De la era de la disuasión a la era del control

Andrés Gaitán Rodríguez

Los Estados, desde su construcción tras la Paz de Westfalia y su consolidación a finales del siglo XVIII, como principales actores del Sistema Internacional, se han mantenido en una búsqueda constante por los métodos más eficientes para la obtención de sus intereses nacionales, la adquisición y el mantenimiento del poder y conseguir su fin principal: la supervivencia como unidad (Barbé, 1987). Esta indagación ha llevado a los Estados a crear estrategias para actuar de forma que puedan mantener una posición privilegiada y un estadio de paz: "El deseo de poder, del que participan muchas naciones, cada una procurando mantener o destruir el statu quo, conduce por necesidad a la configuración de lo que se ha llamado el equilibrio del poder" (Morgenthau, 1963, p. 227).

Dentro de las labores para alcanzar sus objetivos, uno de los métodos más antiguos se encuentra la disuasión. Siendo la disuasión una de las principales estrategias de comportamiento entre Estados, a partir de la demostración de las capacidades propias en su afán de lograr sus metas, la actualidad presenta un gran reto para este concepto. Los recursos que tienen los Estados para perseguir sus fines se han visto enriquecidos gracias a los avances tecnológicos, lo cual les ha permitido encontrar nuevas formas de mantener la paz y el orden en el sistema internacional. El ciberespacio, como nuevo dominio, presenta un sinnúmero de ventajas, facilidades y oportunidades de acción para los Estados, convirtiéndolo en un escenario cada vez atractivo, pues el control que se puede tener sobre el adversario es un fenómeno nunca antes visto.

La intención del presente capítulo es analizar el concepto de disuasión dentro de un momento histórico sin precedentes, en el cual, a partir del manejo del ciberespacio, se despliega el control como estrategia dominante. Esto permitiría explicar si los cambios en el modo de operar exigen modificaciones dentro de la doctrina de la disuasión por ser un concepto anacrónico, o si la realidad que se presenta hoy solo es una adaptación de la disuasión a los fenómenos y los nuevos medios. Esto se llevará a cabo a partir de un recorrido histórico por el marco conceptual de la disuasión, un segundo momento reflejará cómo el ciberespacio ha construido un entorno de control y, en último lugar, una reflexión acerca del papel que desempeña la disuasión en el contexto contemporáneo.

La disuasión no es, en absoluto, un fenómeno novedoso. Las sociedades desde sus primeras y rudimentarias organizaciones, hasta la creación y la consolidación del Estado nación, como se conoce hoy día, han buscado, como unidad política, "manipular el comportamiento de sus oponentes a través de amenazas o el uso real de la fuerza" (Pardesi, 2005, p. 10), siendo siempre consientes acerca de las consecuencias que sus actos pueden tener sobre los demás actores. Michael Quinlan (2004) afirma que incluso los romanos eran conscientes de la importancia de influir sobre el otro, cuando se formuló el axioma latino: *Si vis pacem, para bellum* (Si quieres la paz, prepárate para la guerra).

En un intento por definir qué es disuasión, se encuentran múltiples autores dedicados a dicha misión. Para hacer una primera referencia, la Real Academia Española (s.f.) define el verbo disuadir como "inducir o mover a alguien a cambiar de opinión o a desistir de un propósito". Desde una perspectiva más militar, en el *Diccionario Militar, Aeronáutico, Naval y Terrestre* se define la disuasión como la:

> Acción y efecto de disuadir, inducción al desistimiento; convencimiento negativo; cuyo concepto central, por su parte, es descrito como: inducir, convencer a otro para que cambie de opinión o desista de un empeño. No ha de intervenir la amenaza ni la fuerza, sino exclusivamente la persuasión o el razonamiento. Su valoración depende de los fines; ya que cabe disuadir de un crimen, de la deserción, de una guerra, así como de un arranque heroico por

> el recuerdo del sacrifico o de los sufrimientos familiares ulteriores. (Caballenas de Torres, 1961, p. 601)

Continuando un recorrido conceptual, André Beaufre (1966), uno de los principales autores que han hecho referencia al concepto de disuasión, afirma que esta pretende impedir que una potencia adversaria tome la decisión de emplear las armas o que reacciones ante una situación específica, mediante la existencia de un conjunto de disposiciones que constituyan una amenaza suficiente. Para este autor, la disuasión solo pretende alcanzar un efecto sicológico sobre los tomadores de decisiones.

Durante la década de los setenta, la definición que predomina es aquella que afirmó que es:

> El intento de reestructurar el conjunto de opciones que se ofrecen a los dirigentes de un país o grupo de países, llevado a cabo por los dirigentes de otra nación o grupo de naciones, mediante la formulación de una amenaza a sus valores fundamentales. Mediante esa reestructuración se pretende excluir la consideración de la agresión armada. (Brody, 1974, p. 775)

Otros autores que han definido la disuasión han aportado nuevos elementos. Collins (1980) afirma que esta se basa en una estrategia para la paz y no para la guerra e intenta transmitir un mensaje cuya pretensión es convencer al oponente de que cualquier agresión es la menos beneficiosa de las alternativas. En el *Diccionario Militar, Estratégico y Político*, la disuasión es la "acción psicológica, política, militar o moral, capaz de obligar al adversario a renunciar a una agresión o ataque, por el peligro que ello puede suponerle" (De Bordeje Marencos, 1981, p. 51). Por último, Hamon (1996) afirma que la disuasión es semejante al arte de la persuasión: "Para vencer la resistencia de un individuo o de un pueblo hay que suscitar en su espíritu, a la vez, el temor de ser destruido y la esperanza de obtener ventaja" (p. 67).

Como concepto, es importante hacer una claridad y esta se refiere a que al ser un término mayormente usado en textos académicos en el idioma nativo de los Estados Unidos, se debe diferenciar entre *deterrence* y *dissuassion:* "Como concepto estratégico el término *dissuassion* es impreciso, significa persuadir a otras potencias de abstenerse

de iniciar una carrera armamentista o una competencia de capacidades militares, mientras que *deterrence* significa convencer a otros de no emplear capacidades que ya posee" (Yost, 2005, p. 2). Esta precisión es importante porque las capacidades serán un factor determinante para el auge y el aparente declive del concepto de disuasión durante los últimos 50 años.

Entre las principales características de la disuasión Kepa Sodupe (1991) reconoce tres básicas. En primer lugar, que esta se refiere a situaciones de conflicto, es decir, cuando las partes tienen intereses antagónicos; en segundo lugar, los únicos protagonistas que pueden participar en una relación disuasoria son los Estados. Por último, el tipo de amenaza que tiene la disuasión como esencia está asociado al uso de la fuerza.

Las definiciones mencionadas con anterioridad simplifican un concepto que, en realidad, no puede ser sintetizado de esta forma, es decir, las definiciones se encargan de mostrar el objetivo que pretende cumplir un Estado al usar la disuasión. Pero el fenómeno de esta doctrina va mucho más allá, pues ha cambiado con el paso del tiempo, ha explicado de forma clara fenómenos importantes de la historia y ha intentado adaptarse a otros momentos. Por esta razón, la revisión académica debe ser mucho más profunda y eso se hará a continuación.

El momento de mayor relevancia para el concepto de la disuasión y su aplicación como estrategia de los Estados se dio durante la Guerra Fría que se convirtió en el centro del pensamiento estratégico con el advenimiento de la era nuclear (Pardesi, 2005). A partir de su desarrollo, la doctrina más importante de la disuasión es la nuclear, la cual determinó el comportamiento político y el discurso estratégico de la época.

El concepto de disuasión nuclear fue presentado por Bernard Brodie durante 1945. Su frase más famosa acerca del tema es: "Hasta ahora, el principal objetivo de nuestra institución militar ha sido ganar guerras. A partir de ahora su principal objetivo debe ser evitarlas" (Brodie, 1945). Para Robert Oppenheimer: "El hombre no tomó las armas atómicas para hacer la paz. Pero la bomba atómica fue el punto de quiebre. Hizo que la perspectiva de una guerra sea insoportable" (Oppenheimer, 1946, p. 714).

La disuasión nuclear puede ser definida de forma estricta como "una estrategia de las naciones que poseen arsenales nucleares importantes para influir en el comportamiento de otras naciones que, por lo general también poseen arsenales nucleares" (Johnson, 1998, p. 2). En otras palabras, se encarga de establecer incentivos para que otras naciones no participen en ciertos tipos de acciones militares, específicamente, en no iniciar una guerra nuclear. Es importante resaltar que este tipo de disuasión es exclusivo de aquellos Estados con recursos nucleares, es decir, para esta época, solo función entre la Unión Soviética y los Estados Unidos (Clarke, Gearson y Shaud, 2010).

La disuasión nuclear ofreció un poder mucho más concreto a partir de una estrategia, ya que estaba basada en "la creencia que las armas nucleares son la mejor herramienta de disuasión para proteger integridad de un país a través del uso o la amenaza de un ataque nuclear" (Rajmil, 2015, p. 11); y es claro porqué funcionó, un Estado no podría acarrear con todos los gastos que puede generar una guerra nuclear. Además, el momento de la Guerra Fría ofreció todas las condiciones para una disuasión nuclear funcional entre los dos bandos: el alcance del daño superaría cualquier capacidad de reacción, ninguno podría evitar una represalia y además era probable que con un solo ataque, el otro actor fuera eliminado por completo. Por lo tanto, la interpretación que queda es que la disuasión nuclear hizo una notable contribución a la paz durante el periodo de posguerra (Ford, 2013).

Pero no todos los autores que han tratado este tema están de acuerdo. Para MccGwire (2006), durante la Guerra Fría, "el dogma disuasión nuclear no era responsable de la prevención de la guerra" (p. 780). El autor asegura que los costos que tuvieron que asumir los Estados Unidos y la Unión Soviética fueron mucho mayores que los beneficios que se podrían haber obtenido, especialmente desde la perspectiva de la Unión Soviética, independientemente de la amenaza de represalia nuclear.

Es un hecho que la Guerra Fría terminó y la amenaza nuclear dejó de ser el factor de tensión, por lo tanto, la disuasión, como concepto, se vio en la obligación de intentar mantenerse a flote y no quedarse en ese periodo: "La doctrina de la disuasión nuclear ya no es adecuada dentro de un mundo en evolución en el siglo XXI" (Quilés, 2013,

p. 8). Por esto, los tratadistas se han encargado de adaptarla a otros momentos históricos, redefinirla para convertirla en un concepto más amplio y generar un número importante de características y clasificaciones, con el objetivo de no dejarla atrás. El Departamento de Defensa ha definido la disuasión como "la prevención de la acción por miedo a las consecuencias. La disuasión es un estado mental provocado por la existencia de una amenaza creíble de acción contraria inaceptable" (Departamento de Defensa, 2015, p. 67).

T.V. Paul (2009) expone que la disuasión, la cual él denomina clásica, se logra cuando "un atacante potencial, por temor a un castigo inaceptable o denegación de la victoria, decide renunciar a una ofensiva planeada" (p. 2); y a su vez, explica que para que la disuasión tenga éxito, debe cumplir con tres premisas fundamentales: El disuasor debe tener las capacidades suficientes, su amenaza debe ser creíble y debe ser capaz de comunicar esa amenaza a su oponente (Paul, 2009). Lo que T.V. Paul denomina disuasión clásica, otros autores la llaman convencional, esta entendida como "una política de Estado que implica una capacidad real, en términos de poder nacional y una voluntad política que la hagan creíble" (Bustos Carrasco y Rodríguez Marcos, 2004, p. 12).

Este tipo de disuasión debe tener la capacidad física para infligir el daño, mostrar el poderío y ser creíble (García Covarrubias, 2001); además, en ella como deben participar todos los elementos del poder nacional para hacerla una estrategia que genere un impacto sustancial, de forma preponderante se encuentra el poder militar y la voluntad política, para lograr una mayor convicción de que los costos de actuar superaran los beneficios de mantenerse en el *statu quo* (Alvayay, 2013).

Rafael Calduch (1991) propone un acercamiento teórico más estructurado a partir de la construcción de una ecuación. El autor afirma que el "EFECTO DlSUASOR = Capacidad Estimada X Intención Estimada X Daño Estimado" (p. 21). Donde el efecto disuasorio es directamente proporcional a la capacidad de ejecución de la amenaza, la intención de ejecución de dicha amenaza y el perjuicio que puede llegar a causar; y el punto más relevante que propone el autor, es que si alguna de las tres variables, sin importar cuál, se cuantifica en cero, toda la estrategia disuasiva desaparece. Además, como características adicionales, el proceso de disuasión debe contar con racionalidad,

suponiendo que cada actor debe ser altamente adverso al riesgo y con una estructura de fuerza que le permita al adversario sobrevivir a cualquier ataque o represalia (Howlett, 2002).

Además de las características, los teóricos se han dedicado a clasificar la disuasión según algunos criterios. Se ha clasificado por tipo de acción, épocas, beneficiario, iniciativa y uso de la fuerza. La primera condición se divide entre disuasión defensiva, que trata de evitar una acción del adversario que resulte perjudicial para el disuasor y la disuasión ofensiva que trata de evitar que el disuadido se oponga a una acción que el disuasor desea llevar a cabo (Caldush, 1991).

La disuasión por época hace la distinción entre disuasión clásica o racional y disuasión perfecta. La primera se enfoca en las relaciones entre Estados y los centros nucleares, y está fuertemente marcada por el realismo político, en el cual el Estado debe confiar su seguridad en sus capacidades propias y para mantener la armonía, se mantiene el *statu quo* (Kumar, 2007). Por otro lado, la disuasión perfecta, usando teoría de juegos, ofrece un nuevo enfoque:

> El punto central de la teoría de la disuasión perfecta radica en el trabajo de disuasión mutua, y la disuasión mutua funciona mejor cuando ambos jugadores son capaces de plantear amenazas creíbles. La capacidad de un jugador significa una habilidad de infringir daño y por lo tanto la capacidad se convierte en una condición necesaria para el éxito de la disuasión. La credibilidad de un jugador significa que una amenaza pueda ser racionalmente creída. Por lo tanto, es entendido que solo las amenazas racionales son creíbles. (Kumar, 2007, p. 245)

En tercer lugar, la disuasión que respecta al beneficiario se divide en dos: "Cuando el beneficiario de la disuasión resulta ser uno de los países que intervienen en la relación disuasora, nos encontraremos ante una disuasión directa, en cambio cuando se realiza en favor de un tercer país ajeno a la relación, la calificaremos de disuasión Indirecta" (Calduch, 1991, p. 23). Desde la perspectiva de la iniciativa del Estado que desea disuadir, se encuentran aquella que por negación pretende que el disuadido no actúe por temor a un daño mayor que los beneficios que espera obtener con esa acción; y la disuasión por castigo, en la cual el

disuadido no debe oponer resistencia por temor a una acción que le produciría más pérdidas que dicha resistencia (Mearsheimer, 1983).

Por último, haciendo referencia al empleo de la fuerza, se encuentra la disuasión total, cuando se afecta a todas modalidades de fuerzas posibles que pueden llegar a ser utilizadas por el adversario y la disuasión limitada, cuando solo se afecta a ciertos sectores dentro del uso de la fuerza (Calduch, 1991).

Está claro que se ha hecho un gran esfuerzo para poner de nuevo en contexto el concepto de disuasión, y si bien es innegable que aún tiene relevancia en los comportamientos estatales, la nueva realidad a la que se enfrenta el sistema internacional hace que la disuasión enfrente un escenario de muchas contradicciones y ya no sea tan efectiva y creíble. La concepción de disuasión, al no basarse en el poder nuclear, enfrenta uno de los problemas más graves y es que ya no es lo suficientemente inductora y su alcance ya no es global; por lo tanto, no será suficiente para disuadir al otro Estado de no actuar:

> Al respecto se ha desarrolla una visión que sostiene que los efectos de la disuasión convencional tienen un lapso de vida limitado […] Sin duda, esta afirmación tiende a explicar una falencia de este sistema disuasivo, que no ha logrado, *per se*, ser un elemento decantador de conflictos, a diferencia de las armas nucleares que actúan por su sola presencia, dejando de manifiesto su mayor vulnerabilidad en cuanto a instrumento al servicio de la paz. (Bustos Carrasco y Rodríguez Marcos, 2004, p. 33)

Por otro lado, desde el fin de la Guerra Fría y la desintegración de la Unión Soviética, el espectro de seguridad y la lista de amenazas han variado de forma significativa, pues han aparecido nuevos Estados con armas nucleares, han aumentado fenómenos como el terrorismo, el tráfico de armas, el aumento de peligros para el medio ambiente (Bergman y Ware, 2013), lo cual hace que el protagonismo de la disuasión por actuar en un escenario de tensión nuclear haya desaparecido:

> Las operaciones nucleares parecen menos relevantes en un mundo caracterizado por la diversidad de los desafíos tales como Estados fallidos, desastres humanitarios, conflictos genocidas, la

> proliferación de armas, el terrorismo y el conflicto asimétrico […] Los Estados que adoptan la disuasión como parte de una estrategia global deben ser capaces de determinar, con un grado razonable de certeza, que las políticas y las iniciativas destinadas a impedir un comportamiento realmente logren su objetivo. Aquí es donde el concepto de la disuasión en el siglo XXI comienza a descomponerse. (Lowter, 2010, p. 1)

Además, es indispensable hacer precisión sobre la acción por la cual se va a ejercer un efecto disuasivo, el adversario y el momento; la realidad actual refleja una ambigüedad sobre la amenaza, la dificultad para legitimar la estrategia de acción y para la identificación de los actores, además de la complejidad para los recursos que generen una capacidad física de proyección y ataques que sean creíbles (Alcolea Navarro, 2015). La disuasión como concepto perdió claridad luego del fin de la Guerra Fría, es decir, los conceptos que se han construido para adaptarse a las nuevas necesidades del siglo XXI la han convertido en un concepto maleable que se adecua a la situación que el tratadista quiera explicar; y es en este punto en que la disuasión pierde aún más su poder y hace su aparición el ciberespacio y la capacidad de control que este ofrece.

El ciberespacio pretende informatizar todos los aspectos que los Estados usan para funcionar, algunos de ellos son el sector defensa, económico y de infraestructura. El sector defensa, de seguridad y la parte militar son fortalecidos con celeridad, precisión y sigilo. Ahora es claro que casi todos los Estados tienen la capacidad de tecnificar y sistematizar sus procesos a través del entorno cibernético para hacerlos más fáciles y para ejercer un manejo que no exija grandes desplazamientos o una inversión innecesaria. Pero estos avances que pueden simplificar las formas de dirección de los Estados y sus gobernantes, también abren la puerta a condiciones que aumentaron las vulnerabilidades, lo que convierte sus componentes en estructuras críticas, con las cuales, si el adversario es capaz de controlar, puede atacar en cualquier momento y causar graves daños.

Definir el alcance que puede llegar a tener la estrategia de control a través del ciberespacio exige un estudio del entorno cibernético

como nuevo dominio, las acciones que se pueden llevar a cabo a través y gracias a él, los focos de acción y la demostración que ya se han realizado acciones las cuales han cumplido con el objetivo de la estrategia mencionada. El ciberespacio ha sido definido de muchas formas desde su primitiva aparición durante los años sesenta hasta hoy. Para la Casa Blanca (2003), el ciberespacio es "el sistema nervioso de las infraestructuras, el sistema de control de nuestro país. Comprende cientos de miles de ordenadores interconectados, servidores, enrutadores, conmutadores y cables de fibra óptica que hacen que nuestras infraestructuras críticas funcionen" (p. 1).

Por otro lado, el Estado Mayor de los Estados Unidos (2006) lo define como "un dominio que se caracteriza por el uso del espectro electrónico y electromagnético para almacenar, modificar e intercambiar información a través de los sistemas de información en red y las infraestructuras físicas" (p. 3). Según Gregory Rattray (2001), el ciberespacio es un dominio resultante de la creación de sistemas y redes que permiten interacciones electrónicas de información, es un entorno hecho por el hombre para la creación, la transmisión y el uso de la información en una variedad de formatos y se compone del equipo accionado electrónicamente, redes, sistemas operativos y las normas de transmisión.

Este nuevo escenario tiene un sinnúmero de características que lo diferencian de cualquier otro dominio que el hombre haya manejado alguna vez. Por una parte, solo es apreciable a los sentidos cuando se manejan los dispositivos electrónicos, pero no se puede percibir más allá de eso, por lo tanto, no se alcanza a distinguir su dimensión, posibilidad o peligro; además, es accesible desde cualquier lugar del mundo y por alguien que tenga conocimiento del tema (Stel, 2014). También, es un entorno de información, compuesto por los datos que se crean, se almacenan y se comparte; por ende, sus sistemas y tecnologías son artificiales. Si bien el ciberespacio es un entorno global, no puede ser denominado como *sin gobierno*, pues hace parte de cada Estado, que debe manejar todas las estructuras, tanto físicas como digitales que dan lugar al ciberespacio (Friedman y Singer, 2014); esta característica es la que va a permitir ejercer control del oponente, pues las estructuras del ciberespacio se vuelven componentes esenciales de los Estados,

abriendo la puerta para ejercer acciones que afecten directamente al Estado adversario.

Pero las características del ciberespacio no solo lo convierten en un escenario distinto, también lo hacen más atractivo para llevar a cabo acciones por parte de los Estados; esto debido a que es un dominio casi infinito y puede conectar todos los demás dominios; evoluciona a una velocidad sin precedentes, pues no necesita solo de nuevas tecnologías para avanzar, sino también pequeñas construcciones de carácter informático que permitan aumentar su capacidad de expansión. El ciberespacio convierte la información en el componente más valioso y es esta la que convierte a los Estados en actores vulnerables (López de Turizo y Sánchez, 2012).

El número de técnicas que se pueden aplicar en el ciberespacio para controlar al adversario es amplio, por todas las particularidades que este ofrece. En primer lugar, se puede hablar de la información y cómo se puede ver afectada. La guerra de información es definida como una "serie de medidas adoptadas con el fin de afectar a los sistemas de información y la información del adversario, mientras se logra la defensa de los sistemas de información y la información propios, para lograr objetivos específicos contra el rival" (Delibasis, 2007, p. 6). Es posible decir que este tipo de conflicto por la información ha existido siempre, pues quien tiene información tiene poder y puede controlar el comportamiento del adversario; el punto es que el mundo hoy es mucho más dependiente de la información (Jones, Kovacich y Luzwick, 2002, p. 5), y toda esa información se encuentra en un espacio que, con los recursos adecuados, un Estado puede manejar y obligar a otro a actuar de acuerdo con sus intereses.

"La guerra informática es un subconjunto de operaciones de información que se realizan con el fin de alterar la información y los sistemas de información del adversario, mientras se protege la información y los sistemas de información propios" (López, 2007, p. 219), es decir, pretenden hallar nueva información, alterar o destruir la información existente y transmitir esa información a su Estado para manejarla de forma que se pueda conocer y controlar el comportamiento y el funcionamiento del otro.

La guerra de información representa el despliegue de acciones en un nuevo entorno: "el diseño de bancos de datos y *software*, la capacidad de cegar las infraestructuras de información del oponente y la superioridad de las mismas de un Estado, son tan importantes como la superioridad de las armas y la fuerza militar" (Taddeo, 2012, p. 113); esto hace que cada vez sea más importante para los Estados dedicar e invertir en infraestructuras que protejan su información y permitan conseguir la de otros, así como mejorar sus capacidades.

Entre los principales objetivos de este tipo de acción en el ciberespacio se encuentran dañar o destruir los sistemas de información y comunicación del adversario, infiltrar, degradar o subvertir los sistemas de información y penetrar de forma silenciosa en los sistemas de información y comunicaciones del rival para cambiar las percepciones, dar forma a las opiniones y engañar (Crawford y Cronin, 1999, p. 258); así se consigue el control sobre el otro, no solo con la información que se puede obtener, sino también entregando información que los obligue a actuar de acuerdo con los intereses propios.

Existen dos tipos de técnicas: ofensivas y defensivas. Entre las ofensivas se encuentra "la manipulación de los sistemas electrónicos de información para influir en las percepciones y el comportamiento de un adversario" (Miller, 1997, p. 158); el engaño y la emisión de acciones que nieguen, exploten, dañen o destruyan los sistemas adversarios. Por otra parte, en cuanto a la cuestión defensiva, el objetivo es proteger los sistemas de información propios de cualquier alteración, daño o explotación por parte de un rival (Fredericks, 2007).

La estrategia de control mediante la guerra de la información ofrece varios rasgos que la caracterizan y además la hacen un método brillante para alcanzar sus objetivos. Tiene un bajo costo, pues exige preparación de los actores, pero su manutención no exige grandes inversiones como las armas tradicionales, las acciones pueden traspasar fronteras sin convertirse en un problema de invasión a otros Estados, se puede aumentar sustancialmente el poder del engaño y de las actividades de manipulación. Supera los métodos antiguos de recolección de información, se puede conseguir una gran cantidad a menores costos y a gran velocidad; al existir coaliciones entre Estados y pueden

tener una mayor cantidad de información que los hace vulnerables (Molander, Riddile y Wilson, 1996. p. XIV).

Otra forma que permite ejercer control por medio del manejo de la información es el espionaje mediante el ciberespacio. La información que se obtiene puede ir desde secretos de seguridad nacional hasta propiedad intelectual de entidades públicas y privadas (Cox, 2013); está ayuda a la construcción de datos que apoyen la inteligencia de los Estados, lo que genera una ventaja para quien la consigue, pues podría usarse en las tomas de decisiones, las operaciones tácticas y el control completo del campo de batalla y del adversario (Braganca, 2013).

Lo que esto refleja es que existe un cambio que les permite a los Estados controlar todo el escenario y las acciones que tienen previstas sus rivales: "La inteligencia es una forma de mejorar la comprensión de una situación […] crear un conocimiento preciso de las capacidades e intenciones de sus adversarios y aliados, y proporcionar una ventaja en la decisión respecto a los adversarios" (Braganca, 2013, p. 41). A partir de esta información, los Estados pueden obtener una visión que por ningún otro medio tendrían conocimiento y control en los planes, las operaciones, los avances tecnológicos, los secretos industriales y las vulnerabilidades del adversario.

> Espías cibernéticos robaron los datos de las empresas que trabajan en el avión Joint Strike Fighter F-35, que se basa en millones de líneas de código de software y es el programa de armas más caras en la historia de Estados Unidos. La propagación de códigos malisiosos pasó sin ser detectada y estuvo a punto de entregar los planes operativos a manos de un adversario desconocido. (Lord y Sharp, 2011, p. 17)

Las técnicas principales que se usan para conseguir la información siempre cuentan con una línea de acción de cuatro pasos que le otorga a quien usa el espionaje cibernético todas las ventajas para controlar el escenario. En primer lugar, se selecciona y se investiga el objetivo, es decir por qué es importante, qué ventajas puede traer conocer dicha información, qué dificultades se pueden presentar y las generalidades del otro actor. A continuación, se presenta la explotación y la infiltración, es decir, el uso del arma cibernética (un *malware* especializado,

agentes de campo, ingeniería social) y se lleva a cabo la toma de la información. En tercer lugar, se debe mantener el acceso por medio de la infraestructura de mando y control, así como la vigilancia de cualquier nueva información que pueda aparecer. Por último, se produce la extracción, es decir, el traspaso de la información del adversario a los sistemas de información propios (Baich, 2011). Queda claro que, si se hace de forma correcta, el control se consigue de un par de acciones que no requieren grandes esfuerzos ni movilizaciones.

Durante la última década, las industrias críticas, principalmente el sector comercial, financiero y milita de los Estados se han convertido en el blanco de las intrusiones de inteligencia extranjera (Baker, Ivanov y Waterman, 2010): "El espionaje industrial hecho por gobiernos como fuente de amenaza, está motivado por la ventaja competitiva, el espionaje económico o los secretos nacionales" (Pérez Cortés, 2012, p. 266). La creciente dependencia de los Estados y sus instituciones ha aumentado sustancialmente el riesgo de espionaje efectivo, debido a que los sistemas centrales están conectados al ciberespacio, y los datos que se encuentran allí son de gran importancia y sensibilidad (Waterfall, 2011):

> La información es poder, por lo que, cuando se roba información, el robo puede neutralizar cualquier ventaja que el propietario original de los datos tuviese. Esto se aplica si el objetivo es un Estado-nación, la celebración de secretos militares o un negocio con propiedad intelectual y secretos comerciales que les dan una ventaja competitiva. (Kaspersky, 2013, p. 7)

La cibernética y los avances tecnológicos no solo han permitido que el control se ejerza a través del ciberespacio; el uso de la tecnología para la creación de elementos físicos conectados al entorno cibernético se convierte en un recurso cada vez más popular para los Estados. Algunos de estas creaciones son los aviones no tripulados (conocidos coloquialmente como Drones) y las armas robóticas. Si bien el uso de las nuevas herramientas hace más fácil, productivo, seguro, veloz y eficaz el cumplimiento de los objetivos, también puede llegar a elevar los presupuestos que deben usar las instituciones estatales y la dependencia

de estar conectados al ciberespacio del Estado, lo hace más vulnerable (Grauer, 2013).

> Robots, edificios inteligentes, dispositivos médicos implantables, coches que se conducen solos o aviones que vuelan de forma automática en un espacio aéreo controlado son ejemplos de sistemas ciber-físicos. Hoy, los sistemas ciber-físicos pueden encontrarse en industrias tan diversas como la industria aeroespacial, automoción, energía, salud, manufactura, infraestructura, electrónica de consumo y comunicaciones. La vida cotidiana es cada vez más dependiente de estos sistemas. (Steering Committee for Foundations for Innovation in Cyber-Physical Systems, 2012, p. 2)

Estas tecnologías emergentes unen la autonomía y la precisión que ofrecen las directrices del ciberespacio con el direccionamiento de los tomadores de decisiones, y son usados para mantener bajo control a los adversarios (Asaro, 2012). Usar los recursos como el GPS para detectar un enemigo, o simplemente procesar imágenes que le entregan información al Estado que ejerce el control es una capacidad que antes no era posible con la rapidez y la exactitud que lo es ahora.

A partir de los avances tecnológicos, los cambios que han estado sucediendo en las últimas décadas presentan un escenario que podrá caracterizarse por necesitar instrumentos y herramientas cibernéticas más eficientes, participantes más capacitados en temas tecnológicos y cibernéticos que en los demás dominios, los avances rápidos en la potencia de cálculo, datos, inteligencia artificial, miniaturización y robótica, entre otros, harán los sistemas conectados al ciberespacio cada vez más capaces, autónomos y rentables (Brimley y Work, 2014). Los nuevos inventos serán capaces de reemplazar a los actores humanos en las tareas más peligrosas, pues podrán cubrir un mayor espectro en menor tiempo, obtener información más confiable; así mismo, serán un componente multiplicador de fuerza y mejoraran un sinnúmero más de condiciones que les impiden a los Estados controlar al adversario (Abney, Bekey y Lin, 2008).

> El progreso científico y técnico del deslumbramiento de las últimas décadas ha dado lugar a los medios y métodos de guerra sin

> precedentes. Algunas de estas nuevas tecnologías (como la observación y combate drones) ya están en uso, mientras que otros (nanotecnologías, robots de combate y armas láser) se encuentran todavía en fase experimental y de desarrollo. Además de la necesidad de capacidades militares en tierra, mar y espacio aéreo, grandes ejércitos están reconociendo la necesidad de contar con capacidades militares en el ciberespacio. (Bernard, 2012, p. 458)

El alcance y el control que ejercen los Estados con capacidades cibernéticas, como las mencionadas anteriormente, se refleja mediante las consecuencias dañinas sobre las infraestructuras críticas de los Estados rivales. Estas, que representan el corazón del Estado, son cada vez más dependientes del ciberespacio y están conectadas a él, confiando su funcionamiento y la información acerca de los procesos vitales de los Estados. "Hoy el término infraestructuras críticas se ha convertido en el punto clave para enfrentar las emergencias de muchas naciones. La mayoría de las definiciones apuntan hacia sistemas que son de vital importancia para la sociedad" (Kelly, Peerenboom y Rinaldi, 2001, p. 11).

Algunos conceptos acerca de la infraestructura crítica exponen que esta, a menudo, se identifica como el tipo de estructura, cuyo funcionamiento incorrecto, aunque sea por tiempo limitado, puede afectar negativamente la economía de los sujetos individuales o grupos, con pérdidas económicas e incluso exponer a la población a riesgos para la seguridad (Angelini, Arcuri, Baldoni y Ciccotelli, 2013). Por otro lado, la Ley Patriota de los Estados Unidos define que son "los sistemas y activos, físicos o virtuales, tan vitales que la incapacidad o la destrucción de dichos sistemas y activos tendrían un impacto debilitante en la seguridad, la economía nacional, la salud pública o cualquier combinación de esos asuntos" (Copeland, Fischer y Moteff, 2003, pp. 6-7).

Aunque existen diferencias en la clasificación de qué estructuras internas de los Estados pueden clasificarse como infraestructuras críticas, algunas que son comunes para todos son la agricultura, incluyendo la seguridad alimentaria, el agua, la salud pública, el sector defensa, los servicios de emergencia, el gobierno, la información y telecomunicaciones, la energía, el transporte, la banca y finanzas, la industria y el comercio (Dudenhoeffer, Hartley, Pederson y Permann, 2006). Es cada

vez más común reconocer que estos sectores son altamente vulnerables por las múltiples amenazas cibernéticas (Carr, 2010).

Por lo general, son tan vulnerables como cualquier otro sistema informático interconectado, pero su fracaso tiene un alto impacto socioeconómico, pues ya alcanzan tanto las infraestructuras virtuales vitales (la financiera por ejemplo), como las infraestructuras físicas (plantas eléctricas), por lo tanto, la amenaza ya no es contra los sistemas con un valor económico limitado, sino contra las infraestructuras que soportan la vida cotidiana (Bessani, Correia, Ferreira, Sousa y Verissimo, 2008) Actualmente, casi todas las funciones y los servicios de la infraestructura crítica y sus respectivos recursos clave están habilitados a través de la infraestructura cibernética; al no encontrase integrada adecuadamente la seguridad cibernética, el riesgo para el cumplimiento de las misiones de los sectores es mucho mayor (McDaniel Chairman y Stephan, 2008).

En este punto ya se ha hecho un recorrido por el método de disuasión y cómo este funcionó principalmente durante la Guerra Fría, ofreciéndoles a los Estados con capacidades nucleares el poder de convencer al adversario que una guerra solo traería consecuencias negativas. Con el fin de la época bipolar, aparece un nuevo paradigma, el de control a partir de los recursos cibernéticos, pues ya los Estados no solo cuentan con recursos para persuadir al otro, sino que también ya pueden entrar a su infraestructura y controlarlos desde allí. A continuación, algunos ejemplos de acciones cibernéticas serán el fiel reflejo de esta capacidad de controlar.

China se ha convertido en un Estado capaz de manejar los recursos informáticos de una forma bastante beneficiosa, ya que "cuenta con enormes recursos por el tamaño de su población y el número de graduados en matemáticas y ciencias de alta calidad" (Carr, 2010, p. 171). Los chinos han aprovechado la vulnerabilidad de la falta de seguridad para atacar, socavar, bloquear y restringir, el uso de los recursos informáticos y del ciberespacio por parte de los Estados Unidos, sacando de esto grandes réditos como información privilegiada, restringida y propiedad intelectual (Mancera, 2014).

El conflicto que existe entre Estados Unidos y China se debe a que el país norteamericano, aparentemente identificó a China mientras este

cometía acciones clasificadas dentro del concepto de guerra de información y ciberespionaje. Desde el 2002 se reconoció actividad fuera de lo común dentro de los sistemas de información estadounidenses y se dio inicio a una investigación que arrojó datos sorprendentes. La primera serie importante de incidentes de espionaje cibernético atribuidos a China se conoció *Titan Rain*; esta tenía como objetivo filtrar grandes cantidades de información de organizaciones estadounidenses o que tuviesen relación con dicho gobierno. De 2003 a 2005, los piratas informáticos incluyeron organizaciones como la Agencia de Sistemas de Información de Defensa (DISA), los Laboratorios Nacionales Sandia, el Banco Mundial, Lockheed Martin y la NASA (Ruef, Shakarian y Shakarina, 2013).

> Titan Rain ilustra algunos principios básicos de una operación de espionaje cibernético. Estas operaciones comienzan con una fase detallada de reconocimiento. Al término de esa tarea, el hacker procede a su misión de infiltrarse en los sistemas de destino. Una vez que los hackers tuvieron acceso a los sistemas, trabajaron con rapidez y eficacia para obtener los datos deseados y filtraron los datos a un sistema intermediario en un esfuerzo por cubrir sus huellas. La naturaleza de los datos, aunque no clasificada, se restringió bajo control de exportación que puede indicar que los atacantes tenían objetivos estratégicos relacionados con la obtención de los conocimientos tecnológicos con fines económicos y militares. (Ruef, Shakarian y Shakarina, 2013, p. 127)

Este tipo de acciones no se detuvieron y para 2011 surgió un nuevo nivel de preocupación al enfrentarse a los ataques *Shady RAT*, dirigidos hacia más de setenta gobiernos, instituciones internacionales, empresas y tanques de pensamientos. Este tipo de incidentes involucraron la copia no autorizada y la exportación de un sinfín de datos valiosos, desde secretos de Estado y tecnología de armas, pasando por estrategias de negocio de propiedad intelectual y de negociación corporativa a archivos personales y comunicaciones, tanto de personas de alto rango y miembros del público en general (Lieberthal y Singer, 2012).

Otra acción de ataque cibernética se vivió en Estonia transcurriendo en 2007. Durante dos semanas, entre abril y mayo, Estonia fue

víctima de agresiones cibernéticas en forma masiva sobre su infraestructura, considerado el primer asalto cibernético dirigido a la seguridad nacional de un país (Ashmore, 2009). Tras algunas tensiones de orden político con la minoría rusa que habita el país báltico y algunas protestas civiles ante las principales instituciones del Estado, todo parecía retornar a la calma, pero no fue así. Para el 29 de abril, si bien ya no habían protestas en escenarios públicos, se propagaba por internet una campaña de interrupción y denegación de servicios a lo largo de la infraestructura electrónica, usando paquetes de sobrecarga, desconfiguración de páginas web y avalanchas de correos no deseados y cargados de virus (Ruef, Shakarian y Shakarian, 2013).

La infraestructura cibernética se vio seriamente afectada, pues fueron cerrados los sitios web de todos los ministerios, de varios partidos políticos, de algunos bancos y portales de medios de comunicación; y se llegó a desactivar por completo el servicio correo electrónico del parlamento. Fue tal el alcance que los daños a los medios de comunicación hicieron que fuera imposible para los lectores, dentro y fuera del territorio, ingresar a los portales web, lo que generó una situación de desconocimiento total. Y las violaciones de seguridad que sufrieron las entidades financieras, como HansaBank, produjeron pérdidas por casi un millón de dólares, pues los clientes dentro y fuera de Estonia no pudieron disponer de su dinero; a pesar de estar fuera de circulación por tan solo una hora y media (Schdmit, 2013).

La dimensión del ataque alcanzó tal nivel debido a que Estonia basa el funcionamiento de su infraestructura crítica en la internet. Sus redes informáticas son esenciales para la labor de las operaciones gubernamentales, plantas energía eléctrica, servicios bancarios y suministro de agua. En Estonia, el 97 % de las transacciones bancarias se producen en línea y el Estado estonio es tan dependiente de internet que su modelo de operaciones del gobierno se conoce como "gobierno sin papel" (Herzog, 2011). Sobre quien fue el responsable de estas acciones, todo apunta a que fue el gobierno ruso el encargado de actuar contra Estonia, las direcciones IP fueron rastreadas hasta territorio ruso, el grupo pro-Kremlin *Nashi*, acusado con anterioridad de trabajar en nombre de Moscú, se adjudicó la responsabilidad de los daños, no hicieron propuestas para detener o frenar los ataques cibernéticos

que se estaban gestando desde su territorio y el día con mayor acción cibernética fue el 9 de mayo, "Día de la Victoria" en el cual se conmemoraba el triunfo de Rusia sobre el ejército alemán en la Segunda Guerra Mundial (Iasiello, 2013).

No muy distante en tiempo y accionado aparentemente por el mismo atacante, durante 2008, Georgia también vio cómo su estructura cibernética colapsó sin poder responder de forma prudente. Si bien, entre Rusia y Georgia se desarrolló una guerra convencional, esta dejó de serlo cuando una empresa de seguridad informática dio a conocer que se estaba llevando a cabo un ataque cibernético por medio de una denegación de servicios contra los sitios web en el país (Kastenberg y Korns, 2009). Los ataques se produjeron en dos momentos; en primer lugar, la denegación de servicios se dirigió a los sitios web gubernamentales y los principales medios de comunicación nativos y, a continuación, se amplió el espectro de daños a instituciones financieras, empresas instituciones educativas y medios de comunicaciones de carácter global (Ruef, Shakarian y Shakarian, 2013).

Además de interrumpir y negar los servicios que prestaban las plataformas informáticas, se usaron métodos de desconfiguración de redes y el aspecto de mayor relevancia fue que se apoderaron de una gran cantidad de información valiosa que fue de bastante utilidad para el comportamiento ruso, y la derrota sufrida por el ejército georgiano ante las Fuerzas Militares rusas (Cyber Committee of AFCEA, 2012). Kenneth Corbin (2009) afirmó que "los fines que motivaron la guerra en el ciberespacio por parte de los rusos, fueron aislar y silenciar a los georgianos. La ciberguerra logró callar a los medios de comunicación y aislar al país de la comunidad global", con lo cual controlaron el comportamiento del gobierno georgiano y de toda su población.

El último ejemplo que permite visualizar cómo el ciberespacio le entrega el control a un Estado sobre otro es el caso Stuxnet, sucedido en Irán durante 2010. El 17 de junio de 2010, investigadores de seguridad de VirusBlockAda identificaron un *software* malicioso (*malware*) que infectaba las redes informáticas y computadores a través de dispositivos USB. Durante los meses siguientes la comunidad de seguridad informática identificó un nuevo gusano informático conocido como Stuxnet, un *software* diseñado específicamente para afectar

equipo industrial y concretamente una planta de tratamiento de uranio (Shakarian, 2011).

La mayoría de las infecciones fueron descubiertas en Irán y se dio un inexplicable daño en las centrífugas de la planta de enriquecimiento de combustible iraní en Natanz; en los medios de comunicación se especuló que la meta final de Stuxnet era atacar las instalaciones nucleares iraníes. Esta teoría fue confirmada por un estudio realizado por Symantec, empresa encargada de la construcción y la comercialización de *software*, principalmente de seguridad, durante 2010, en el cual se afirmó que la concentración de infecciones en Irán indicaba que este era el objetivo inicial para las infecciones y donde se sembraron en un primer momento (Kerr, Rollins y Theohary, 2012).

Un gusano informático es un programa que realiza copias de sí mismo, para infectar a otros ordenadores y se propaga automáticamente en una red, independientemente de la acción humana (Sáez Collantes, 2012). Stuxnet, sofisticado programa informático, estaba diseñado para penetrar y establecer control sobre los sistemas remotos que mantenían en funcionamiento las centrifugadoras. Usando vulnerabilidades desconocidas para los ingenieros iraníes y que, por lo tanto, no tenían protección, Stuxnet fue capaz de atacar y reprogramar por completo el ordenador de la planta en Irán (Farwell y Rohozinski, 2011).

En este caso, el punto de innovación es la capacidad de hacer daño a infraestructuras físicas, "reales", exclusivamente por medios cibernéticos, es decir, como un arma completamente cibernética puedo afectar la infraestructura crítica y causar daños tangibles. El incidente dañó casi 1000 tubos de centrífuga en la instalación iraní de Natanz. Se produjo una disminución del 23 % en el número de centrifugadoras en funcionamiento desde mediados de 2009 hasta mediados de 2010, debido a Stuxnet (Gamero Garrido, 2014). Este incidente fue atribuido a un plan fraguado entre los Estados Unidos e Israel: necesitaba frenar el progreso iraní ante la construcción de una bomba atómica sin lanzar un ataque militar tradicional (Nakashima y Warrick, 2012).

Para concluir, el recorrido académico hecho con anterioridad, se pueden construir una serie consideraciones finales. En primer lugar, la disuasión se puede definir como la capacidad de inducir al actor adversario a no actuar en contra del disuasor, pues los costos de dicha

acción sobrepasarán los posibles beneficios y no se verán recompensados de la forma esperada. Entre sus principales características se encuentra que solo se puede dar entre Estados, que la amenaza de quien disuade debe ser creíble y, a su vez, este debe contar con los recursos para llevarla a cabo en caso de ser necesario.

Esta doctrina brilló durante la Guerra Fría porque existían dos actores con el suficiente poder nuclear para disuadirse el uno al otro y porque las armas de este tipo ejercían una influencia real, por su alcance y su capacidad de daño, pero al llegar la década de los noventa, con el fin de este periodo y la desaparición de la Unión Soviética, la disuasión como estrategia perdió fuerza, pues las condiciones ya no eran las adecuadas para seguir llevando un comportamiento persuasivo.

Con la aparición del entorno cibernético cobró fuerza un concepto que superaba el alcance de la disuasión y es el de control. Aparece gracias al ciberespacio, porque las oportunidades que ofrece este para que un Estado se sumerja en él le abren un abanico de posibilidades no solo para llegar a inclinar la decisión del adversario hacia la más conveniente para el Estado, le permite convencerlo y manejar sus decisiones a partir de la modificación de información, el engaño y los alcances físicos y virtuales sobre su infraestructura.

> El mundo físico actual está fuertemente integrado con el mundo virtual de la información en el ciberespacio. El ciberespacio toca prácticamente todos los aspectos de la sociedad moderna: economía, transporte, salud, infraestructuras civiles, seguridad pública y seguridad nacional. En particular, las capacidades militares se están convirtiendo rápidamente en dependientes de las innovaciones creadas por la tecnología cibernética. Por lo tanto, la tecnología informática está emergiendo como una fuerza dominante la guerra en el siglo XXI. La vulnerabilidad a la explotación ofensiva por los adversarios potenciales puede convertirse en una debilidad estratégica. Ya no hay ninguna necesidad de subrayar que el ciberespacio plantea serios desafíos. (Delpech, 2012, p. 151)

Los casos de acciones cibernéticas son el fiel reflejo de las capacidades de control que puede obtener un Estado sobre otro. China obtuvo información que puede llevarlo a conseguir ventajas económicas y

políticas y que obliga a los Estados Unidos a cambiar sus estrategias. Rusia consiguió, con Estonia, advertir los efectos que puede tener desafiar su poder, y con Georgia, derrotar y ganar una guerra a partir de la información y su uso adecuado. Por último, Estados Unidos e Israel consiguieron detener y retrasar el avance de un país como Irán que representaba un acto de rebeldía a su monopolio sobre el uso de la energía nuclear, sin necesidad de amenazarlo o sancionarlo.

En cuanto al punto que genera todo el debate entre disuasión y control, la disuasión solo logra lo que el Estado le permite, es decir, aquello que tiene dentro de sus capacidades, por lo tanto, esta debe adaptarse a cada caso particular y ver si se es capaz con lo que se posee, de persuadir al otro de no actuar en su contra; y además, requiere que exista un diálogo y el otro conozca las pretensiones propias. El control que se ejerce mediante el ciberespacio no depende solo de las capacidades del Estado, se enriquece a partir de las debilidades de los otros. Además, las acciones a través del ciberespacio poseen características que no exige su adaptación: son precisas, son efectivas, son rápidas y no exigen un contacto con el otro, lo cual impide que este pueda advertir el paso por seguir, le entrega la capacidad de sorprender.

La disuasión se hace creíble exclusivamente cuando el Estado es capaz de demostrar sus propias capacidades, puesto que depende en gran medida de las que se tiene y de las que se pueden desarrollar. La era del control surge por supuesto de las capacidades propias (cibernéticas e informáticas), pero se hacen mucho más fuertes con las vulnerabilidades y oportunidades que ofrece el contrincante, y que en un mundo tan interconectado como el de hoy, cada vez aumentan en número, sensibilidad y valor.

Referencias

Abney, K.; Bekey, G. y Lin, P. (2008). *Autonomous Military Robotics: Risk, Ethics, and Design*. California: Department of the Navy.

Alcolea Navarro, D. (2015). De la disuasión convencional a la protección. *Revista Ejercito 76* (888), 8-15.

Alvayay Castro, E. (2013). *La disuasión convencional interestatal y su relación con el rol de las Fuerzas Armadas en seguridad: un caso de éxito*

y otro de fracaso en América del Sur. Santiago de Chile: Academia de Guerra Naval.

Angelini, M., Arcuri, M. C., Baldoni, R. y Ciccotelli, C. (2013). *Critical Infrastructure and Other Sensitive Sectors Readiness*. Roma. Luiss Guido Carli.

Asaro, P. (2012). How Just Could a Robot War Be? En E. Gaston y P. Tamara (Eds.), *Ethics of 21st Century Military Conflict* (pp. 257-269). New York: International Debate Education Association.

Ashmore, W. (2009). Impact of Alleged Russian Cyber Attacks. En *Baltic Security & Defence Review, 11*, 4-40.

Baich, R. (2011). *Cyber Espionage: The harsh reality of advanced security threats*. Londres: Deloitte.

Baker, S., Ivanov, G. y Waterman, S. (2010). *In the Crossfire: Critical Infrastructure in the Age of Cyber War*. California: McAfee.

Barbé, E. (1987). EL papel del realismo en las relaciones internacionales (La teoría política internacional de Hans J. Morgenthau). *Revista de Estudios Políticos, 57,* 149-176.

Beaufre, A. (1966). *Disuasión y estrategia*. Madrid: Instituto de Estudios Políticos.

Bergman, T. y Ware, A. (2013). Dinosaur, Dragon or Durable Defence: Deterrence in the 21st Century: A Summary of Perspectives on Nuclear Deterrence. R. van Riet (Ed.), *Moving Beyond Nuclear Deterrence to a Nuclear Weapons Free World* (pp. 63-72). Londres: Nuclear Abolition Forum.

Bernard, V. (2012). Science cannot be placed above its Consequences. *New technologies and warfare, 94* (886), 457-466.

Bessani, A., Correia, M., Ferreira, N., Sousa, P. y Verissimo, P. (2008, nov.-dic.). The Crucial Way of Critical Infrastructure Protection. *IEEE Security and Privacy, 8,* 18-25.

Braganca, M. (2013, oct.). Hunt for Red October. The New Face of Cyber Espionage. *SIAK-Journal, 2*, 37- 44.

Brimley, S. y Work, R. (2014). *20YY: Preparing for War in the Robotic Age*. Washington D.C.: Center for a New American Security.

Brodie, B. (1945). *The atomic bomb and American security*. Connecticut: Yale Institute of International studies.

Brody, R. (1974). *Enciclopedia de las Ciencias Sociales* (vol. 3). Madrid: Aguilar.

Bustos Carrasco, M. y Rodríguez Marcos, P. (2004). *La disuasión convencional, conceptos y vigencia*. Santiago de Chile: MAGO.

Caballenas de Torres, G. (1961). *Diccionario Militar, Aeronáutico, Naval y Terrestre*. Buenos Aires: Claridad.

Calduch, R. (1991). Relaciones Internacionales. Madrid: Ediciones Ciencias Sociales. Recuperado de http://pendientedemigracion.ucm.es/info/sdrelint/indicelibro1.htm

Carr, J. (2010). *Inside Cyber Warfare*. California: Mike Loukides.

Casa Blanca (2003.) *The National Strategy to Secure Cyberspace*. Washington D.C.: Casa Blanca.

Clarke, M., Gearson, J. y Shaud, J. (2010) Post-Conference Briefing Note. En A. Cain, *Deterrence in the twenty-first century: proceedings* (pp. 291-296). Londres: Air University Press

Collins, J. (1980). *Los principios de la disuasión*. Washington D.C.: Air University.

Copeland, C., Fischer, J. y Moteff, J. (2003). *Critical Infrastructures: What Makes an Infrastructure Critical?* Washington D.C.: The Library of Congress.

Corbin, K. (2009, mar.). Lessons From the Russia-Georgia Cyberwar. *InternetNews.com*. Recuperado el 10 de marzo de 2016, de http://www.internetnews.com/government/article.php/3810011/Lessons-From-the-Russia-Georgia-Cyberwar.htm

Cox, A. (2013). *The Cyber Espionage Blueprint: Understanding Commonalities In Targeted Malware Campaigns*. Massachusetts: RSA.

Crawford, H. y Cronin, B. (1999). Information Warfare: It Application in Military and Civilian Contexts. *The Information Society, 15,* 257-263.

Cyber Committee of AFCEA (2012). *The Russo-Georgian War 2008: The Role of the cyberattacks in the conflict*. Fairfax: AFCEA.

De Bordeje Marencos, F. (1981). *Diccionario Militar, Estratégico y Político*. Madrid: San Martín.

Delibasis, D. (2007). *The Right to National Self-defense: In Information Warfare Operations*. Tennessee: Arena.

Delpech, T. (2012). *Nuclear Deterrence in the 21st century Lessons from the Cold War for a New Era of Strategic Piracy*. California: RAND Corporation.

Departamento de Defensa (2015). *Dictionary of Military and Associated Terms*. Washington D.C.: Departamento de Defensa.

Dudenhoeffer, D., Hartley, S., Pederson, P. y Permann, M. (2006). *Critical Infrastructure Interdependency Modeling: A Survey of U.S. and International Research*. Idaho: Idaho National Laboratory.

Estado Mayor Conjunto (2006). *The National Military Strategy for Cyberspace Operations*. Washington D.C.: Departamento de Defensa.

Farwell, J. y Rohozinski, R. (2011, feb.-mar.). Stuxnet and the Future of CyberWar. *Survival 53* (1), 23-40.

Ford, C. (2013). Conceptual Challenges to Nuclear Deterrence En R. van Riet (Ed.), *Moving Beyond Nuclear Deterrence to a Nuclear Weapons Free World* (pp. 4-7). Londres: Nuclear Abolition Forum.

Fredericks, B. (1997). Information Warfare: The Organizational Dimension. En R. Neiison (Ed.), *Sun Tzu and Information Warfare* (pp. 79-102). Washington, D.C.: DIANE Publishing.

Friedman, A. y Singer, P. W. (2014). *Cybersecurity and Cyberwar: What everyone needs to know*. New York: Oxford University.

Gamero Garrido, A. (2014). *Cyber Conflicts in International Relations: Framework and Case Studies*. Massachusetts: Universidad de Harvard.

García Covarrubias, J. (2001). La disuasión convencional. *Military Review, 81* (2), 72-80.

Grauer, R. (2013, feb.). Old Wine in New Bottles: The Nature of Conflict in the 21st Century. *The Whitehead Journal of Diplomacy and International Relations,* Volumen *14*. 9-23.

Hamon, L. (1996). *Estrategia contra la guerra*. Madrid: Guadarrama.

Herzog, S. (2011, jun.). Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses. *Journal of Strategic Security, 4* (2), 49-60.

Howlett, D. (2002). New concepts of deterrence. *Analysis, 16,* 17-23.

Iasiello, E. (2013). Cyber Attack: A Dull Tool to Shape Foreign Policy. En M. Maybaum, K. Podins y J. Stinissen (Eds.) (2013). 5th International Conference on Cyber Conflict (pp. 451-468). Tallin: NATO CCD COE Publications.

Johnson, J. (1998). *Encyclopedia of Applied Ethics*. Oregon: Eastern Oregon State College. Recuperado de https://people.eou.edu/jjohnson/files/2012/12/NUCLEAR-DETERRENCE.pdf

Jones, A., Kovachich, G. y Luzwick, P. (2002). *Global Information Warfare: How Businesses, Governments, and Others Achieve Objectives and Attain Competitive Advantages*. Estados Unidos: Auerbach Publications.

Kaspersky, E. (2013). *Who's spying on you? No business is safe from cyber-espionage*. Moscu: Kaspersky Lab.

Kastenberg, J. y Korns, S. (2009). Georgia's Cyber Left Hook. *Parameters*, Volumen 38. 60-76.

Kelly, T. K., Peerenboom, J. P. y Rinaldi, S. M. (2001). Identifying, understanding, and analyzing critical infrastructure interdependencies. *IEEE Control Systems Magazine,* 11-25.

Kerr, P., Rollins, J. y Theohary, C. (2012, dic.). The Stuxnet Computer Worm: Harbinger of an Emerging Warfare Capability. En *CRS Report for Congress*. Washington D.C.: UNT Digital Library.

Kumar, A. (2007). Theories of Deterrence and Nuclear Deterrence in the Subcontinent. En E. Sridharan (Ed.), *The India-Pakistan Nuclear Relationship: Theories of Deterrence and International Relations* (pp. 239-265). New Delhi: Routledge.

Lieberthal, K. y Singer, P. W. (2012). *Cybersecurity and U.S.-China Relations*. Washington D. C.: Brookings Institute.

López de Turizo y Sánchez, J. (2012, feb.). La evolución del conflicto hacia un nuevo escenario bélico. *El Ciberespacio: nuevo escenario de confrontación, 126*, 117-167.

López, C. C. (2007, may-ago.). La guerra informática. *Boletín del Centro Naval, 817,* 219-224.

Lord, K. y Sharp, T. (2011). America's Cyber Future. Security and Prosperity in the Information Age Volume I. Washington, D.C.: Center of New American Security.

Lowter, A. (2010) Framing Deterrence in the Twenty-first Century. Conference Summary. En A. Cain (Ed.), *Deterrence in the twenty-first century: proceedings* (pp. 1-14). Londres: Air University Press.

Mancera, J. M. (2014). La ciberguerra china desde la lógica de la guerra irrestricta. *Ciencia y Poder Aéreo, 9,* 89-96.

MccGwire, M. (2006). Nuclear Deterrence. *International Affairs, 82* (4), 771-784.

McDaniel Chairman, M. y Stephan, R. (2008). *A Guide to Critical Infrastructure and Key Resources Protection at the State, Regional, Local, Tribal, and Territorial Level*. Washington D.C.: Office of Infrastructure Protection.

Mearsheimer, J. (1983). *Conventional Deterrence*. Londres: Cornell University Press.

Miller, J. (1997). Information Warfare: Issues and Perspectives. R. Neiison (Ed.). *Sun Tzu and Information Warfare* (pp. 145-167). Washington, D.C.: DIANE Publishing.

Molander, R., Riddile, A. y Wilson, P. (1996). *Strategic Information Warfare: A new face of war*. Estados Unidos: RAND Corporation.

Morgenthau, H. (1963). *La lucha por el poder y por la paz*. Buenos Aires: Editorial Sudamericana.

Nakashima, E. y Warrick, J. (2012, jun.). Stuxnet was work of U.S. and Israeli experts, officials say. *The Washington Post*. Recuperado el 15 de marzo de 2016, de https://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html

Oppenheimer, R. (1946). The Atomic Bomb and College Education. En J. Kaplan (Ed.) (1992), *Bartlett's Familiar Quotations*. Boston: Little Brown.

Pardesi, M. (2005). *The Impact of RMA on Conventional Deterrence: A Theoretical Analysis*. Singapur: Institute of Defence and Strategic Studies.

Paul, T.V. (2009). *Complex Deterrence: Strategy in the Global Age*. Illinois: University of Chicago Press

Pérez Cortés, M. (2012, feb.). Tecnologías para la defensa en el ciberespacio. En: *El ciberespacio: Nuevo escenario de confrontación 126,* 255-304.

Quilés, P. (2013). Nuclear Deterrence: Not Suitable for the 21st Century. En R. van Riet (Ed.), *Moving Beyond Nuclear Deterrence to a Nuclear Weapons Free World* (pp. 8-12). Londres: Nuclear Abolition Forum.

Quinlan, M. (2004). Deterrence and Deterrability. *Contemporary Security Policy, 25* (1), 11-17.

Rajmil, D. (2015) Oriente próximo; disuasión y disuasión nuclear. *Revista IEEE, 2*. Recuperado de http://revista.ieee.es/index.php/ieee/article/view/239/324.

Rattray, G. (2001). *Strategic warfare in cyberspace*. Massachusetts: Massachusetts Institute of Technology.

Real Academia Española (s. f.). *Diccionario de la Lengua Española*. Recuperado de http://dle.rae.es/?id=DzWnEaA

Ruef, A., Shakarian, J. y Shakarian, P. (2013). *Introduction to Cyber-Warfare: A multidisciplinary approach*. Massachusetts: Elsevier.

Sáez Collantes, L. F. (2012). *La ciberguerra en los conflictos modernos*. Santiago de Chile. Recuperado el 15 de marzo de 2016, de https://www.academia.edu/9339213/LA_CIBERGUERRA_EN_LOS_CONFLICTOS_MODERNOS

Schdmit, A. (2013). *The Estonian Cyberattacks*. En J. Healey (Ed.), *The fierce domain – conflicts in cyberspace 1986-2012*. Washington D.C.: Atlantic Council.

Shakarian, P. (2011, abr.). Stuxnet: Cyberwar Revolution in Military Affairs. *Air & Space Power Journal*, Volumen 8 Número 98. 50-59.

Sodupe, K. (1991). La teoría de la disuasión: un análisis de las debilidades del paradigma estatocentrico. *Afers Internacionals, 22*, 53-79.

Steering Committee for Foundations for Innovation in Cyber-Physical Systems (2012). Strategic R&D Opportunities for 21 Century Cyber-Physical Systems: Connecting computer and information systems with the physical world. Illinois: Foundation for Innovation in Cyber-Physical Systems.

Stel, E. (2014). Seguridad y Defensa del Ciberespacio. Ayacucho: Editorial Dunken.

Taddeo, M. (2012, mar.). Information Warfare: A Philosophical Perspective. *Philosophy & Technology, 25* (1), 105-120.

Waterfall, G. (2011). *E-espionage What risks does your organization face from cyber-attacks?* Londres: PricewaterhouseCoopers LLP.

Yost, D. (2005) Dissuasion and Allies. *Strategic Insights, 4* (2). Recuperado de http://calhoun.nps.edu/bitstream/handle/10945/11472/yostfeb05.pdf?sequence=1