte de diversos actores de la sociedad internacional, así como la utilización del campo de batalla virtual (ciberespacio) por parte de los Estados y sus fuerzas armadas para garantizar la seguridad nacional, ofrecen la oportunidad de examinar el poder de la tecnología digital y el espectro electromagnético como medios de ataque y destrucción de los potenciales enemigos así como medio de defensa de la información estratégica crítica. De igual forma, esta fórmula entre tecnologías de la información y poder, presenta una nueva condición de conflicto internacional que debe ser regulado, a fin de: evitar las atrocidades del pasado observadas en conflictos interestatales, garantizar el respeto de los no combatientes y definir claramente cuando se debe utilizar la fuerza militar para responder a un ataque cibernético. Por ello, el ciberespacio se ha convertido en un ámbito de la guerra en donde las vulnerabilidades del enemigo son explotadas sin necesidad de la fuerza; en consecuencia

Palabras claves:
Ciberespacio, ciberguerra, ciberestrategia, ciberamenaza, ciberespionaje

Keywords:
Cyberspace, cyberwar, cyber strategy, cyber threat, cyber espionage

Palavras Chaves:
Ciberespaço, a guerra cibernética, e-estratégia, ameaça cibernética, cyber-espionagem

1. Artículo de reflexión de investigación en proceso. El presente documento forma parte de la investigación, "Ciberseguridad, la nueva cara de la seguridad internacional en el siglo XXI" la cual es parte de la línea de investigación en Globalización y Persona Humana: aportaciones para la Seguridad Integral y el Desarrollo Sustentable de México de la Universidad Anáhuac Norte, México.

2. Doctorando en Seguridad Internacional de la Universidad Anáhuac Norte, México. Magíster en Estudios México-EEUU de la Universidad Nacional Autónoma de México, México. Licenciado en Relaciones Internacionales de la Universidad Nacional Autónoma de México, México. Investigador de la Universidad Anáhuac Norte, México. Representante legal de la compañía Merex Inc. Representante comercial de la revista Airtrade. Contacto: adolfoarreola@yahoo.com.mx.

los Estados deben contar con una estrategia que dé respuesta oportuna y precisa a las amenazas que se enfrentan.

Abstract

The progress of the cyber means and their application as a defense-offense means by different actors of the international society as well as the use of the virtual battle field (cyberspace) by States and their armed forces to guarantee the national security, offer an opportunity to examine the power that the digital technology and the electromagnetic spectrum have as means to attack and destroy potential enemies, as well as the a the way to defend the critical strategic information. At the same time, this formula made of information technologies and power, presents a new international conflict condition that should be regulated, with the objective of: avoiding the atrocities of the past observed in the interstate conflicts, guaranteeing the respect of the non-combatants and, clearly, defining when the military force must be used to respond to a cyberattack. So, the cyberspace has become one of the war domains on which the enemy´s vulnerabilities are exploded without the need of force; consequently the States should have a strategy to answer, promptly and precisely, to the threats they face.

Resumo

O progresso dos meios cibernéticos e sua aplicação como meio de defesa - ataque por parte de vários atores da sociedade internacional, assim como o uso do campo de batalha virtual (Cyberspace) pelos Estados e suas forças armadas para garantir a segurança nacional, proporcionar a oportunidade de examinar o poder da tecnologia digital e do espectro eletromagnético como um meio de ataque e destruição dos inimigos potenciais, bem como a defesa da informação estratégica crítica. Da mesma forma, esta fórmula entre tecnologia de informação e poder, apresenta um novo status como conflito internacional que deve ser regulado, a fim de: evitar as atrocidades do passado vistas em conflitos interestaduais, assegurar o respeito dos não combatentes e definir claramente quando devesse usar a força militar para responder a um ataque cibernético. Portanto, o ciberespaço tornou-se um campo de guerra, onde as vulnerabilidades do inimigo são exploradas sem necessidade da força; em conseqüência os Estados devem ter uma estratégia que dê resposta oportuna e precisa às ameaças que enfrentam.

Introducción

El poder obtenido a través del manejo de la información y el conocimiento, ha dado pie a una serie de programas gubernamentales para manipular la mente de

los hombres y controlar sus acciones. Esto coincide con la forma en que Morgenthau (1992, p. 43) define el poder-control[3], pero también con lo que literatos mexicanos argumentan sobre el poder político que ostentan las naciones más fuertes sobre las débiles desde una perspectiva novelesca y como una consecuencia del control de la información estratégica de los sometidos.

Tal es el caso de Leopoldo Mendivil López quien en sus obras "Secreto 1910" "Secreto 1929" y "Secreto R Conspiración 2014" hace una narrativa de las ventajas obtenidas, tanto por gobiernos extranjeros como por grandes corporaciones internacionales en el mercado Mexicano e internacional, gracias al conocimiento anticipado de: las intenciones, debilidades y secretos de los gobernantes en turno, la situación de las finanzas y negocios internacionales, y los temores-aspiraciones de la sociedad en general. La trilogía es una muestra del juego excitante de la diplomacia como el medio perfecto para influenciar y obtener los secretos mejor guardados por los gobiernos a través de las relaciones internacionales que fungen como instrumentos de conocimiento y vigilancia. A lo cual hay que sumar, la cooptación de las elites y líderes políticos; la generación de conflictos; la explotación de las aspiraciones de la población; la esperanza de una vida mejor; y el uso de la información estratégica como parte de la estructura para ejercer el poder.

Lo presentado por Leopoldo (2014) es consecuencia, entre otras cosas, del deseo de reconstruir realidades dentro de un marco de ilusión, que no ofenda a nadie pero exponga todo; ya que lo que aparece en sus escritos pudiera ser bien considerado como un caso más de las Teorías de la Conspiración.

Por ejemplo, Leopoldo (2014, p. 15) describe una red secreta de control de las políticas y acciones del mundo, a la cual define como la "Intraestructura" un esquema compuesto de nueve subestructuras entre las que se encuentran conocidos organismos del sistema de inteligencia estadunidense como son la Agencia Central de Inteligencia (CIA); la Agencia de Proyectos de Investigación Avanzada de la Defensa (DARPA) y la RAND Corporation, un instituto de investigación dependiente del Pentágono. Lo cual permite reflexionar sobre los hechos, y afirmar que la información es poder.

La narrativa de Mendivil a lo largo de sus tres obras, hace mención del uso inadecuado e incluso personal de los medios de inteligencia institucionales, lo que expone esa dualidad del sistema de inteligencia como medio de información-vigilancia. Esa transformación de las misiones de los sistemas de inteligencia, fue expuesta por Harry Truman[4] (1963), el creador de la National Security Agency

3. Hans Morgenthau define el concepto de poder como el control del hombre sobre las mentes y las acciones de otros hombres. Dicha interpretación puede ser llevada al ámbito internacional y ser reinterpretada como sigue: poder es el control que tiene un Estado sobre las políticas y acciones de otro(s) Estado(s). Concepto en donde además está presente la simbiosis entre los conceptos de control y poder; o poder y control; que para el desarrollo del artículo son de suma importancia.

4. Harry S. Truman fue presidente de los EE.UU. de 1945 hasta 1953 y tuvo que lidiar con la reorganización de los servicios de

(NSA) y la Agencia Central de Inteligencia (CIA), en un artículo publicado el 22 de diciembre de 1963, afirmando: "*For some time I have been disturbed by the way CIA has been diverted from its original assignment. It has become an operational and at times a policy-making arm of the Government. This has led to trouble and may have compounded our difficulties in several explosive areas*". ["Por algún tiempo me he visto perturbado por la forma en que la CIA se ha desviado de su asignación original. Se ha convertido en un arma operativa y en algunas ocasiones generadora de políticas del Gobierno. Esto ha llevado a un problema y ha agravado nuestras dificultades en diversas áreas explosivas"].[5]

Truman (1963) posteriormente concluye remarcado que la libertad de sus instituciones y la capacidad para mantener una sociedad abierta y libre es lo que ha dado prestigio a su nación, cerrando con: "*There is something about the way the CIA has been functioning that is casting a shadow over our historic position and I feel that we need to correct it.*" ["Hay algo raro en la forma en que la CIA ha estado funcionando, lo cual ha determinado el ensombrecimiento de nuestra postura histórica, considero que eso es algo que debemos corregir".][6]

Lo anterior es evidencia de dos cosas: la necesidad que tienen los líderes nacionales de contar con información imparcial sobre los asuntos vitales para el desarrollo del país y, la desviación de las funciones de los sistemas de información, para lograr acciones sombrías con base en el conocimiento anticipado. Todo lo anterior, Truman (1963), lo hace manteniendo la reserva sobre la *National Security Agency* (NSA), otra de sus obras en la reingeniería del sistema de inteligencia/espionaje de los EE.UU. El trabajo de Leopoldo se ve complementado por la narrativa de escritores como Manuel Buendía en su obra "La CIA en México" (1984) quién a la usanza de los grandes espías, describe el imperio oscuro del control de la información y las redes de la CIA en México con sumo detalle.

La trasformación jurídica y el derecho de guerra es algo inevitable y, en el presente – debido al empleo cada vez más intensivo de la tecnología como arma de guerra – las instituciones internacionales, los Organismos No gubernamentales, las grandes corporaciones y la sociedad civil en su conjunto levantan la voz para establecer un marco jurídico eficaz para regular los actos de ciberguerra. Principalmente porque los actos ofensivos emprendidos por los Estados, pueden ser enmascarados como actos criminales cometidos por grupos delictivos y por ello no requieren de una respuesta militar.

inteligencia, por ello creó la CIA en 1947 con el objetivo primario de obtener información del estado del mundo por medio de la recopilación de información sobre Gobiernos extranjeros, corporaciones e individuos; analizar esa información comparándolos con las de otras agencias; para finalmente brindar una evaluación sobre inteligencia para la seguridad nacional; y la NSA en creada en secreto el 4 de noviembre de 1952 y encargada con todo lo relacionado con la seguridad de la información.

5. Traducción propia.

6. Traducción propia.

La dificultad para identificar la fuente de los ciberataques está íntimamente ligada a la cantidad de aditamentos, usuarios y accesorios que se utilizan o conectan a la red; lo cual ha sido y seguirá siendo consecuencia del avance tecnológico. Es precisamente el incremento de las actividades no solo gubernamentales sino cotidianas lo que da pie a una dependencia de la vida en el ciberespacio; que al convertirse en el centro de la actividad es sujeto de agresiones que ponen en jaque los sistemas estratégicos de una nación.

En este tenor de ideas, Castells (2005) a finales del siglo XX hace ya mención de la existencia de un poder informático[7] que se obtiene por el dominio de la infraestructura de comunicaciones digitales y las computadoras. Es ahí donde se puede ver el nacimiento de una nueva forma de controlar a las masas a través del dominio del entorno virtual en el cual se desarrolla la vida cotidiana del presente siglo y, ¿por qué no? las batallas.

Hasta antes de la aparición de las computadoras y el internet, los ámbitos de la guerra se dividían en cuatro: terrestre, marítimo, aéreo y espacial. Sin embargo, de la misma forma como la artillería se liga con el desarrollo de la guerra terrestre; la construcción de grandes navíos al poder marítimo; el uso de aeronaves como catalizador del poderío aéreo y el uso de los satélites llevó a la llamada "Guerra de las Galaxias" con las tecnologías de la información apareció el fenómeno de la ciberguerra. Esta situación permite considerar ahora un quinto dominio de la guerra, el ciberespacio.

Partiendo de la existencia de un poder virtual que predomina en un nuevo ámbito de la guerra, se analizan los elementos distintivos que lo definen. Esto lleva a una revisión de las causas de las guerras, que si bien son cosmovisiones que se aplican al mundo material, pueden ser adoptadas para interpretar lo que ocurre u ocurrirá en el ciberespacio.

El estudio se enfocará esencialmente en los siguientes aspectos: por qué el ciberespacio debe ser considerado como el nuevo ámbito de la guerra; por qué las tecnologías de la información deben ser consideradas como un arma militar que brinda mayores ventajas a la ofensiva; cuáles son las principales amenazas que enfrentan los Estados en el ciberespacio; y por qué es preciso hablar de ciberguerra.

Partiendo de lo anterior, el presente estudio se estructura en tres temas centrales. El primero, examinará las condiciones que hacen del ciberespacio el nuevo ámbito de guerra; donde, a pesar de su invisibilidad, se pueden realizar ataques contra los Estados, su infraestructura y su población. En segundo término, se analizará el por

7. Castells, M. (2005). *La era de la información: economía, sociedad y cultura en la sociedad red*. (vol.1). Madrid, España: Alianza Editorial. Algunas veces le llama el poder cibernético.

qué las computadoras y sus accesorios son potencialmente tanto armas de guerra como los blancos de los ataques cibernéticos. Para posteriormente pasar a la descripción de las principales amenazas a la seguridad de los Estados y las razones que motivan a los diversos actores a realizar ciberataques que pueden escalar hasta la ciberguerra.

Metodología de la investigación

El presente trabajo de investigación se basa en el análisis literario, de discurso e histórico de diversos documentos oficiales, académicos, gubernamentales, tecnológicos y mediáticos que permiten abordar el tema en cuestión desde perspectivas teóricas y mediático-realistas, es decir desde los acontecimientos que ocurren en nuestro mundo en el día a día. Lo anterior teniendo por objetivo la correlación de los acontecimientos cotidianos con la explicación teórica de los mismos; ya que la historia, al ser una fuente esencial de información, presenta una serie de indicadores y eventos recurrentes que permiten anticiparse a los hechos aplicando los preceptos teóricos. Es en esta visión que la estrategia se basa y desarrolla, y recomienda estudiar la guerra para preservar la paz o estudiar la paz para evitar la guerra.

El objetivo del presente documento es explicar la importancia de la ciberseguridad[8] como medio de defensa, respuesta y ataque dentro del contexto de la ciberguerra. Es claro que al no existir un consenso sobre la ciberguerra, el desarrollo de la presente obra, ofrecerá al lector elementos con los cuales podrá construir un concepto personal sobre el tema y una justificación para las respuestas de las fuerzas armadas a los ataques contra la red que ponen en riesgo la ciberseguridad.

Los objetivos específicos de la presente investigación son: primero, determinar los rasgos característicos del ciberespacio, que hacen de este el nuevo ámbito de la guerra, en donde con mayor frecuencia se realizan ataques contra la red de computadoras que controlan actividades vitales para la defensa y seguridad nacional de los Estados; segundo, descubrir como las tecnologías de la información, particularmente las digitales, se han convertido en el arsenal digital de los Estados, que pudiera ser empleado en los conflictos interestatales del siglo XXI; y tercero, establecer las características de los conflictos actuales que dan vida al concepto de ciberguerra.

Características bélicas del Ciberespacio

La antigua ciencia militar conceptúa al campo de batalla como el espacio geográfico donde se desarrollan las batallas, por lo tanto era de suma importancia elegirlo y utilizarlo sabiamente. Esto fue practicado en cada conflicto durante los

8. Sería aún más preciso hablar de una ciberseguridad nacional, ya que esta intenta resguardar todos los activos y pasivos que son vitales para la supervivencia del Estado desde la perspectiva del mundo virtual, pero con impacto en la vida material.

siglos XVII, XVIII y XIX en donde la guerra de posiciones fue considerada como el medio para alcanzar la victoria. Sin embargo, los avances tecnológicos han traído nuevos escenarios en los que las batallas se combaten; por ello, para realizar una aproximación a los "nuevos campos de batalla" es adecuado definir como se entiende el campo de batalla, cómo pueden clasificarse y cuáles son sus características esenciales.

De acuerdo con el "Diccionario Enciclopédico de la Guerra" (1958) el campo de batalla se define como: "[…] el terreno en que combaten dos ejércitos, o tiene lugar una batalla"; lo que se ha prestado a debate porque existen dos vocablos que aluden al enfrentamiento de los combatientes (combate y batalla), pero que deben ser diferenciados. En un intento por aclarar la situación se emplean las definiciones ofrecidas por el Diccionario de la Real Academia de la Lengua Española (2014) para cada palabra, en donde se definen como sigue: primero, combate "Acción bélica o pelea en que intervienen fuerzas militares de alguna importancia."; segundo, batalla es "Serie de combates de un ejército con otro, o de una armada naval con otra".

Definiciones que establecen que el combate tiene un carácter táctico y la batalla muestra un alcance estratégico, pero que no incorporan a los dominios aéreo, espacial ni virtual. Lo anterior invita a proponer la siguiente definición para batalla: "serie de combates en que intervienen dos oponentes en un ámbito físico o virtual." En donde los enfrentamientos pueden darse en un espacio material o virtual, según las particularidades y propósitos del combate, y con ello ampliar el alcance del concepto a las nuevas realidades.

A lo anterior se debe agregar el entorno en que se desarrollan los combates. Si bien por el desarrollo tecnológico alcanzado hasta mediados del siglo XX, el campo donde se realizaban las batallas era entendido únicamente como el espacio geográfico / material dentro o fuera de la atmósfera terrestre, ahora se habla de un ciberespacio que no se toca pero sí se siente.

En consecuencia, el cibercampo de batalla puede interpretarse como el espacio virtual en que se llevan a cabo uno o varios combates entre dos oponentes.

A pesar de que gran cantidad de conceptos pueden parecer muy avanzados, son tan antiguos como la historia militar, y han sido adaptados a las circunstancias del momento histórico. Esto sirve como justificación para hablar de la clasificación del terreno[9] establecida por Sun Tzu y su potencial adaptación al mundo del presente. De acuerdo con la tipología propuesta por Sun Tzu (2008: p. 109) los tipos de terrenos se clasifican en:

9. Terreno es como tradicionalmente se conoce al área en la cual potencialmente se puede llevar a cabo la batalla y consideras todo los espacios geográficos.

Tabla 1: Tipología del terreno

Tipo	Características	Observaciones
Accesible	De fácil acceso por los contendientes	Si se llega primero se tiene ventaja
Engañoso	Es fácil salir pero difícil volver	No se obtiene ventaja. Sólo ataca si estás seguro de vencer
Neutral	Desfavorable para ambos	Nadie toma la iniciativa del ataque; se presta para maniobras de atracción y contraofensiva
Estrecho	Ocupa, bloque accesos y espera	Se presta a ofensivas condicionadas
Accidentado	Si llegas primero ocupa mejor posición y espera Si llegas segundo atrae al enemigo, no lo sigas	No se persigue al oponente
Distante	Determina la inutilidad de atacar o atraer al combate	Es un *impasse*

Fuente: Elaboración propia. Sun Tzu (2008).

La información incluida en la tabla sirve como recordatorio de que dentro de las características del terreno se deben considerar: la forma, la extensión, la distancia, la posición geográfica, la orografía, el clima, la flora y fauna. Aunque a primera vista, algunos de estos detalles no existen en el mundo digital, poco a poco se va descubriendo la existencia de fenómenos dentro de la red o del espectro electromagnético que puede ser comparados con sus similares del mundo material. Por ejemplo, hablar de una flora digital aún es algo inviable, pero hablar de animales virales ya es posible. De hecho son estos virus de diseño programable los que se convierten en las ciberarmas utilizadas para la defensa y el ataque en el entorno de la ciberseguridad.

Adicionalmente, si se aplica la tipología del terreno antes citada al ciberespacio, se obtiene que, debido a la naturaleza flexible del ciberespacio, éste posee la capacidad de emular cada uno de los tipos señalados por Sun Tzu (2008) o incluso una combinación de ellos bajo ciertas condiciones y momentos. Por ejemplo, es claro que el internet es un espacio de libre acceso, del que toman ventaja aquellos que primero llegan; pero en ciberataques con *exploit*[10] bien pudiera funcionar el ciberespacio bajo la clasificación de estrecho, ya que el *exploit* es la llave que permite el avance de las fuerzas amigas, pero limita los movimientos del enemigo.

10. *Exploit* se entiende como un programa o parte de un programa malicioso que busca "explotar o aprovechar" las vulnerabilidades de los sistemas; puede ser diseñado para inhabilitar o destruir el sistema al cual ataca.

Es decir, el ciberespacio es un escenario reflejo de lo que ocurre en el mundo material, y por ello todo estratega debe atender lo que Sun Tzu (2008, p. 117) concluye para el terreno: "Conoce el terreno, conoce las condiciones meteorológicas; entonces tu victoria será total". Con esto se resalta la importancia del ciberespacio como nuevo escenario para la ciberseguridad de las naciones.

El termino ciberespacio[11] data de la segunda mitad del siglo XX, y fue presentado por Alvin Toffler en su libro *Future Shock* (1970). El concepto de ciberespacio presentado por Toffler fue recreado por William Gibson (2007, p. 71), quien lo presentó primeramente en su obra "Burning Chrome" (1982) y lo popularizó en su obra "*Neuromancer*" (1984) como sigue:

> El ciberespacio. Una alucinación consensual experimentada diariamente por billones de legítimos operadores, en todas las naciones, por niños a quienes se enseña altos conceptos matemáticos… Una representación gráfica de la información abstraída de los bancos de todos los ordenadores del sistema humano. Una complejidad inimaginable. Líneas de luz dispuestas en el no-espacio de la mente, agrupaciones y constelaciones de datos […] el propio terreno de lo virtual, donde todos los medios se juntan (fluyen) y nos rodean.

Definición que toca dos temas importantes: la conexión global en red y la representación gráfica de los bancos de información, que llevan a la conformación de una realidad virtual que todo conecta. Lo anterior es un indicador de la procedencia futurista y civil del término; ya que fue el mundo tecnológico que trajo consigo la computadora el que dio vida al concepto de ciberespacio, para después ser adoptado por la ciencia militar. En breve, el fenómeno del ciberespacio fue contra todo pronóstico de la práctica a la táctica.

Los autores antes citados fueron seguidos por algunos otros como Benedikt (1991, 15) que se refiere al ciberespacio como "[…]nuevo universo, universo paralelo creado y sostenido por las computadoras y las líneas de comunicación del mundo[…]"[12] o Batty (1993, pp. 615 - 616) que indica que el ciberespacio es "un nuevo tipo de espacio, invisible a nuestros sentidos, un espacio que se podría convertir en algo más importante que el mismo espacio físico[13] […]". En donde ya se encuentran indicios de la alta dependencia de la vida en sociedad en el ciberespacio, lo que finalmente atrajo la atención de los gobiernos y ha llevado al desarrollo de la ciberseguridad.

11. El termino ciberespacio desde la década de los años 1990 inicio con su conversión a sinónimo de internet y posteriormente de la WWW, en específico entre los círculos académicos y grupos de activistas.

12. Traducción propia.

13. Traducción propia.

Esta condición de dependencia la expone Sampaio (2001) diciendo que las sociedades que se han construido sobre la interacción en todos los ámbitos a través de las redes de computadoras y del ciberespacio si bien han logrado mejorar sus procesos de producción, comunicación, prestación de servicios, etc. de igual forma se han vuelto más vulnerables, poniendo en riesgo su defensa y seguridad. Conocidas estas vulnerabilidades por el enemigo son fácilmente utilizables para generar el caos y desmoralización, lo cual pone en práctica más de uno de los principios de la doctrina militar de Sun Tzu (2008, pp. 69-72), entre los que destacan: a) para avanzar sin encontrar resistencia hay que atacar los puntos débiles; y b) un ejército evita lo fuerte y ataca lo débil.

Con el tiempo, el ciberespacio ha crecido en importancia dentro de las estratégicas de seguridad nacional de los Estados que cada vez más dependen de la interacción con la red para sus actividades no sólo comerciales, académicas, financieras sino también de defensa y ataque. Por ello, la puntilla a la discusión internacional sobre la conceptualización bélica del ciberespacio la ofreció, el ex Secretario de Defensa de los EE. UU., William J. Lynn III (2010) quién definió el ciberespacio como el "quinto dominio de la guerra".

Con ello se derribaron las diferencias, se aceptó que existe una competencia férrea entre los Estados en ese ámbito bélico desde finales del siglo XX y los Estados tecnológicamente dependientes se enfocaron al fortalecimiento de sus medios de ciberseguridad. De igual forma, para aquellos Estados que no habían considerado la fragilidad de los sistemas digitales de mando y control de sus instalaciones vitales, esta declaración significó el comienzo de un plan para elaborar una estrategia para defender y obtener ventajas en dicho escenario virtual de guerra[14].

De igual forma, con base en las declaraciones de Lynn la sociedad internacional se ha dado a la tarea de establecer una regulación para las actividades (bélicas o no) que se realizan tanto en el ciberespacio como en el internet y que pudieran dar lugar a ciberconflictos. Sin embargo, existen un alto grado de incertidumbre debido a la falta de conceptos que definan algunos de los fenómenos que ocurren dentro del ciberespacio; en especial, temas como los ciberataques, la identificación efectiva de los atacantes, el grado de respuesta necesario, las reglas del combate y la definición legal de ciberarma. Si lugar a dudas, este novedoso escenario de guerra se encuentra en todos lados y todos se convierten en un potencial ciberguerrero, y por su flexibilidad genera una serie de cuestionamientos sobre el derecho de la guerra y la soberanía nacional.

14. Al respecto tenemos que de acuerdo con la *European Union Agency for Network and Information Security* (enisa) sólo la tienen 56 Estados del mundo. (22 Europeos, y 36 del resto del mundo – destaca que en la lista se encuentren países como Jamaica y Dominica, ya que a pesar de que los gobiernos correspondientes enfrentan problemas económicos han tomado la ciberseguridad como un asunto que requiere un plan de acción para salvaguardar la seguridad de su nación).

Armamento digital disponible

La historia de la guerra indica que la influencia de los desarrollos tecnológicos aplicados a los armamentos ha generado grandes cambios en las estrategias y tácticas de guerra. La llegada de las computadoras como centros de control y su posterior interconexión a través de la red, es un fenómeno que cada día atrae la atención de los ejércitos para lograr sus objetivos minimizando los riesgos. Todo parece indicar que en el siglo XXI, los avances tecnológicos han permitido la generación de armamentos electrónicos y digitales, que parecen sacados de una película de ciencia ficción. De hecho la popularidad de la red de redes y la dependencia que dicha herramienta de comunicación ha creado, se convierten en el medio idóneo para poner a prueba la efectividad de las armas digitales.

Que se entiende por ciberarma

Según se relata en la Ilíada (Homero, 1997), el caballo de Troya es el primer utensilio de guerra que con base en el engaño y el ingenio logró la toma de una ciudad desde dentro. Es el precursor, del uso de medios inexplorados que aprovechando otra dimensión (en este caso la tercera dimensión) pudieron traspasar las barreras y tomar una posición ventajosa en la retaguardia enemiga: "Y en nuestro sacro alcázar emplazamos el monstruo de la desgracia" (Ilíada II; s.t. p. 245). Esta hazaña lograda utilizando una dimensión "desconocida" ha sido emulada por la ciberseguridad, que ha recurrido al empleo de la "cuarta dimensión" para lograr sus objetivos. Incluso una de las ciberarmas existentes se denomina troyano, debido a la forma en que se inocula y su poder destructivo.

En el presente existe un serio debate sobre lo que se entiende por ciberarma; sobre todo porque las potencias no han llegado a un consenso sobre dicho tema. En el mismo tenor de ideas Tomas Rid y Peter McBurney (2012), exponen que es difícil definir las ciberarmas porque constituyen una novedosa forma de generar daño.

Sin embargo, ya que un arma es todo aquello que se utiliza para causar daño, y se han documentado casos en donde se han realizado ataques virtuales, utilizando la información y al espectro electromagnético como instrumento y medio de guerra, respectivamente, se puede hablar de ciberarmas.

Cabe recordar que las armas digitales son diseñadas para causar daños materiales y físicos a través del espectro electromagnético y el internet; sin importar si el daño paraliza una ciudad, un pueblo, una organización o la vida de un individuo. Ya en discusiones recientes, Peter Lorents y Rain Ottis (2010) han definido las ciberarmas como: "una tecnología informática basada en sistemas del mismo orden (software,

hardware, y medio de comunicación) que ha sido diseñada para perjudicar y dañar la estructura y funcionamiento de algún otro sistema". Esta amplitud de la definición permite la instauración de diversas clasificaciones para las armas tecnológicas que atentan contra la ciberseguridad de los Estados.

Se debe aclarar que no existe un consenso sobre la mejor manera de definir una ciberarma; sin embargo, con base en las definiciones existentes para armas se puede generar un constructo que busque dar claridad a esta situación. La definición de arma ofrecida por el Diccionario de la Real Academia Española es: "[…] (Del lat. arma, -ōrum, armas). 1. f. Instrumento, medio o máquina destinados a atacar o a defenderse." (RAE, s.f.) que sirve perfectamente como punto de partida para los objetivos del presente trabajo.

Por ello, al adaptarla para expresar lo que podría ser definido como ciberarma queda como sigue: instrumento, medio o máquina destinados a atacar o defenderse en cualquier ámbito (material o virtual) del conflicto. Definición que permitiría además utilizar la clasificación tradicional entre armas convencionales y de destrucción masiva proporcionada por la Oficina de Asuntos de Desarme de las Naciones Unidas (s.f.) [15] para enmarcar a los instrumentos de ciberataque y ciberdefensa como un arma convencional; pero, sin olvidar que a la luz de los avances y el impacto de los ciberataques pudiera llegar a convertirse con mucha facilidad en un arma de destrucción masiva. Su capacidad y rapidez de transformación de un arma no letal a un arma letal[16] es precisamente lo que atrae a los estudiosos de la seguridad nacional.

Las ciberarmas se pueden clasificar de acuerdo con su alcance, método de implantación y propósito. Entre los más importantes son: virus, gusanos, programas maliciosos[17], bombas lógicas, *botnet*, programas espía (spyware), *backdoors* y troyanos. Para el efecto se incluye una breve descripción de algunas de las ciberarmas arriba mencionadas, con base en la información presentada por la compañía de ciberseguridad *Panda Security* (s.f.).

Virus: programas de características diversas que se introducen en las computadoras a través de correo electrónico, USB, internet, etc. Se caracterizan por reproducirse infectando otros archivos o programas y realizar acciones molestas o dañinas para el usuario. Su nombre se debe a su enorme parecido con los virus humanos. Se les puede llamar micro-progamas.

15. Para mayor información sobre la clasificación de las armas en el ámbito internacional consultar: http://www.un.org/es/disarmament/

16. El arma no letal se define como un arma que esta explícitamente diseñada y empleada para inutilizar al personal y material, minimizando las pérdidas humanas, las heridas de largo plazo a las personas y los daños no deseados a la propiedad y el medio ambiente.

17. El conjunto de ellos se definen como *malware* que se puede definir como cualquier programa, documento o mensaje que puede causar daño a una computadora. También se conocen como amenazas a la seguridad de las computadoras.

Gusanos: Similares a los virus porque se auto-replican y son dañinos, pero se diferencian en que no necesitan a otros archivos para reproducirse. Se reproducen a sí mismo sin dañar otro archivo pero con suma rapidez lo que colapsa las redes. Se propagan generalmente por correo electrónico.

Programas maliciosos (*malware*): implica tanto pérdida de datos como pérdida de productividad; entre los programas que se incluyen están: *dialer*, *joke*, riesgo de seguridad, herramienta de *hacking*, vulnerabilidad, programa espía, *oax*, *spam*.

Troyanos: se diferencia de los virus porque no se reproduce infectando a otros archivos ni tampoco se propaga haciendo copia de sí mismo. Emulan a los astutos griegos de la mitología y llegan a la computadora como un programa aparentemente inofensivo, sin embargo al ejecutarlo aparece su segunda arma, el troyano. Pueden ser sumamente peligrosos realizan acciones tales como captura de textos introducidos por el teclado o registro de las contraseñas.

Backdoor: programa que se introduce en la computadora de manera encubierta, aparentando ser inofensivo. Una vez ejecutado establece una "puerta trasera" a través de la cual se puede controlar la computadora. Permite realizara acciones que comprometan la información o dificulten el trabajo del usuario. Pueden dar acceso a toda la información, eliminar archivos, destruir información, reenviar datos confidenciales a una estación externa o abrir puertos de comunicación.

A estas armas habría que sumarle las ciberarmas que tienen la capacidad de aprender del entorno y se modifican de acuerdo con las condiciones en las cuales se desarrollan; son las llamadas "*learning weapons*" (armas que aprenden).

Tabla 2. Clasificación de los virus informáticos.

Según el destino de infección	Según sus acciones y/o modo de activación
Archivos ejecutables	Bombas
Sector de arranque	Camaleones
Virus multipartición (pueden simultáneamente infectar archivos, sectores boot de arranque y tablas FAT)	Reproductores
Residentes en memoria	Gusanos
Macrovirus	Backdoors (puertas traseras)
Actives Agents y Java Applets	
Html	
Caballo de Troya	

Técnicas de programación de virus A sabiendas que son contrarrestados por las herramientas antivirus los nuevos virus utilizan diversas técnicas para lograr burlar a los guardianes de la seguridad cibernética, entre ellas se encuentran: stealth (ocultamiento de los signos de infección); tunneling (sobrepasamiento para lograr acceder directamente a los servicios del sistema a través de sus direcciones originales, sin pasar por el control de otros programas); armouring o antidebuggers (un debugger es un programa que permite descompilar ejecutables para conocer su código original); polimorfismo o automutación (consiste en cambiar el método de encriptación de generación en generación, usa un algoritmo de encriptación para dificultar la acción del antivirus); y TSR (programas residentes en memoria (TSR) permanecen alojados en esta durante toda su ejecución).	

Fuente: Elaboración propia. (nisu.org, s.f.).

Aclarando que su consideración como ciberarmas es resultado de que dichos programas o códigos maliciosos bajo ciertos contextos pueden sabotear y dañar tanto sujetos como objetos; por ello, una vez que logran atentar contra la ciberseguridad de las instituciones y de los individuos e incluso causar su destrucción o muerte, se convierten en un instrumento de guerra de suma utilidad en el ciberespacio.

La diversidad de formas para hacerse con el control de infraestructura crítica de una nación convierte a las ciberarmas en el medio idóneo para doblegar la voluntad del enemigo sin luchar. Esto se lograría si un Estado no toma las medidas políticas, económicas, sociales y militares para garantizar la ciberseguridad. De esta forma tal y como lo menciona Kenneth Geers (2009) no anticipar que un Estado puede entrar en una parálisis al perder el control de sus plantas nucleares, sus sistemas de control de tráfico aéreo, de las casas de bolsa y sistema financiero, de la información estratégica y secreta de los planes nacionales, se convierte en una vulnerabilidad que puede ser explotada por los potenciales enemigos con suma facilidad y gran impacto en el poder de respuesta.

Desde el inicio de su artículo Geers (2009: p. 1) invita a los gobiernos a tomar en serio la amenaza proveniente del ciberespacio e invertir más en su ciberseguridad diciendo: "*As dependence on IT and the Internet grow, governments should make proportional investments in network security, incident response, technical training, and international collaboration*." ["Según como la dependencia en las TI y el internet aumenta, los gobiernos deben hacer inversiones proporcionales en la seguridad de la red, respuesta a incidentes, capacitación técnica y colaboración internacional[18]."]. Esto Geers lo expresa como una advertencia de lo que pudiese ocurrir en un mundo cada vez más dependiente de las tecnologías de la información en donde los efectos de las ciberarmas pueden ser incluso más devastadores que los efectos de las armas tradicionales.

Como ejemplo de los efectos negativos de los ciberataques a instalaciones de la infraestructura crítica se tienen: primero, el ciberataque que se fraguó contra Estonia en 2007 (Jenik, 2009) y que afectó los sistemas de servicios gubernamentales, bancarios, y de comunicación que se brindan a través de la red paralizando la ciudad por algunas horas o incluso días; segundo, el ataque a la planta nuclear ubicada en Natanz con el objeto de frenar el programa nuclear del gobierno iraní, fue un ataque concertado entre fuerzas estadounidenses e israelíes (Farwell, 2011); tercero, existen evidencias del ciberataque realizado por Israel contra Siria bajo la "Operación Huerto" (Rid, 2012) para desarticular los sistemas de defensa aérea durante el 2007 y poder realizar un ataque aéreo contra una supuesta instalación nuclear de Siria.

Por otro lado, tres de las ciberarmas que han generado mayores daños, en años recientes, a la infraestructura de las naciones atacadas son: *Stuxnet, Duqu* y *Flame*. Dichas armas han sido utilizadas con efectividad en cada uno de sus casos logrando sus objetivos con creces y por años sin ser descubiertos. Tal es su complejidad y sofisticación que incluso de acuerdo con un comunicado conjunto de prensa de *Kaspersky Lab* e ITU (2012) son consideradas como "super-ciberarmas". Lo cual equivale a tener ciberarmas de grandes proporciones y potencialmente de destrucción masiva, como ha sido sugerido anteriormente en este trabajo.

Tabla 3. Tres ciberarmas de gran impacto

Nombre	Objetivo	Posible origen
Stuxnet	El programa nuclear de Irán, lo lanzó el presidente Bush bajo la operación "Olympic Games". Diseñado para atacar los sistemas de control de la marca Siemens.	EE.UU. e Israel

18. Traducción propia.

Duqu	Troyano, diseñado para el robo de información. Creado sobre la plataforma de Stuxnet. Tiene una versión Duqu 2.0	EE.UU. e Israel
Flame	Computadoras del Medio Oriente con el objeto de robar todos los datos; tiene capacidad para grabar sonidos, comunicaciones de bluetooth, capturas de pantalla, datos de contacto y conversaciones de mensajería por internet. Se dice es una versión mejorada del virus Stuxnet. En especial se piensa en Irán. Tiene por principal objetivo el ciberespionaje.	EE.UU. e Israel
Todos ellas se convierten en un conjunto de herramientas con características flexibles que conjugan la forma de actuar de los virus, los gusanos, las puertas traseras y los troyanos. Trabajan de forma modular y utilizan el LUA como lenguaje de programación.		

Fuente: Elaboración propia. Datos de (eleconomista.com.mx, 2012); (eleconomista.com.mx, 2011); (latam.kaspersky.com, s.f.); (latam.kaspersky.com, s.f.); y (securelist.com).

Con base en lo anterior, se puede definir a la ciberarma como la combinación de un método de propagación, explotación y carga con el propósito de crear efectos destructivos tanto materiales como virtuales/digitales. Pero, para que los programas de computadora sean considerados ciberarmas, al menos momentáneamente, deben ser utilizados en un conflicto entre los actores clásicos de las relaciones internacionales; en otras palabras, por un Estado contra otro Estado, lo cual remite a una interpretación estato-céntrica y realista de la ciberseguridad. Esta interpretación teórica choca con la realidad que se vive en el ciberespacio, en donde todos los participantes se convierten tanto en garantes como en amenaza a la ciberseguridad, es decir no existe una clara separación – ni jurídica ni técnica – entre el cibercrimen y el ciberacto de guerra.

En relación el impacto económico de los ciberataques en las finanzas estatales, los más recientes estudios sobre los costos de los ciberataques hablan de que por lo general, un ataque cibernético a los sistemas una pequeña o mediana empresa genera gastos de recuperación y respuesta de hasta medio millón de dólares por evento; pero alcanzan miles de millones de dólares si impactan redes del sistema financiero y de grandes empresas transnacionales[19].

Lo anterior lleva a los expertos de Grand Thornton a calcular un gran total de 315 mil millones de dólares en costos totales por los ataques sufridos desde 2009 (Leyva, 2015). La multiplicación de los ataques contra grandes consorcios, han tenido en respuesta un aumento en los costos de los seguros contra robo de datos personales, de acuerdo con un reporte de la Cnet (Collins, 2015) los límites superiores de los seguros se han establecido en $100 millones de dólares, lo que hace que las empresas tengan grandes dificultades y/o riesgos para operar en un mundo cada vez más interconectado y por lo tanto más vulnerable.

Como se puede observar estos ciberarmamentos se centran en desestabilizar la economía de organizaciones, pero al mismo tiempo, en efecto domino, de las naciones que las albergan o patrocinan. Estamos sin lugar a dudas en una ciberguerra económica, que busca destruir la fortaleza económica de grandes empresas y de naciones enteras al destruir su prestigio, interrumpir sus operaciones, robar sus activos, y finalmente tomar el control de todas sus redes e información. Después de analizar el daño económico que generan las ciberarmas, esto sugiere una alta sofisticación, personal profesional y altamente capacitado así como de una gran infraestructura de soporte; lo que genera cuestionamientos como ¿Cuál es el costo de construir o diseñar una ciberarma? ¿Cuánto tiempo se requiere para construir una ciberarma? ¿Son los Estados los principales productores de ciberarmas?

Costo de las armas digitales

El nuevo avión caza *F-35 Lighting* II también conocido como el *Joint Strike Fighter*[20] de los EE.UU. contiene lo último en tecnología aeroespacial, de materiales, de comunicaciones y de armamento y, es el ejemplo más reciente de los altos costos de las armas convencionales. Para lograr su construcción han transcurrido aproximadamente 15 años desde la presentación del prototipo *Lockheed Martin* X-35[21], con un costo de

19. Los ataques sufridos por las compañías de Sony ($100 millones de dólares aproximadamente), Target ($264 millones de dólares) y Home Depot ($234 millones de dólares) son un ejemplo reciente de los costos provocados en términos monetarios, credibilidad y confianza de sus consumidores, accionistas y socios.

20. Es un proyecto militar internacional para generar el próximo avión caza iniciado en 2001 bajo el nombre del programa *Joint Advanced Strike Technology (JAST)*.

21. La licitación para la fabricación del nuevo avión caza de la Fuerza Aérea de los EE.UU. fue ganada por Lockheed Martin el 26 de octubre de 2006 con el prototipo X-35, el cual entró en producción en 2006 bajo la denominación de F-35 y luego renombrado F-35 Lighting II. Información adicional se puede encontrar en: http://www.jsf.mil/

producción aproximado de entre 89 a 200 millones de dólares por unidad (según el reporte de costo de armamento de la Fuerza Aérea de los EE.UU.).

Se cree que durante el ataque que sufrió la compañía *Lockheed Martin* el 21 de mayo de 2011 fueron sustraídos datos importantes sobre las especificaciones técnicas de la aeronave a pesar de que la compañía aseguró a la Casa Blanca que "Ningún cliente, programa o dato personal de los empleados ha sido comprometido" (2011, anónimo).

En comparación con el costo y la dificultad de acceso a las armas convencionales, las ciberarmas pueden ser obtenidas en el Mercado Negro internacional por algunos cuantos dólares. Las ciberarmas tienen por característica ser más baratas que las armas tradicionales, difíciles de detectar y no se pueden atribuir a un atacante en específico. Esto ha sido sostenido por exfuncionarios de agencias de inteligencia de los EE. UU. como James Woolsey (Aitoro, 2009) al decir "Good hacker software is easier to obtain than a tank or a rifle. Intelligence officials such as former CIA Director James Woolsey warn that even terrorist groups will possess cyber weapons of strategic significance in the next few years." [Un buen programa hacker es más fácil de obtener que un tanque o un rifle. Los oficiales de inteligencia como el ex Director de la CIA James Woolsey advirtió que incluso los grupos terroristas tendrían en su poder armas de importancia estratégica en los próximos años."[22]]

Capacidad de destrucción

Pero las ciberarmas no solamente tienen efectos monetarios. Al ser armas multidisciplinaria puede ocasionar daños psicológicos y sociales, destruyendo la moral de la sociedad para lograr su apoyo o para desestabilizar al gobierno; efectos políticos, al desacreditar los esfuerzos que los líderes hacen para salvaguardar a su población e implantar políticas públicas de bienestar general; y por supuesto efectos militares, ya que pueden deshabilitar la infraestructura estratégica critica de una nación, poniendo en jaque a las fuerzas armadas por no contar con medio de comando y control efectivos ni instrumentos suficientes para brindar ciberseguridad a sus instalaciones, activos, personal y materiales estratégicos.

Pero ¿qué ha detenido la carrera de ciberarmamento? De acuerdo con lo establecido por Trias and Bell (2010: p. 97) es el miedo a los peligros colaterales que pudiera tener un ciberataque ofensivo o defensivo; dichos autores lo establecen como sigue: "Los ataques a través del ciberespacio contra activos cibernéticos de igual forma pueden resultar en daños colaterales en cascada. El temor de estos efectos secundarios comunes ha evitado que los líderes estadounidenses de aprieten el disparador del armamento cibernético."

22. Traducción propia.

Principales medios para realizar los ciberataques

Las ciberarmas son utilizadas para realizar diversos ciberataques, entendidos como: actos deliberados lanzados a través del ciberespacio para manipular, destruir, denegar, degradar o destruir a las computadoras o sus redes, y/o la información que se encuentra en ellas, que generan daños en el ciberespacio o en el mundo material y comprometen la seguridad nacional de un Estado.

Por ello, los ciberataques se han convertido en una prioridad para los sistemas de defensa de los Estados. Los ciberataques que se registran a lo largo del mundo se llevan a cabo utilizando una diversidad de tácticas y ciberarmas.

De acuerdo con el "*Internet Security Threat Report*" (Sysmantec, 2015) entre las principales amenazas a la seguridad de los Estados, organismos e individuos se tienen a: ciberespionaje, infecciones con virus, robo de información, ataques contra la seguridad de las industrias, intercepción de comunicaciones con puertas traseras y ataques de reconocimiento. Los ciberataques tienen por objetivo el espionaje, el daño financiero y la manipulación de la infraestructura critica nacional; su impacto es suficiente para influir en el curso de los conflictos entre gobiernos, entre ciudadanos y entre ellos. En consecuencia los ataques se pueden clasificar acorde a los actores de los ataques como patrocinados por los Estados o realizados por actores de la sociedad civil colectiva o individualmente.

En resumen, los medios utilizados como instrumentos de ciberataque tienen por objetivo paralizar la vida de una nación conectada a la red; es decir, mediante la introducción de virus informáticos se puede anular total o parcialmente la información que circula por las redes establecidas a nivel mundial. De acuerdo con el documento presentado por la ONU (2013, X) existen ciberataques que van desde desfigurar los sitios web, pasando por la negación de servicios hasta el robo de información e infiltración en las redes de computadoras y servidores. Es por ello que Lin (2012) advierte lo siguiente: "Los ciberataques tienen el objetivo de prevenir que los usuarios tengan acceso a los servicios o interrumpir las maquinas que son controladas por computadora, mientras que la ciber-explotación es realizada para penetrar las computadoras para obtener información". Quedando claro que los ciberataques se orientan a la búsqueda o destrucción de información, el control de las máquinas y negar acceso a los servicios, lo cual desquicia con facilidad las actividades de una nación dependiente de la red.

Los ciberataques tienen por objetivo entre otras muchas cosas: primero, explotar el poder y alcance del internet (Goble, 1999); segundo, explotar su vulnerabilidad (Fulghum et al, 2007); tercero, los Ciberatacantes se benefician del anonimato (Geers, 2008); y cuarto, incluso los Estado-nación pueden ser considerados

como objetivos (Keizer, 2009). En consecuencia, entre las características que hacen de los ciberataques un medio efectivo para atentar contra la seguridad de los Estados se tiene las siguientes: a) Baratos – los medios de ataque pueden ser comprados en internet a un bajo costo o incluso gratis; b) Simples – un atacante con habilidades básicas en el manejo de tecnologías de la información puede llevar a cabo el ataque; c) Efectivos – incluso los ataques más pequeños pueden causar grandes daños; y d) Bajo riesgo – es fácil para los agresores evadir la detección y persecución a través de la red de computadoras y de programas que esconden los rastros.

Amenazas digitales contra la seguridad nacional de los Estados

La naturaleza de las amenazas está determinada por sus motivaciones e intenciones. Por ello, de acuerdo con el *"Global Internet Security Threat Report*" publicado en abril de 2009 por Sysmantec, se pueden mencionar al ciberespionaje, las ciberoperaciones militares, el ciberterrorismo, y al cibercrimen como las principales amenazas a la seguridad de los Estados[23]. Clasificación que presenta dos amenazas procedentes de otros Estados (ciberespionaje y ciberoperaciones militares); una con un uso dual entre los Estados y los grupos terroristas (el ciberterrorismo) y uno más que se podría decir es exclusivamente autoría total de los grupos criminales (el cibercrimen). Esta tendencia de las amenazas se ha visto continuada a lo largo de la segunda década del siglo XXI; por ejemplo, el *Internet Security Threat Report* (Sysmantec, 2014:5), nuevamente menciona al ciberespionaje como una de las principales amenazas a la seguridad del internet, lo cual confirma que este flagelo es uno de los enemigos a vencer por las fuerzas de seguridad.

Sin temor a equivocarse y como resultado del análisis de la tendencia de los conflictos del siglo XXI, el ciberespacio estará presente en cualquier guerra (incluso antes de iniciar el combate) que se produzca en el futuro; ya que se utiliza como medio de lanzamiento de las ciberarmas militares, pero en tiempo de paz y durante el conflicto se puede emplear para el ciberespionaje que se convierte la táctica para obtener información estratégica del enemigo. Por ello, los Estados deben reaccionar con acciones que garanticen la ciberseguridad con una estrategia de ciberguerra.

Ciberguerra un concepto inacabado

La estructuración de conceptos sólidos y universales para los diferentes fenómenos que atentan contra la seguridad internacional es una obligación de todos los actores del sistema internacional. Sin embargo, la llegada de nuevos conceptos que son, por una razón u otra, popularizados trae consigo un empleo de los mismos

23 Symantec, "Global Internet Security Threat Report," April 2009 y 2014.

que no sigue reglas y genera más confusión que certeza. Tal es el caso del término "ciberguerra", que designa vagamente algún tipo de ataque o represalia, intrusión ilícita de una red de computadoras o un acto de ciberespionaje. Lo anterior puede ser parte de una estrategia u conflicto político / militar para abatir la ciberseguridad de un Estado al reducir las capacidades de defensa y ataque de un actor internacional en el ciberespacio, al mismo tiempo que se emprende un ataque directo con fuerzas materiales.

Lo anterior ha llevado a que la ciberguerra se considere como infoguerra, guerra de redes o guerra digital y se confunda con la guerra electrónica[24]; y que el ciberespacio se convierta en el Talón de Aquiles de los sistemas cibernéticos. Sobre todo cuando las fuerzas armadas al igual que gobiernos y economías que protegen son cada vez más dependientes de las tecnologías de la información; un ejemplo de lo anterior es lo que Orton (2009) indica sobre la fuerza aérea estadunidense "*In 2010, the United States Air Force will procure more unmanned than manned aircraft for the first time*."[En 2010, la Fuerza Aérea de los EE.UU.obtendrá más aernovaes no tripuladas que tripuladas por primera vez[25]."]

Qué es la ciberguerra

Para explicar el fenómeno de la ciberguerra habría que retomar las causas y motivaciones de la guerra que presenta Stephen Van Evera en su libro "Causes of War: power and roots of conflict" (1999:4). Las causas según Van Evera se pueden clasificar en cinco grupos principales de hipótesis: la guerra es más probable cuando el control de los recursos; cuando el poder de los Estados fluctúa repentinamente; la conquista es fácil; cuando la ventaja radica del primer lado; y finalmente, cuando Estados caen presa del falso optimismo. Todas estas causas se ven impulsadas por dos motivaciones principales (Howard, 1984:10): la búsqueda del poder propio y el temor del poder de otros.

La diferencia entre motivaciones y causas radica en que las motivaciones son parte de la naturaleza humana[26], es decir son pasionales y nada racionales; mientras que las causas son elementos racionales que se encuentran en el preámbulo de la guerra y conducen a ellas. Sin embargo, ambas tienen como objetivo final mantener o incrementar el control e influencia sobre otros. Exponiendo para el efecto lo que el realista Thomas Hobbes (1958:86) dice sobre el poder, "existe como inclinación

24 La guerra electrónica (*Electronic Warfare*) se entiende como las acciones que tienen por objetivo bloquear, interceptar y/o negar la transmisión del mensaje entre un Transmisor y un Receptor.

25 Traducción propia.

26 La naturaleza humana ha sido identificada como la principal motivación de la guerra desde la época de Tucídides quien dice al respecto lo siguiente: "la conducta humana es guiada por el miedo (Phobos), el interés propio (Kerdos) y el honor (Doxa). Estos aspectos de la naturaleza humana provocan guerra e inestabilidad…en Kaplan, R. (2002). El Retorno de la Antigüedad. Barcelona, España: Ediciones B, p. 87.

general de toda humanidad un perpetuo e incansable deseo de poder y más poder que cesa solamente con la muerte".

Esta búsqueda incansable del poder por el poder, es un factor clave en la aparición de conflictos entre Estados, los cuales utilizarían todos los medios y ámbitos de la guerra a su disposición para hacer doblegar la voluntad de lucha de su oponente incluso la ciberguerra. Para entender este último precepto es preciso partir del concepto establecido para la guerra desde el punto de vista de Karl Von Clausewitz (2005: 1) quien en su obra maestra "De la Guerra" define la guerra como:

> […] La guerra no es más que un duelo en una escala más amplia. Si quisiéramos concebir como una unidad los innumerables duelos residuales que la integran, podríamos representárnosla como dos luchadores, cada uno de los cuales trata de imponer al otro su voluntad por medio de la fuerza física […]

Definición que claramente establece lo siguiente: existen dos oponentes, con fuerza o habilidad suficiente para enfrentar al otro, tiene por objetivo imponer la voluntad propia utilizando todos los medios disponibles para tal efecto. De hecho nunca menciona que debe ser exclusivamente a través de fuerzas armadas, lo cual si bien coincide con la visión realista de los conflictos predominante en su época, abre la puerta para las operaciones especiales o la guerra asimétrica.

Con base en lo anterior, se dice que los líderes de opinión y doctrina son los países con mayor desarrollo en el tema de la ciberseguridad, por lo tanto determinan y construyen los conceptos a utilizar por el resto del mundo. Estudiar a esos Estados o líderes de opinión permite establecer parámetros de comparación y crítica. Por ello se cita lo que de acuerdo con el Departamento de Estado de los EE.UU. (DoS, 2010) se define como ciberguerra:

> ***Cyber Warefare (CW):*** *An armed conflict conducted in whole or part by cyber means. Military operations conducted to deny an opposing force the effective use of cyberspace systems and weapons in a conflict. It includes cyber attack, cyber defense and cyber enabling actions.*
>
> **[Ciberguerra (CG):** Un conflicto armado conducido en su totalidad o en parte por medios cibernéticos. Las operaciones militares conducidos para negar a una fuerza opositora el uso efectivo de los sistemas y de las armas del ciberespacio en un conflicto. Esta incluye las acciones de ciberataque, ciberdefensa y ciberhabilitación][27].

27 Traducción propia.

En el mismo tenor, según Jeffrey Carr el concepto de ciberguerra que fue conformado por el Departamento de Defensa es: "…*Cyber Warfare is the art and science of fighting without fighting; of defeating an opponent without spilling their blood*…" (Carr, 2011, p. 2). […Ciberguerra es el arte y la ciencia de combatir sin combatir; de vencer a un oponente sin derramar su sangre[28]…]. En donde se puede ver que dicha definición retoma las ideas presentadas por Sun Tzu en su obra "El arte de la Guerra", cuando se refiere a los actos estratégicos de un Estado en tiempos de guerra.

> En contraste, el autor Jeffrey Carr en su libro *Inside Cyber Warfare: Mapping the Cyber Underworld* (Carr, 2011, p. xiii) indica que los militares clasifican erróneamente a los actos internacionales de ciberconflicto como ciberguerra. En palabras del autor queda como sigue: "…*International acts of cyber conflict (commonly but inaccurately referred to as cyber warfare) are intricately enmeshed with cyber crime, cyber security, cyber terrorism, and cyber espionage*…" […"Los actos internacionales de ciberconflicto (comúnmente referidos como ciberguerra de manera errónea) están intrínsecamente entrelazados con el cibercrimen, la ciberseguridad, el ciberterrorismo y el ciberespionaje[29]…"].

Desde una perspectiva Europea se tiene lo que el Mando Conjunto de Ciberdefensa de España entiende por ciberguerra (Gobierno, 2013). Para esta dependencia la ciberguerra es: "…Ciberguerra: El uso de capacidades basadas en la red de un Estado, para interrumpir, denegar, degradar, manipular o destruir información residente en ordenadores y redes de ordenadores, o los propios ordenadores y las redes de otro estado…". Estableciendo que los objetivos de la ciberguerra son: la información en redes de computadoras, las computadoras, sistemas accesorios y finalmente la totalidad de la infraestructura de información y comunicaciones del enemigo.

Definiciones en las cuales se pueden encontrar como elementos comunes, los ciberataques, redes de computadoras, sistemas de control y comunicaciones, Estados como actores, ser parte de un conflicto armado en donde puede haber o no derramamiento de sangre. Al reflexionar sobre este hecho en donde las consideraciones son diferentes y/o no se cuenta con una definición internacional única se puede concluir lo siguiente: a) La ciberguerra es confundida con actos ilegales de diversa

28 Traducción propia.

29 Traducción propia

índole realizados por agentes no estatales; b) Los actos violatorios de la ciberseguridad pueden ser utilizados como la cubierta perfecta para los actos de guerra de un Estado; c) La ciberguerra es el conjunto de actos emprendidos exclusivamente por las fuerzas de un Estado para dominar o dañar a un tercero; y d) La ciberguerra es un medio idóneo para el equilibrio de poder, con base el conocimiento y la información.

El impacto logrado por los ciberataques así como los autores de dichos actos son los que determinan si un atentado contra la ciberseguridad es un acto de ciberguerra. Sin embargo, la condición de anonimato de los atacantes es la principal barrera para identificar con certeza cuales son los actos de ciberguerra y para hacer uso de los ciberejércitos como garantes de la ciberseguridad. En la actualidad, existe una línea muy tenue entre las actividades de ciberguerra y las del cibercrimen, que permite que los actores del sistema internacional que atentan contra la ciberseguridad de otros, queden impunes o sean clasificados equivocadamente. Tal fue el caso de tres ciberataques sufridos por Estados como Estonia, Rusia, Irán durante las primeras décadas del siglo XXI, que a pesar de los indicios con los que se cuenta sobre los atacantes y su efecto en las actividades de los Estados no han dado lugar a un conflicto armado de mayores proporciones.

Es conveniente señalar que los ciberataques que preocupan a los Estados son aquellos que provienen de otros Estados, grupos de ciberterroristas y hacktivistas; ya que son los que atentan contra la seguridad nacional, las instituciones y el poder del Estado. Sin embargo, la confluencia del cibercrimen con la acción de los Estados ha dado pie a una mezcla peligrosa que puede ser utilizada para atacar a otro Estado a través de cibermercenarios. Es decir, el Estado desarrolla y patrocina el diseño, desarrollo y producción de las ciberarmas, mientras que el cibercrimen las utilice para llevar a cabo ciberataques subrogados por los Estados, pero que de esta forma no pueden ser atribuibles a terceras partes. Algunas preguntas que surgen para reflexionar al respecto son: ¿cómo luchar una guerra donde el enemigo es un desconocido? ¿cuáles son los efectos colaterales de los ciberataques?

En respuesta a algunas de las preguntas los Estados han iniciado con la organización de fuerzas cibernéticas específicamente dedicadas a realizar la ciberofensiva y establecer las ciberdefensas. Estas nuevas unidades de las fuerzas armadas han consolidado los términos de ciberejércitos y ciberguerreros. En el análisis que hace Charlie Miller (s.f.) en su presentación titulada “How to build a cyberarmy to attack the U.S.” menciona a tono de burla que su ciberejército costaría $ 49 millones de dólares, que sería un costo menor que el presupuesto que gastan los EE.UU. (105 millones USD), Corea del Norte (56 millones USD) o Irán (76 millones USD) en mantener sus ciberfuerzas.

Además Miller (s.f.) le asigna algunas funciones esenciales a estos ciberguerreros, entre las que se encuentran: contar con sistemas de comunicación redundantes, realizar ciberataques tipo Distributed Denial of Service (DDoS), doblegar a los blancos duros, atacar y defender la infraestructura crítica, y atacar las redes áreas. Lo cual habla de las modificaciones en la organización y presupuestos de los sistemas de defensa y ataque de las fuerzas armadas del mundo; cada vez más se transforma en un ejército con fuerzas ciberespeciales.

En el mismo tenor, la revista Forbes en el 2012 hizo pública una lista de los costos de las ciberarmas llamadas exploits, que muestra los costos de 6 de los exploits zero-day que son ofrecidos por medio del grupo intermediario Grugq30, que según el artículo obtiene 80% de sus ganancias de hacer negocios con los EE.UU. En especial con el gobierno de ese país. La diferencia en costos con un arma convencional es abismal, y habla de la facilidad que existe para hacerse con una ciberarma.

Tabla 4. Costo de *exploits zero-day.*

Tabla 4. Costo de exploits zero-day	
Adobe Reader (5-30 mil USD)	Windows (60-120 mil USD)
Mac OSX (20-50 mil USD)	Firefox o Safari (60-150 mil USD)
Android (30-60 mil USD)	Chrome o Internet Explorer (80-200 mil USD)
Flash or Java Browser plug-in (40-100 mil USD)	IOS (100-250 mil USD)
Microsoft Word (50-100 mil USD)	

Fuente: Forbes, 2012.

En resumen, la ciberguerra es muy atractiva para las naciones pequeñas, ya que se requieren pocos medios para crear una bomba digital. Esta condición permite hablar de la ciberguerra asimétrica tal y como lo describe Geers (2011) "Because cyber warfare is unconventional and asymmetric warfare, nations weak in conventional military power are also likely to invest in it as a way to offset conventional disadvantages". ["Debido a que la ciberguerra es una guerra asimétrica, las naciones en poder militar convencional tienen probabilidades de invertir en ella como una forma de equilibrar las desventajas convencionales.31"] La ciberguerra representa para todos los Estados del mundo una alternativa muy eficaz para contrarrestar la falta de armas convencionales, es una forma de hacer la guerra que no requiere de una

30. De acuerdo con Forbes (2012) el grupo *Grugp* no es el único en este negocio sus competidores son, entre otros: *Vupen, Endgame* y *Netragard* que se dedican a la compra venta de *exploits*.

31. Traducción propia.

gran capacidad tecnológica, sino de individuos ingeniosos y expertos que exploten las debilidades de la infraestructura digital en beneficio de su nación. Corea del Norte y Siria son dos ejemplos de lo antes mencionado, ya que son Estados pequeños que han desarrollado grandes capacidades para iniciar y sostener una ciberguerra.

Del mismo modo la ciberguerra requiere de una preparación desde tiempo de paz, y por ello, el grupo de líderes nacionales deben desarrollar estrategias que den respuesta a los potenciales eventos conflictivos del ciberespacio. Sin embargo, las dificultades que enfrentarán para desarrollar estrategias efectivas se encuentran desde la definición del concepto mismo, es decir ¿Qué es lo que se califica como ciberguerra?

Conclusiones

El ciberespacio es el quinto dominio de la guerra y requiere de la elaboración de tácticas y estrategias que por un lado, maximicen los efectos de las ciberarmas; y por el otro, garanticen la ciberseguridad nacional. Es en el ciberespacio en donde toma forma el ciberpoder, entendido como el ataque y explotación de la red de computadoras, para de manera relativamente barata inhabilitar de manera efectiva el poder militar de un Estado adversario. Por lo tanto, los peligros que surgen del ciberespacio motivan que los ataques en represalia se efectúen sólo cuando los pilares de la seguridad nacional se vean en riesgo; lo cual también conlleva a una seria reconsideración de los conceptos de seguridad internacional y seguridad humana.

Debido a las características flexibles de tanto las ciberarmas como del ciberespacio, por ahora no hay una tecnología que garantice la ciberseguridad de los sistemas. A lo cual se debe agregar que las ciberarmas representan una seria ciberamenaza que atenta contra la ciberseguridad nacional en todos y cada uno de los campos de la actividad social que se encuentran conectados a la red. Remarcando el hecho de que no existe un sistema de alerta temprana contra ciberataques con ciberarmas; en consecuencia, la ciberseguridad es un trabajo constante de preparación y reacción a eventos. Por primera vez en la historia, las ciberarmas permiten que los Estados pequeños y con reducidos presupuestos para cuestiones de defensa causen severos daños a un enemigo poderoso. Sin lugar a dudas en las guerras futuras, las ciberarmas se pueden convertir en el medio eficaz para igualar la fuerza.

Hoy la ciberguerra cuenta con suficientes capacidades para realizar gran parte de las tareas estratégicas que anteriormente eran realizadas por medio del poder aéreo, naval, espacial o terrestre. Es decir, el poder cibernético o ciberpoder descrito por Castells (2005) empieza a tomar el lugar preponderante para vencer a un enemigo. En esta guerra del siglo XXI todo, absolutamente todo, puede convertirse en un objetivo de los ciberataques. Por ello, los Estados deben prepararse para lo imprevisto y para

desconectarse en caso de ser necesario o buscar medios alternos para el mando y control de los diferentes instrumentos de la ciberguerra.

Referencias

Anónimo. (29 de mayo de 2009). Lockheed bloqueó un "tenaz" ciberataque. CNN-expansión. [Edición en línea]. Recuperado el 10 de noviembre de 2015, de: http://www.cnnexpansion.com/negocios/2011/05/29/lockheed-bloqueo-un-tenaz-ciberataque

Anónimo. (29 de mayo de 2011). Lockheed, primer contratista del Pentágono, desbarata el ciberataque en su contra. Elmundo.es. [Edición en línea]. Recuperado el 10 de noviembre de 2015, de: http://www.elmundo.es/america/2011/05/29/estados_unidos/1306677928.html

Batty, M. 1993: The geography of cyberspace. Environment and Planning B: Planning and Design 20, 615-61. [Edición digital]. Recuperado el 15 de noviembre de 2015, de http://epb.sagepub.com/content/20/6/615.short

Benedikt, M. 1991: Introduction. In Benedikt, M., editor, Cyberspace: first steps, Cambridge, MA:MIT Press, 1-18

Buendía, M. (1984). La CIA en México (Vol. 11). Léon y Cal.

Carr, J. (2011). Inside Cyber Warfare: Mapping the Cyber Underworld. O'Reilly Media; Edición: 2 (31 de diciembre de 2011). Sebastopol, California, EE.UU.

Castells, M. (2005). La era de la información: economía, sociedad y cultura en la sociedad red. (vol.1). Madrid, España: Alianza Editorial

Collins, K. (12 de octubre de 2015). Computer attack insurance rates rise after high-profile breaches. Cnet. [Edición digital]. Recuperado el 15 de noviembre de 2015, de http://www.cnet.com/news/computer-attack-insurance-rates-rise-after-high-profile-breaches/

Diccionario de la Real Academia Española. (2014). 23ª ed., Edición del Tricentenario, [en línea]. Madrid: Espasa. Recuperado el 10 de noviembre de 2015, de http://lema.rae.es/drae/srv/search?id=oaOb3XHL0DXX20XGgLz8

Diccionario de la Real Academia Española. (2014). 23ª ed., Edición del Tricentenario, [en línea]. Madrid: Espasa. Recuperado el 10 de noviembre de 2015, de http://lema.rae.es/drae/srv/search?id=MGVDFlXuHDXX21Fm8K9h

Diccionario de la Real Academia Española. (s.f.) Arma. DRAE. [Edición digital]. Recuperado el 10 de noviembre de 2015, de http://lema.rae.es/drae/srv/search?id=VQPyw97SLDXX2XNv4IED

Farwell, J. P., y Rohozinski, R. (2011). Stuxnet and the future of cyber war. Survival, 53(1), 23-40.

Forbes. (23 de marzo de 2012). Shopping For Zero-Days: A Price List For Hackers' Secret Software Exploits. Forbes. [Edición en línea]. Recuperado el 10 de noviembre de 2015, de: http://www.forbes.com/sites/andygreenberg/2012/03/23/shopping-for-zero-days-an-price-list-for-hackers-secret-software-exploits/

Fulghum, D. A., Wall, R., & Butler, A. (2007). Cyber-Combat´s First Shot. Aviation Week & Space Technology 167(21), 28.

Geers, K. (2009). The cyber threat to national critical infrastructures: Beyond theory. Information Security Journal: A Global Perspective, 18(1), 1-7.

Geers, K. (2011). Sun Tzu and cyber war. Cooperative Cyber Defence Centre of Excellence. [Edición en línea]. Recuperado el 17 de noviembre de 2015, de: http://www.ccdcoe.org/articles/2011/Geers_SunTzuandCyberWar.pdf

Geers, K. (27 de agosto de 2008). Cyberspace and the Changing Nature of Warfare. SC Magazine. [Edición en línea]. Recuperado el 17 de noviembre de 2015, de: www.scmagazineus.com.

Gibson, William. (1987). Burning Chrome. Canadá: Ace Books.

Gibson, William. (2007). Neuromante. Barcelona, España: Minotauro.

Goble, P. (9 de octubre de 1999) Russia: Analysis from Washington: a Real Battle on the Virtual Front. Radio Free Europe/Radio Liberty. [Edición en línea]. Recuperado el 17 de noviembre de 2015, de: www.rferl.org

Homero, E. M. (1997). La ilíada y la odisea. Editorial Ink.

Howard, M. (1984). The causes of wars. The Wilson Quarterly (1976-), 90-103.

Jenik, A. (2009). Cyberwar in Estonia and the Middle East. Network Security, 2009(4), 4-6.

Kaplan, R. (2002). El Retorno de la Antigüedad. Barcelona, España: Ediciones B, p. 87

Kaspersky Lab e ITU. (2012. Kaspersky Lab e ITU descubren una nueva ciberamenaza avanzada cuyo reto es el ciberespionaje: Flame. Kaspersky. [Edición en línea]. Recuperado el 15 de noviembre de 2015, de http://latam.kaspersky.com/mx/sobre-kaspersky/centro-de-prensa/comunicados-de-prensa/kaspersky-lab-e-itu-descubren-una-nueva-ciber

Keizer, G. (2009). Russian 'cyber militia' knocks Kyrgyzstan offline. Computerworld. 1, 28. [Edición en línea]. Recuperado el 17 de noviembre de 2015, de: www.computerworld.com

Leyva, J. (19 de octubre de 2015). Ataques Cibernéticos cuestan 315 mil mdd. El Financiero. [Edición digital]. Recuperado el 10 de noviembre de 2015, de http://www.elfinanciero.com.mx/economia/ataques-ciberneticos-cuestan-315-mil-mdd.html

Libicki, M. (2009). Ciberdeterrence and Cyberwar. California, EE.UU.: RAND Corporation.

Lin, H. (2012). A virtual necessity: Some modest steps toward greater cybersecurity. Bulletin of the Atomic Scientists, 68(5), 75-87.

López, G. (1958). Diccionario Enciclopédico de la Guerra. Madrid, España: Gloria.

Lorents, P., & Ottis, R. (Junio, 2010). Knowledge based framework for cyber weapons and conflict. In Proceedings of Conference on Cyber Conflict, CCD COE Publications, Tallinn, Estonia.

Mendivil-López, R. (2010). Secreto 1910. México: Grijalbo.

Mendivil-López, R. (2012). Secreto 1929. México: Grijalbo.

Mendivil-López, R. (2014). Secreto R. Conspiración 2014. México: Grijalbo

Miller, C. (s.f.). How to build a cyber army to attack the U.S. DEFCON. [Edición en línea]. Recuperado el 10 de noviembre de 2015, de: https://www.defcon.org/images/defcon-18/dc-18-presentations/Miller/DEFCON-18-Miller-Cyberwar.pdf

Morgenthau, H. J. (1992). Colección estudios internacionales. Política entre las naciones: la lucha por el poder y la paz. Grupo Editor Latinoamericano. Buenos Aires. AR.

ONU. (s.f.). Oficina de Asuntos de Desarme de las Naciones Unidas. [Edición digital]. Recuperado el 15 de noviembre de 2015, de http://www.un.org/es/disarmament/

Orton, M. (14 de enero de 2009). Air Force remains committed to unmanned aircraft systems. U.S. Air Force. [Edición en línea]. Recuperado el 10 de noviembre de 2015, de: U.S. Air Force Web site: www.af.mil

Panda Security. (s.f.). Virus, gusanos, troyanos y backdoors. Panda Security. [Edición en línea]. Recuperado el 15 de noviembre de 2015, de http://www.pandasecurity.com/mexico/homeusers/security-info/about-malware/general-concepts/concept-2.htm

Rid, T. (2012). Cyber war will not take place. Journal of Strategic Studies, 35(1), 5-32.

Rid, T., & McBurney, P. (2012). Cyber-weapons. the RUSI Journal, 157(1), 6-13.

Sampaio, F. (2001). Ciberguerra: guerra electrónica e informacional, um novo desafio estratégico. Organização para Estudos Científicos (OEC). Escola Superior de Geopolítica e Estratégia. Porto Alegre. 2001.

Sun Tzu. (2008). El Arte de la Guerra. México: Grupo Editorial Tomo.

Sysmantec. (2014). Internet-Security-Threat-Report 2014. Sysmantec. [Edición digital]. Recuperado el 10 de noviembre de 2015, de http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v19_21291018.en-us.pdf

Sysmantec. (2015). Internet-Security-Threat-Report-Volume-20-2015. Sysmantec. [Edición digital]. Recuperado el 10 de noviembre de 2015, de https://www4.symantec.com/mktginfo/whitepaper/ISTR/21347932_GA-internet-security-threat-report-volume-20-2015-social_v2.pdf

Toffler, A. (1970). Future Shock. EE.UU.: Bantam House.

Trias, E. D., & Bell B. M. (2010). Cyber this, cyber that… so what?. Air & Space Power Journal, 24(1), 90–100).

Truman, S. H. (1963). Limit CIA Role To Intelligence. The Washington Post. [Edición digital]. Recuperado el 10 de noviembre de 2015, de http://www.maebrussell.com/Prouty/Harry%20Truman%27s%20CIA%20article.html

US Department of Defense (DoD). (2010). Department of Defense Dictionary of Military and Associated Terms. Department of Defense. [Versión electrónica]. Recuperado el 31 de enero de 2015, de http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf

Van Evera, S. (1999). Causes of war: Power and the roots of conflict. Cornell University Press.

Von Clausewitz, C. (2005). De la guerra. La Esfera de los Libros.

William J. Lynn III. (2010). "Defending a New Domain: The Pentagon's Cyberstrategy", in Foreign Affairs, 2010, pp. 97–108; Economist, "The threat from the internet: Cyberwar", 2010, [Edición digital]. Recuperado el 10 de noviembre de 2015, de http://www.economist.com/node/16481504?story_id=16481504