# Ejercicio del ciberpoder en el ciberespacio*

## Exercício Cyberpower no ciberespaço**

## Cyberpower Exercise in Cyberspace***

Luis Eduardo Chávez[a] y Santiago Velásquez Tovar[b]
Escuela Superior de Guerra. Bogotá, Colombia

**CIENCIA Y PODER AÉREO**
ISSN 1909-7050 / E- ISSN 2389-9468 / Volumen 12/ Enero-Diciembre de 2017/ Colombia/ Pp. 236-244
Recibido: 21/11/2016
Aprobado: 02/03/2017
Doi: http://dx.doi.org/10.18667/cienciaypoderaereo.575

**Para citar este artículo:**
Chávez, L., & Velásquez, S. (2016). Ejercicio del ciberpoder en el ciberespacio. *Ciencia y Poder Aéreo*, *12*, 236-244. Doi: http://dx.doi.org/10.18667/cienciaypoderaereo.575

---

[1] *Artículo científico resultado de un proyecto de investiagación llevado a cabo por el Griupo de Masa Crtítica de la Escuela Superor de Guerra.*

[2] *Artigo científico resultado de um projeto de investigação conduzido a cabo pelo Griupo de Masa Crtítica da Escola Superor de Guerra.*

[3] *Scientific article as a result of a research project carried out by the Crítica Mass of the Superor War School.*

[a] Coronel de Infantería de Armada de Colombia de la reserva activa, Abogado de la Universidad la Gran Colombia, Especialista en Derecho Marítimo de la Universidad Externado de Colombia. Profesional en Ciencias Navales de la Escuela Naval de Cadetes "Almirante Padilla"y especialista en Estado Mayor de la Escuela Superior de Guerra. Magister en Derecho Internacional Público, relaciones exteriores e Internacionales, del Campus Stellae- España. Correo electrónico: lechp8@gmail.com

[b] Politólogo internacionalista, con énfasis en seguridad y defensa de la Universidad Militar Nueva Granada (UMNG), Escuela superior de guerra. Coordinador diplomados UMNG. Bogotá, Colombia. Correo electrónico: santiagovelasqueztovar@hotmail.com

**Resumen:** en la actualidad, la tecnología avanza más rápido de lo que podemos imaginar. Prueba de ello es que cada factor de la vida humana se encuentra en el ciberespacio en una base de datos correspondiente a temas políticos, militares, seguridad, económicos, sociales y hasta personales.
La información es la materia prima que se utiliza en el ciberespacio; además, es una valiosa herramienta para satisfacer cualquier tipo de interés, lo mismo que lograr ciberpoder. Con esta nueva forma de aplicar el poder, se puede conseguir la información necesaria para cumplir cualquier interés y hacer cumplir una voluntad. En los últimos años, la seguridad y defensa de los estados han logrado grandes avances en tecnología para ejercer su voluntad de manera más eficiente, mediante el ciberpoder.
Sin embargo, de la misma manera como el ciberpoder se puede ejercer según una voluntad, un gran número de actores lo puede ejercer para su propia conveniencia en un área determinada como el ciber espacio. Las nuevas amenazas son inevitables y por ello estar preparados en este campo multidimensional es una obligación para evitar la vulnerabilidad y consecuencias que pueden originarse debido a un ataque realizado desde el ciberespacio.

**Palabras clave:** ciberpoder, ciberespacio, ciberseguridad, información, multidimensional

**Resumo:** Hoje, a tecnologia está avançando mais rápido do que podemos imaginar, ea prova é que todos os fatores da vida humana reside no ciberespaço em um banco de dados para, militar, segurança, questões políticas económicas, sociais e dados mesmo pessoal.
A informação é a matéria-prima utilizada no ciberespaço, e também é uma ferramenta valiosa para satisfazer qualquer interesse, bem como alcançar cyberpower. Com esta nova forma de aplicar o poder, você pode obter as informações necessárias para satisfazer qualquer interesse e fazer cumprir a vontade.
No entanto, da mesma forma como o cyberpower pode ser exercida de acordo com uma vontade, um grande número de jogadores que você pode exercer para sua própria conveniência. Por esta razão, novas ameaças são inevitáveis e estar preparado neste campo multidimensional, é a obrigação de evitar a vulnerabilidade e as consequências que podem surgir devido a um ataque do ciberespaço.
Nos últimos anos, a segurança e defesa dos Estados têm feito grandes progressos na tecnologia de exercer a sua vontade de forma mais eficiente, por cyberpower.

**Palavras-chave:** Ciberpoder, Ciberespaço, Cibersegurança, Informação, Multidimensional

**Abstract:** Nowadays technology moves faster than it can be imagined. Evidence of such is that every factor of human life is in cyberspace in a database showing on political, military, security, economic, social and (even) personal affairs.
Information is the raw material used in cyberspace, and it is also a valuable instrument for satisfying any interest, as well as to achieve cyber power. With this new way of applying power, needed information can be obtained in order to fulfil any request and enforce a will. In the last years, security and defense of the states have made great advances in technology to exert their will more efficiently by means of cyber-power.
However, in the same way as cyber power can be exerted in accordance with a will, a great number of actors may exert it for their own sake in cyberspace. New threats are inevitable, thus being prepared in this multidimensional field is an obligation in order to avoid vulnerability and consequences that may arise due to an attack from cyberspace.

**Key Words:** Cyber power, Cyberspace, Cyber Security, Information, Multidimensional Spectrum

## Reflexión sobre cómo se ejerce el ciberpoder en el ciberespacio.

> Así como en el siglo XIX tuvimos que consolidar la presencia en los mares para nuestra seguridad nacional y prosperidad, y en el siglo XX tuvimos que consolidar el aire, en el siglo XXI tendremos que garantizar nuestra superioridad en el ciberespacio.
> Oficina de Ciberseguridad del Reino Unido

El Departamento de Estado de los Estados Unidos ha reconocido que la tripulación del destructor estadounidense Donald Cook quedó seriamente desmoralizada tras su encuentro con el avión de combate ruso Su-24, que no transportaba bombas ni misiles, sino únicamente un contenedor con un sistema de guerra electrónica. Algunos medios de comunicación aseguraron que 27 marineros estadounidenses solicitaron la baja del servicio. Bajo su fuselaje, había tan solo un contenedor con un sistema de guerra electrónica llamado ***Jibiny*** (Valaguin, 2014).

Desde estos hechos recientes y su desarrollo, es necesario conocer la amplitud del tema del ciberpoder, pues incluye una serie de elementos que inciden en el comportamiento y liderazgo de las naciones y que salen de sus límites tradicionales territoriales y naturales, enmarcados en un área bien sea terrestre, marítima o aérea.

Luke (2003) sostiene que en la actualidad se viven épocas de cambios de poder. El mundo de las corrientes materiales ha sido sustituido y las fronteras ya no son líneas imaginarias sino electrónicas, en especial digitales, las cuales se desplazan en el ciber-espacio, donde hay una nueva forma de ver la geopolítica en un mundo marcado por las TIC.

Según la Real Academia Española, el poder implica tener expedita la facultad o potencia de hacer algo, la cual da la capacidad para influenciar el comportamiento de otros así como de obtener los resultados que se desea para cumplir con cualquier interés que se tenga en un determinado momento, ya sea desde la óptica estatal, empresarial o personal.

Bobbio define el poder como "la capacidad de una persona de influir, condicionar y determinar el comportamiento de otro individuo" (Bobbio, 1982. Pp 135). Ello da a entender que el poder es también la capacidad de influencia. Asimismo, explica que el poder puede ser invisible, como lo es en la informática, y que conforme avance podrá ser ejercido con mejores resultados, es decir, cumpliendo más con los objetivos deseados.

Para Joseph Nye, teórico de las relaciones internacionales, el poder se divide ***en hard power*** y ***soft power***[1]. El primero puede verse como el método que se utiliza para conseguir intereses mediante las fuerzas militares, mientras que el segundo es el método para incidir en las acciones o intereses de otros actores a través de medios culturales, ideológicos y diplomáticos (Nye, 1990)[2].

La unión entre ***hard power*** y ***soft power*** da como resultado el ***smart power*** o poder inteligente, el cual puede definirse como **"**una aproximación que destaca la necesidad de una armada fuerte y organizada, así como también el establecimiento de todo tipo de alianzas y de asociaciones, tanto entre países como entre instituciones, y a todos los niveles"[3]**.**

Con el poder inteligente, puede detallarse la capacidad de manejar y controlar el ciberespacio. El principal interés que se advierte en él es la información estatal, personal, económica o social, entre otras, de quienes la ponen a disposición. Lo importante es tenerla para tener poder y generar ventajas determinantes que ayuden a cumplir con mayor facilidad cualquier tipo de objetivo. De esa manera, el ejercicio del poder sobre el ciberespecio es la evaluación y definición del uso de la información para lograr ejercer dominación en el mismo.

Al respecto, el Gobierno colombiano ha definido la ciberdefensa como la "Capacidad del Estado para prevenir y contrarrestar toda amenaza o incidente de naturaleza cibernética que afecte la soberanía nacional" (CONPES, 2011, p 38)[4].

En este recorrido de significados, también es importante destacar que este último está constituido por dos palabras que componen un solo término, y una sin la otra carece de valor, toda vez que el significado se altera, si se considera separado en cada palabra. Por ciber (o cyber en inglés) se entiende "el espacio virtual que contiene todos los recursos de información y comunicación disponibles en la red"; y el poder significa "una capacidad para realizar algo".

De lo expuesto, es posible afirmar que el ciberpoder es la capacidad de utilizar el ciberespacio para crear ventajas e influenciar sobre eventos en todos los ámbitos operacionales con los instrumentos de poder. Además, es necesario establecer si el ciberespacio es un dominio como la tierra, el aire, el mar y el espacio, ello dentro del concepto geopolítico de estos términos.

1. Poder duro y poder blando respectivamente
2. Joseph Nye explica este concepto en su libro ***Bound to Lead: The Changing Nature of American Power***, y luego lo desarrolla en ***Soft Power: The Means to Success in World Politics***. El ***soft power*** fue popularizado por la candidata presidencial Hilary Clinton.
3. CSIS Commission on Smart Power: A Smarter, More Secure America.
4. Documento CONPES 3701/11

Antes de hablar sobre la creación de un plan estratégico de ciberseguridad, se dará a conocer la definición de ciberespacio de Kuehl quien dice que es un marco o dominio operacional en el cual el uso electrónico está y del espectro electromagnético son para crear, guardar, modificar, intercambiar, y desarrollar por medio interconexiones los sistemas de información de internet con sus infraestructuras asociadas.

Los actores del ciberespacio pueden agruparse en tres categorías: gobiernos, organizaciones altamente estructuradas y todas las personas bajo las redes, con una estructura muy débil. La característica que diferencia el mundo virtual del mundo real o físico es justamente su "no existencia", en tanto que en un momento dado existe una porción del ciberespacio y enseguida ha sido anulado, se ha volatilizado (Llongueras, 2011). Al obtener información en el ciberespacio se logra un ***ciberpoder***, pues el ciberespacio puede transformarse en un instrumento de información para el ejercicio del poder político, información, militar y económico.

Cada factor de la vida puede estar en alguna base de datos de tipo económico, social o personal, lo cual nos hace dependientes y además, vulnerables. Cualquier información pública o privada puede estar a disposición de quien la necesite o pague por ella. Por esta razón, la información debe protegerse y limitarse en cuanto a los alcances de las personas, instituciones o gobiernos que tengan acceso y control sobre ella.

En su tesis doctoral ***La ciberguerra: la guerra inexistente*** (2011), Llongueras sostiene que el ciberespacio habilita la capacidad y el poder a actores estatales, el cibercrimen organizado, los hackers y, en definitiva, a cualquier persona para ejercer una influencia en el ámbito político, bien sea en ***hard power*** o en ***soft power***, lo cual hasta hace poco años era de control exclusivo de los Estados.

Con su teoría del poder aéreo, Douhet demostró que se podía conseguir la victoria al utilizar el poder aéreo en un conflicto por medio de la fuerza aérea y dirigir ataques con un potencial destructor al corazón del adversario, con el propósito de impedir la capacidad de lucha. Para cuando Douhet divulgó su teoría, los conflictos se solucionaban por acciones militares en tierra y agua, puesto que la fuerza aérea –hasta ese momento– se mostraba como un nuevo actor en los conflictos armados. Al incluir el poder aéreo, los conflictos pasaron a desarrollarse en una nueva dimensión y en un nuevo campo en el cual se ejerce el poder, ampliando en esta forma el conocimiento, las capacidades y la dinámica de un efecto que se constituyó en la germinación de la ampliación del tema del poder y que cambia el plano de acción hacia el futuro. Con el desarrollo de nuevos espacios, se tendrá que buscar la forma de mantener el control del mismo.

El ciberespacio ha implicado una drástica reducción del diferencial de poder entre los actores estatales y no estatales, siendo ésta una completa aplicación del poder dentro de la visión neoliberal de las relaciones internacionales[5]. Cuando hablamos de información en una base de datos entramos en terrenos del ciberespacio, donde el mundo real está representado en una realidad digital, con libre interpretación y manipulación[6]. Además, la seguridad y la defensa adquieren nuevas dimensiones en una plataforma digital al crear un campo multidimensional. En otras palabras, son diferentes áreas de acción que amplían el contexto habitual limitado, por lo general, por ambientes geográficos y pasando a ambientes virtuales en los cuales las ciberguerras[7] ya se entienden como una realidad virtual, y donde obtener información es el factor más importante y el de la victoria.

La Declaración de Seguridad de las Américas (2003) ha hecho una recopilación de las amenazas tradicionales[8]y las nuevas amenazas[9] de seguridad para los Estados. Dicha recopilación muestra el alcance multidimensional de las amenazas actuales y a su vez, revela los desafíos de la seguridad de los mismos[10] y la vulnerabilidad que deben manejar ante una inseguridad preparada para aprovechar cualquier debilitad. En el evento de que la seguridad sea multidimensional, la inseguridad o las amenazas también lo son de igual manera, por lo cual es necesario estar preparados para dar respuesta a estos eventos.

La informática abarca muchos factores de la realidad física. Los ordenadores están conectados a internet y entre ellos, por lo que cualquier persona puede causar graves daños a otros millones con solo enviar un virus o un ataque contra determinadas estructuras estratégicas de los países. La sociedad es totalmente dependiente de estas tecnologías y de la electricidad: en las empresas, los aeropuertos, los hospitales, los transportes, los bancos o el Estado mismo y sus diferentes dependencias, entre otros (Llongueras, 2011). Esa dependencia genera asimetrías en las relaciones del ejercicio de las capacidades ante las diferentes amena-

5. El neoliberalismo es un sistema reformas económicas que incluye a algunos estados para que no se excluyan en su proceso de acoplamiento al mundo globalizado (Banco de la República, Colombia).
6. El ciberespacio se puede manipular según las capacidades que se tengan para realizar esta acción, es decir, con mayor capacidad y conocimiento de este espacio se logra mayor manipulación del mismo.
7. Ciberguerra es una acción perpetrada por un actor estadual en contra de una computadora o red informática con el propósito de neutralizar la red enemiga (Clarke, 2010).
8. Como conflicto armado, narcotráfico, trata de personas, corrupción, lavado de activos, catástrofes de la naturaleza.
9. Las que están relacionadas con ciberataques.
10. Principalmente de las amenazas de los Estados del continente Américano.

zas; por ello, se han elaborado diferentes protocolos para evitar ser blanco de las mismas.

El actor que logre obtener la información que necesite podrá usarla según su conveniencia: puede lograr el conocimiento necesario para desestabilizar la bolsa de valores de cualquier Estado y afectar su economía. Un hecho de este estilo se puede realizar con poderosos computadores y personal capacitado para operarlos (muy pocas personas son necesarias), generando un tipo de ciberincidente con daños importantes, como es el caso de fenómenos de especulación debido a los intereses que se tengan. Esta modalidad se caracteriza por utilizar diferentes formas de amenaza, siendo las más conocidas el espionaje, el sabotaje y el corte de suministro eléctrico a una población (Vásquez, 2012).

Con el fin de alcanzar el poder, los estados siempre han usado una serie de métodos para obtener la información necesaria: la diplomacia abierta, la diplomacia secreta, el espionaje, el chantaje, las guerras, entre otros (Ministerio de Defensa Colombia, 2009). En este sentido, el ciberespacio abre un nuevo campo para lograr el seguimiento, el control y el manejo de elementos de información de manera rápida y fácil para ser utilizados cuando un Estado u organización decida manipularlos, de acuerdo con sus intereses. De este espacio se puede obtener el máximo provecho, puesto que en él confían, no solo el Estado sino organizaciones y personas que hacen uso del mismo, potencializando su capacidad para ejecutar sabotajes por intermedio de la red y, sobre todo, poniendo a disposición en los archivos mucha información, procesos, técnicas y documentos de interés.

Como el factor más importante de este espacio es la información, ésta se constituye en ***el santo grial*** del ciberespacio y su consecución es la herramienta de proyección del poder. El diseño e implantación de una red mundial de ordenadores es uno de los grandes avances tecnológicos (D'Sousa, 1981), siendo una tarea constante, difícil y no imposible de conseguir. La información y su manejo son, entonces, el interés particular de cualquier usuario del espacio cibernético, y para lograrlos deben crearse métodos apropiados para vencer la defensa y superar la seguridad del sistema contrario. Se necesita una gran capacidad para realizar esta acción, e inclusive, se requiere de una mínima información para conseguir otra.

Saber emplear la información obtenida mostrará la capacidad de poder que puede ejercerse con ella. Puede servir o serle útil para un usuario que la convierta en pieza clave para ejercer poder o ciberpoder, y su utilización puede generar consecuencias para una persona, una empresa o un Estado, lo mismo que para la comunidad de naciones y sus diferentes organizaciones. Esta es la razón por la cual podemos hablar de un poder planetario, porque una determinada información puede afectar los diferentes aspectos del desarrollo político, social, económico y militar de los Estados en particular, y de distintas organizaciones.

La información es multidimensional y cuenta con influencia planetaria de distintos elementos. Por ello, es necesario que los Estados –como garantes de sus asociados– tengan elementos de protección adecuados contra este tipo de amenazas surgidas en el ciberespacio, con el fin de minimizar los posibles riesgos causados por acciones de control sobre la información.

La visión de la seguridad internacional en el siglo XXI se ha tornado más compleja y ambigua que en siglos anteriores debido a la invención y evolución de las tecnologías de la Información y Comunicación a las cuales la sociedad actual es dependiente (Llongueras, 2011). Desde la perspectiva multidimensional, en la cual la seguridad y la defensa son parte fundamental, el ciberespacio obliga a cada Estado a cuidar su infraestructura digital para proteger sus intereses e información, además de desarrollar métodos y programas encaminados a evitar el robo o daño de la misma. Cualquiera que sea la acción en contra de un Estado y que afecte su seguridad digital, puede afectar alguno de sus aspectos, bien sea político, económico, social, militar, etc., y puede traer efectos sobre su soberanía, su población, su territorio, su salubridad o su estabilidad, lo cual implica una amenaza latente contra su supervivencia y mantenimiento. A pesar de que en el mundo virtual es muy difícil identificar los cibercriminales y los ciberatacantes, es imprescindible entrenar personas en el uso de elementos apropiados para identificar las ciberamenazas y tener una capacidad efectiva en el área de la ciberdisuasión, aunque su efectividad puede quedar en entredicho en lo que se refiere a los ciberataques contra la infraestructura crítica de un Estado o de su información.

En su artículo ***Ataques destinados a páginas y portales web,*** Urrego sostiene que en los últimos años los Estados han sufrido múltiples ataques a su infraestructura digital, los cuales se pueden dividir en ataques contra las páginas y portales web, y los ataques contra los usuarios de Internet. Los principales medios de ataque que se presentan en el ciberespacio son: ***Cross Site Scripting*** (XSS)[11], fuerza bruta[12],

11. Se basa en insertar código o script en el sitio web de la víctima, y hacer que el visitante al ingresar en el sitio, lo ejecute y cumpla el cometido para el cual fue escrito, tal como robo de sesiones o datos vulnerables.

12. Se crean procesos automatizados al azar que, mediante prueba y error, logran llegar al usuario y su contraseña. Este ataque se puede dar en cualquier página que requiera anotar un *login* para ingresar, aunque hoy en día, son muchas las técnicas utilizadas para evitarlo.

inyección de código[13], denegación del servicio[14] y fuga de información[15]. Y los principales ataques contra los usuarios son: ***phishing*** (pesca de datos)[16], ***Spoofing***[17], ***Scam***[18] y Troyano[19], entre otros.

Teniendo en cuenta que quien realice las anteriores acciones logre alguna consecuencia y obtenga lo que desea, es evidente que existe muy poca preparación para proteger la información almacenada. Los ataques mencionados permiten realizar espionaje, robo (información, productos, dinero, divisas), sabotaje de servicios o terrorismo informático[20]. Es una acción tan simple que cualquier usuario puede realizarla y generar enormes daños, además de que el costo de la operación es mínimo.

El hombre le da vida al ciberespacio por medio de computadores y conexiones digitales. Dependiendo de la capacidad de las distintas maquinas que operan el ciberespacio, puede decirse que ejercen el ciberpoder. Claro está que los Estados que están a la vanguardia en tecnología son los más poderosos e industrializados[21].

De acuerdo con Sasharien, el listado de las Top500.org[22] muestra los Estados con mejores medios computacionales en capacidad para el año 2014, y da a conocer los que poseen súper computadoras. Ser propietario de cualquiera de estas computadoras da cierto control sobre el ciberespacio o una ventaja más para utilizar mejor este medio. La ventaja sería tener la capacidad de bloquear cualquier ataque que se realice en su contra, al generar un medio de control, haciéndolo físico en el mundo real con las supercomputadoras y digital con el control del ciberespacio.

China es uno de los Estados que tiene mayor inversión en ciberpoder. En la actualidad no posee el mayor número de computadoras poderosas, pero sí tiene las más poderosas[23]. El ranking de los países con mayor número de computadoras poderosas para controlar el ciberespacio lo lidera Estados Unidos con 252, le sigue China con 66, Japón con 30, Reino Unido con 29, Francia con 23 y Alemania con 19 (Fayerwayer, 2013).

El sistema Tianhe-2 de China ocupó el primer lugar por segundo año consecutivo con las supercomputadoras conocidas como ***High-Performance Computer*** (HPC); el segundo lugar lo ocupó el sistema estadounidense HPC Titan. Aunque en el mismo informe no se mencionan los rangos que alcanza a calcular la supercomputadora china, se sabe que duplica el rendimiento de la estadounidense. Todo el poder de la computadora china ha sido usado para llevar a cabo predicciones climáticas y manejar asuntos de defensa nacional (El Tiempo, 2013).

El mayor ciberataque que se ha registrado hasta el momento lo recibió Estonia en 2007. En efecto, el 7 de abril de 2007, al quitar la estatua del soldado de bronce del centro de Tallin, se presentó un problema con Rusia. El 17 de abril de ese año comenzó el ataque con el bloqueo de todas las páginas gubernamentales y de los partidos políticos de Estonia. Sus principales consecuencias fueron dejar a Estonia incomunicada al perder contacto internacional, el mal funcionamiento de los cajeros automáticos, y el colapso del sistema bancario y financiero (Ministerio de Defensa Nacional, 2009).

Entre el 17 de abril y el 19 de mayo, toda la red que conectaba a Estonia con el ciberespacio colapsó y la dejó fuera del mundo interconectado, con lo cual quedó como un Estado débil e indefenso, sin seguridad y sin ciberpoder. Aunque Estonia culpó a Rusia por este ciberataque, no ha podido demostrarse su procedencia. Finalmente, el 19 de mayo todo regresó a la normalidad (Sierra, 2014).

Estonia no es el único país que ha sufrido ciberataques. Las principales potencias del mundo como Estados Unidos y Alemania también han sido ciberatacadas. Es válido mencionar, entonces, algunos hechos ocasionados dentro del Estado, en organizaciones internacionales que ejecutan actividades de ciberataque y actores como ***hakers***[24] profesionales e informales. También incluiremos las medidas que se tomaron para enfrentarlos.

13. Este tipo de ataque inyecta código fuente como SQL, SSI, HTML al sitio web seleccionado, para cambiar su funcionalidad original o revelar datos que tenga almacenados en las bases de datos que utiliza.
14. El atacante aprovecha algún error en la programación del sitio web, y hace que el servidor utilice los recursos como procesador y memoria, hasta llegar al punto límite del mismo, y colapsar el servidor web al no dar más recursos. En consecuencia, logra sacar el sitio web del aire.
15. Es un error del administrador del sitio y consiste en dejar público el registro de errores, lo cual permite que al atacante, ver las fallas exactas del sistema, tomar provecho de ellas, y obtener el control parcial o total del sitio.
16. A través de diversos métodos, se intenta obtener los datos personales de la víctima. Una de las más conocidas es suplantar páginas web, creando un sitio similar al sitio original.
17. Este ataque consiste en suplantar la identidad de la máquina de una persona, mediante la sustitución de datos.
18. Es un método de engaño en el cual se ofrece dinero ficticio para generar una estafa a un usuario ingenuo.
19. Este ataque informático consiste en instalar programas espías dentro del computador afectado.
20. Ministerio de Defensa de Colombia.
21. Alemania, Canadá, Estados Unidos, Francia, Italia, Japón, Reino Unido y Rusia (países miembros del G7 y Rusia).
22. Sasharien es un ranking de las 500 supercomputadoras más poderosas del Mundo y se publica y revisa en el portal www.top500.org
23. ***Los 500 supercomputadores más poderosos del mundo*** es una relación hecha por la organización Top500.org que existe desde 1993. Las posiciones responden al número de cálculos que cada supercomputador es capaz de llevar a cabo por minuto. Un PC promedio realiza cerca de 100 millones de operaciones por segundo. La Tianhe-2 logra 33.860 mil millones en el mismo lapso (Top500.org).
24. Término para designar a alguien con talento, conocimiento e inteligencia que se relaciona conlas operaciones de computadores, redes y seguridad.

***Anonymous*** es una organización internacional de grupos e individuos que protestan a favor de la libertad de expresión en la red. Puesto que es una organización informal y carente de jerarquía, es casi imposible saber la veracidad de sus noticias y hechos que comentan; sin embargo, las acciones realizadas por este grupo sí son reales y han hecho que esta organización se haya convertido en un actor relevante en el ciberespacio. Inclusive, han logrado que parte de su lema[25] se aplique en el ciberespacio, es decir, sean temidos por sus acciones (Berrio, 2012).

Las principales acciones de ***Anonymous*** han sido en contra de los Estados que han impulsado o creado leyes en contra de la libertad de expresión y el libre manejo de internet. Sus ataques se han hecho en todas partes del mundo, con un sinfín de ***hakers*** que han atacado a países como Estados Unidos, Argentina, Colombia, España y México. Sus principales acciones en contra de estos países han sido bloquear sus páginas web gubernamentales para dejarlas sin funcionamiento, así como poner imágenes de la organización para impedir su acceso. También han atacado a empresas como Sony y la Iglesia de la Cienciología, y a celebridades como Gene Simmons.

Por su parte, China ha hecho robos de información a Corea del Norte, Australia, Alemania y Reino Unido. Ha logrado estos ataques por medio de sus supercomputadoras y de agentes civiles y militares entrenados para ejecutar estas acciones en el ciberespacio. Con todo, China nunca ha dado una explicación sobre la razón que tuvo para realizar estas acciones. Además, creó una red con una capacidad ofensiva óptima, y una red defensiva casi impenetrable que protege sus páginas gubernamentales y sus sistemas informáticos (Alfonso, 2015).

Corea del Norte y Corea del Sur tienen constantes enfrentamientos cibernéticos. Se dice que Corea del Norte lleva más de ocho años con una unidad de guerra cibernética especializada en hakear redes militares surcoreanas y estadounidenses. Corea del Sur posee defensas contra los ataques cibernéticos porque los sectores privados han creado fuertes mecanismos de defensa para defender el sector gubernamental y militar.

Por su parte, Estados Unidos creó el Centro de Ciber-comando Unificado que depende de la Agencia de Seguridad Nacional. Este centro optimiza los esfuerzos hechos por las Fuerzas Militares y otras agencias, y provee al país con la capacidad para defender la infraestructura tecnológica, además de conducir operaciones ofensivas (Department of Homeland Security, 2013).

Aunque Estados Unidos tenga supercomputadoras y agencias encargadas de la ciberseguridad, la nación no está totalmente segura frente a este tipo de ataques; ya sufrió la fuga de información más grande que se haya presentado por la acción de WikiLeaks[26], con un total de 1.2 millones de documentos de todo tipo de información estatal, dentro de los cuales se revelaron actos no éticos realizados por miembros de sus fuerzas militares en países como Irak. Además, se comprobó que los Estados Unidos hacían espionaje en sus distintas embajadas. Con este ciberataque, se divulgaron y desencriptaron 251.287 cables diplomáticos con información relevante y comprometedora (CNN, 2013).

Debido a esta fuga de información, los Estados Unidos tuvieron que dar muchas explicaciones para no dañar sus relaciones internacionales con la comunidad internacional y evitar ser aislados o cuestionados por las actuaciones de su diplomacia.

A finales del año 2014, se realizó un ciberataque que involucró dos Estados y una empresa multinacional. Por medio de su espionaje cibernético, Corea del Norte descubrió y reveló que la empresa Sony Pictures estrenaría una película llamada ***The Interview*** que muestra de forma ridícula y cómica a Corea del Norte y su mandatario Kim Jun Un, lo cual representaba una amenaza directa contra los Estados Unidos por parte del gobierno de Corea del Norte, y causaría una tensión internacional. La respuesta de Sony fue retirar temporalmente la película y aplazar su estreno. Por su parte, Corea del Norte no hizo algún ataque contra los Estados Unidos, y el presidente Barack Obama acusó a Corea del Norte de cibervandalismo y a Sony de cometer un error al retirar la cinta. Con todo, la película se estrenó (Mullen, 2014).

El gobierno ruso también tomó medidas activas para evitar el ciberespionaje, y retrocedió varios años al pasado, desconectándose de cualquier red e inhabilitando los medios electrónicos. En Rusia, los documentos oficiales se hacen ahora en máquinas de escribir que, inclusive, se implementaron en su servicio de inteligencia bajo el control del Servicio Federal de Protección (Arreola, 2016).

Tener medios para defenderse de un ciberataque (tales como agencias de seguridad) debe hacer parte de la estrategia de un Estado y ser tema primordial de seguridad y defensa nacional, pues en la actualidad ningún Estado se encuentra a salvo de un ciberataque. Ante el incremento de las amenazas cibernéticas (en cualquiera de sus presen-

25. ***El conocimiento es libre. Somos Anónimos. Somos Legión. No perdonamos. No olvidamos. ¡Témannos!***

26. Organización mediática internacional sin ánimo de lucro que publica, a través de su sitio web, informes anónimos y documentos filtrados con contenido sensible en materia de interés público, preservando el anonimato de sus fuentes.

taciones) que estén en posición de amenazar la seguridad nacional de cualquier país, los gobiernos y fuerzas militares del mundo han empezado a considerar la ciberdefensa y la ciberseguridad como capacidades estratégicas prioritarias que deben fortalecerse (Ministerio de Defensa Colombia, 2009).

Cada día, las redes informáticas crecen más, y los factores económicos, políticos y sociales se mezclan con el ciberespacio, interconectándolo en una red global. La infraestructura del ciberespacio se amplía y se perfecciona, y las organizaciones y actores cibernéticos crecen y se fortalecen, lo cual aumenta los factores de riesgo para los Estados y para cualquier actor.

El ciberespacio se desarrolla conforme con la teoría realista que nos muestra un mundo sin normas, sin gobernantes y anárquico, donde cada quien actúa según su conveniencia. Así, en él cada quien actúa como quiere; para conseguir el ciberpoder, posee un sinfín de medios y recursos, tales como supercomputadoras, personas civiles o militares muy bien capacitadas para moverse en este mundo. Como sostiene el Teniente Coronel Kevin L. Parker, las fuerzas armadas deben continuar el desarrollo de capacidades para operar en el ciberespacio según las políticas que se desarrollen en él, claro está, aprovechando también todos los medios posibles(Parker, 2014).

Para prevenir, contener y disuadir un ataque informático que afecte la infraestructura crítica, el Estado debe ponerse a la vanguardia en tecnología de seguridad informática, tal como lo hacen todos los gobiernos conscientes de la amenaza (Díaz, 2014). Todos los estados deben salvaguardar su infraestructura informática que sustenta la economía, las redes de transporte, la energía, la salud, los sistemas de defensa como el monitoreo del espacio aéreo y el mar territorial, así como hidroeléctricas y acueductos.

Está claro que la reflexión alrededor del tema es muy variante debido a que la tecnología avanza velozmente. Además, el ciberespacio es un área que cambia de manera constante y como se ha indicado, quien mejor método tenga para usarlo tendrá la mejor preparación.

El ciberespecio es un lugar creado por el hombre donde se efectúan diversas operaciones de almacenamiento, procesamiento y desarrollo de capacidades. Su peculiaridad es que no está definido en un lugar geográfico y depende siempre del desarrollo del hombre por no poder reproducirse autónomamente, el cual en su interior requiere de una serie de elementos que requieren cuidados; de no hacerlos, podrían albergar vulnerabilidades que pueden permear la estructura organizacional o estatal.

Con el ciberpoder, el ciberespacio se vuelve un mundo con muchas alternativas y capacidades ilimitadas que dan una ventaja para conseguir los intereses deseados. Sin embargo, hay que saber usar la información obtenida con ciberpoder y darle el uso adecuado, es decir, saber explotar el recurso más importante del ciberespacio. De la información del ejercicio del control surgen elementos como la ciberseguridad, y organizaciones enteras para prevenir su mal uso por medio del ciberespionaje. Todas estas acciones son parte del ejercicio en el ciberespacio, por medio del ciberpoder, pues son cada vez más potentes y seguras las medidas para prevenir su acceso, aunque también cada vez más serán complejas y desarrolladas las formas para acceder a la información.

## Referencias


Actualidad RT. (2014). Vencer sin matar: las armas electromagnéticas de Rusia. [en línea] Recuperado de: http://actualidad.rt.com/actualidad/view/141707-armas-electromagneticas-rusia-guerra-radioelectronica

Alfonso, J. (2015). ***Ataques entre estados mediante Internet. Estudio de casos orientados por el Esquema Nacional de Seguridad***. Tesis no publicada. [en línea] Recuperado de: https://riunet.upv.es/bitstream/handle/10251/56042/Memoria.pdf?sequence=1

Arreola, J. (2016) Ciberseguridad (casi) a prueba del enemigo 'invisible'. ***Revista Forbes México.*** [en línea] Recuperado de: https://www.forbes.com.mx/ciberseguridad-casi-prueba-del-enemigo-invisible/#gs.cSeDvT4

Armitage, R.; Nye, J. (2007). ***CSIS Commission On Smart Power***. Washington, D.C.: The CSIS Press.

Berrio, L. (2012). ***El Hacking Ético y los Grupos Hackitivistas Anonymous y Lulzsec***. [en línea] Recuperado de: http://www.ds-teamseguridad.com/archivos/hackconf/Anonympus_Remington.pdf

Bobbio, N.; Matteucci, N (1982). ***Diccionario de ciencia política***. Editorial Siglo XXI: Madrid.

Department of Homeland Security. (2013). National Security Cyberspace. Washington D.C. Recuperado de: https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf.

Gazeta, Rossiyskaya. (2014). Cultura/Technologias: Russia Beyond The Headlines. Recuperado el 12 de 02 de 2015, de sitio Web Russia Beyond The Headlines: https://es.rbth.com/cultura/2014/06/04/solzhenitsyn_previo_los_acontecimientos_de_ucrania_40621

Libicki, M. C. (2009). ***Cyberdeterrence And Cyberwar***. Washington D.C.: Library of Congress.

Mullen, J. (2014). Corea del Norte y Sony: se intensifica la guerra de palabras. ***CNN en Español.*** [en línea] Recuperado de:

http://cnnespanol.cnn.com/2014/12/22/corea-del-norte-y-sony-se-intensifica-la-guerra-de-palabras/

Palacios, R. (2009). ¿Se están utilizando ya armas psicotrónicas? ***Discovery Dsalud***. [en línea] Recuperado de: https://www.dsalud.com/reportaje/se-estan-utilizando-ya-armas-psicotronicas/

Parker, K. L. (2014). El uso del ciberpoder. ***Military Review***. 69(3) pp. 50-59. [en línea] Recuperado de: https://view.joomag.com/military-review-edici%C3%B3n-hispano-americana-mayo-agosto-2014/0905477001410196776?page=59

Toro Ibacache, L. (2009). El Enfoque Multidimensional De La Seguridad Hemisférica: Una Revisión Al Discurso Hegemónico. ***Revista Estudios Latinoamericanos.*** 1(2) 80-91.

Vásquez, A. N. (2012). El terrorismo y el Derecho Internacional: Los ciber ataques y la guerra justa1 en el marco del Derecho Internacional. Buenos Aires