

Estrategias asimétricas como estrategias del fuerte

Michael Breen y Joshua A. Geltzer
© 2011 Michael Breen e Joshua A. Geltzer

Este artículo originalmente fue publicado en Parameters (primavera de 2011)

ESPOCOLO que se necesita ahondar en los debates más recientes y profundos acerca de la política exterior estadounidense para encontrarse con el concepto sobre las estrategias asimétricas. Así como lo describe la estrategia en sí, el concepto, a menudo parece frustrantemente, amorfo pero, al mismo tiempo, preocupantemente omnipresente y, aún más importante, inconfundiblemente amenazante para Estados Unidos.

En este artículo se toma seriamente la idea de la estrategia asimétrica, sin embargo, se replantea de una manera fundamental. En el presente artículo se cuestiona la constante identificación de las estrategias asimétricas como estrategias del débil, en lugar de considerar las distintas maneras en que están siendo adoptadas por actores cada vez más fuertes. Por consiguiente, también se rechaza la idea de que sólo se pueden emplear las estrategias asimétricas contra Estados Unidos y se busca estimular la reflexión para encontrar las distintas maneras en que Estados Unidos puede adoptar las mismas. Finalmente, también se concluye que los formuladores de la política exterior estadounidense deberían desistir de considerar las estrategias asimétricas como el dominio exclusivo de actores débiles no estatales y, en su lugar, deberían considerarlas incluso, más importantes cuando hábilmente son empleadas por fuertes actores— incluyendo Estados Unidos.

La primera parte de este artículo propone una definición diferente de la estrategia asimétrica

que, a diferencia de muchas definiciones previamente propuestas, identifica tal estrategia independientemente de los actores que las ejecutan: las estrategias asimétricas convierten la percibida fortaleza de un adversario en una vulnerabilidad, que con frecuencia, revela la propia vulnerabilidad percibida como punto fuerte. En la segunda parte se usa la definición para mostrar las maneras en las cuales las estrategias asimétricas ya están siendo adoptadas por los opositores de Estados Unidos, incluyendo los Estados. En la última parte se propone una nueva forma de pensar sobre cómo Estados Unidos puede emplear las estrategias asimétricas contra muchos de sus opositores.

El concepto de estrategias asimétricas: definición

La estrategia asimétrica ha sido un concepto fundamental desde el 11-Septiembre, sin embargo, sigue siendo sumamente difícil de definir.² Muchos de los intentos para precisar el concepto son tan generales que enfocan la definición de estrategia en sí, limitando toda utilidad práctica.³ Por ejemplo, un artículo base sobre la estrategia asimétrica afirma que “la estrategia asimétrica es el uso de algún tipo de diferencia para obtener una ventaja sobre un adversario”.⁴ De ser correcta esta formulación, no queda claro cómo las estrategias asimétricas difieren de otras estrategias: “Destacar sus propios puntos fuertes y explotar las debilidades del adversario es de lo que se trata la estrategia”.⁵

Michael Breen es vicepresidente del Proyecto de seguridad nacional de Truman, Oficial de armas de combate del Ejército de EUA e integrante de la clase de 2011 de la Facultad de Derecho de Yale. Se graduó en el Dartmouth College.

Joshua A. Geltzer, también integrante de la clase de 2011 de la Facultad de Derecho de Yale, tiene a su haber un Doctorado en Estudios de Guerra del College King de Londres, donde estudió con becas académicas de guerra Marshall. Geltzer es el editor de la publicación de Yale Law Journal.



Asistencias militares de la Fuerza Aérea de Estados Unidos en la evacuación por helicóptero de ciudadanos estadounidenses debido al conflicto entre las fuerzas de Hezbolá e israelíes en el Líbano, Embajada de Estados Unidos en Beirut, 24 de julio de 2006.

Otras definiciones comúnmente usadas son más específicas, pero confieren grandes diferencias en la relativa fortaleza de las partes involucradas en un conflicto y las estrategias que usan dichas partes. En otras palabras, estas definiciones parecen sugerir que la estrategia asimétrica prácticamente es cualquier cosa que puede hacer un actor débil ante un rival mucho más fuerte, especialmente, si esa acción es algo inesperada o creativa: “la guerra asimétrica es una acción violenta llevada a cabo por los desfavorecidos contra los privilegiados, mediante la cual los primeros— ya sea el estado o subestados, buscan producir profundas consecuencias...mediante el empleo de sus relativas ventajas contra las vulnerabilidades de adversarios mucho más fuertes”.⁶ Hay que admitir que el fenómeno ya descrito es de interés primordial para Estados Unidos, en su condición de única superpotencia en el mundo. El problema yace en que prácticamente cualquier entidad, actores estatales o no estatales a los que Estados Unidos pudiera enfrentar, serán menos poderosos que este mismo. Si las estrategias asimétricas son simplemente lo que pueden hacer los actores más débiles contra los más fuertes, entonces, desde el punto de vista estadounidense, las estrategias asimétricas

son justamente buenas estrategias contra los Estados Unidos: “Todo plan militar que evite la confrontación directa, fuerza contra fuerza, en una lucha justa en el campo de batalla, también se consideraría asimétrico”.⁷

Nos damos cuenta del hecho de que las anteriores definiciones de estrategia asimétrica han sido útiles para describir al mundo de la post guerra Fría, de adversarios más débiles pero irregulares que confrontan a Estados Unidos. Dicho esto, consideramos que los estrategas, soldados y académicos se beneficiarían por igual de una definición más precisa— una que identifique la estrategia asimétrica como una categoría conceptual en sí misma, independientemente de la fortaleza o debilidad del actor que la utilice.

Las estrategias asimétricas se asemejan al arte marcial japonés *jujutsu*, el cual se basa en la idea de que la fortaleza y energía de un oponente puede usarse en contra del mismo, en lugar de directamente enfrentarlo con la propia fuerza. Al enfrentar a un adversario más alto y más fuerte, por ejemplo, a un practicante del *jujutsu* se le insta ver la ventaja en cuanto a tamaño y masa muscular del adversario como una debilidad que puede aprovechar, ya que tales características tienden a generar un alto centro de gravedad. Igualmente, los practicantes de *jujutsu* usan la

propia fuerza que emplea un adversario al lanzar un golpe para tirarlo al piso, en lugar de bloquear el puñetazo e intentar responderle con la misma fuerza.

Este enfoque ofrece varias ventajas en el combate mano a mano— independientemente de la fuerza relativa de los dos oponentes. Dicho enfoque ayuda a tomar la iniciativa, mientras que el oponente experimenta su propia acción intencionada e inherente fuerza empleada contra sí mismo. La fuerza del practicante de *jujutsu* es, en gran medida, conservada, mientras que, en gran parte, la misma fuerza del oponente es la que produce su derrota en lugar de otra fuerza externa. Aún más importante, el *jujutsu* es muy difícil de contrarrestar: ¿cómo se enfrenta a un oponente, que de modo consistente, revierte su fuerza contra usted mismo?

Si se define y comprende correctamente, la estrategia asimétrica es bastante similar. En virtud de esta comprensión, ofrecemos una definición del concepto: las estrategias asimétricas convierten en vulnerabilidad la fortaleza percibida del oponente, a menudo, mostrando su propia vulnerabilidad como fuerza. La estrategia asimétrica es una forma de arte inherentemente correlativa que a menudo se aprovecha de las percepciones erróneas del oponente, tanto acerca del actor asimétrico como de él mismo.⁸ Lo más importante es que está disponible para cualquier actor estratégico, ya sea débil o fuerte. Los únicos atributos que exige la estrategia asimétrica son destreza y astucia.

Estrategias asimétricas: más que un arma para el débil

Las estrategias asimétricas típicamente son conceptualizadas como las armas del débil. Rod Thornton, por ejemplo, define al “adversario asimétrico” como el “protagonista más pequeño y más débil”.⁹ Thornton no es el único que así lo considera: si bien las estrategias asimétricas han sido motivo de interés desde, al menos, 1995,¹⁰ dicho interés en el concepto evidentemente aumentó desde los ataques del 11-Septiembre, y los estadounidenses han centrado su interés en los adversarios cuya capacidad limitada los hace parecer débiles, por lo menos, en el sentido tradicional.

No es la debilidad inherente de los adversarios no estatales lo que los califica como actores

asimétricos. Veamos la descripción de Thornton de las tres principales características de los nuevos terroristas que deben ser tomadas en consideración: su gran fervor, su incrementada capacidad de llevar a cabo ataques y su mayor capacidad para ocasionar bajas en masa”.¹¹ Ninguno de estos atributos son inherentes del débil. Durante la guerra fría, lo que Estados Unidos temía más de su fuerte adversario, la Unión Soviética, era su gran fervor, su mejorada capacidad de ataque y su gran habilidad para ocasionar destrucción en masa.

Otros autores que exploran las estrategias asimétricas, identifican lo que ciertamente parece ser la novedad acerca de los “grupos terroristas globales” y la amenaza que presenta para Estados Unidos: el hecho es que la economía mundial, las fronteras relativamente permeables, las fuentes abiertas de inteligencia e información y los inadecuados recursos para obligar el cumplimiento de la ley, permite el acceso a una gama de insumos, servicios e información que juntos, pueden transformarse en armas poderosas.¹² En otras palabras, no hubo ninguna característica propia de al-Qaeda, que transformara el ataque del 11-Septiembre en un ejemplo paradigmático de estrategia asimétrica. Más bien, es la ineludible manera correlativa en la que el grupo transformó los atributos de Estados Unidos, considerados siempre como puntos fuertes— por ejemplo, la economía interconectada del país, las fronteras abiertas y el libre flujo de información— en devastadoras vulnerabilidades. Y al-Qaeda lo logró haciendo uso inteligente de aspectos de su propia identidad, las cuales Estados Unidos consideraba como vulnerabilidades, tales como su pequeño número, armas improvisadas y limitado entrenamiento.

Puede ser que un actor no estatal débil tenga mayor motivación para adoptar tales estrategias, a fin de superar la falta de alternativas, pero no hay razón alguna para que un actor estatal fuerte no pueda hacer lo mismo.¹³ En el influyente libro titulado *Unrestricted Warfare*, (Combate sin restricciones, en traducción libre), dos Coroneles del Ejército de Liberación de China Popular sostienen que las estrategias actualmente asociadas con grupos terroristas pueden y deben ser adaptadas para su empleo mediante Estados tales como China: los nuevos y antiguos terroristas quienes regularmente

defendían el principio de recurrir a todos los medios imaginables, siguen siendo los mejores profesores de los gobiernos de cada país.¹⁴ De hecho, como se demostrará en la siguiente sección de este artículo, Estados miembros cada vez más fuertes, ya están utilizando estrategias asimétricas, generalmente relacionadas con actores no estatales. Consecuentemente, la actual tendencia a identificar las estrategias asimétricas con actores no estatales débiles surge del mismísimo evento fortuito histórico y de la confusión conceptual, en lugar de algo inherente en el propio concepto.¹⁵

Si bien los teóricos se centran en las estrategias asimétricas como el dominio de los débiles, actores cada vez más fuertes han comenzado a desplegarlas y a utilizarlas, a menudo con impresionantes resultados. En la siguiente sección se analiza la forma en que los Estados fuertes como China y Rusia, o poderosas entidades no estatales, tales como Hezbolá, han intentado transformar los puntos fuertes percibidos de sus oponentes en vulnerabilidades, utilizándolos como sus propias fortalezas.

Lo que están haciendo contra nosotros

A pesar del enfoque prevaleciente sobre las amenazas asimétricas que los actores no estatales presentan para Estados Unidos y sus aliados, con mayor frecuencia los Estados también elaboran y emplean estrategias que buscan aprovechar los evidentes puntos fuertes estadounidenses como vulnerabilidades latentes. Esto no debería ser ninguna sorpresa. Tal vez motivado por la tríada explicativa de Tucídides que reza, “miedo, honor e interés”, las potencias emergentes tales como China, Rusia e Irán, sienten la necesidad de desarrollar la capacidad de neutralizar o al menos minimizar el poder estadounidense.¹⁶ Dada la posición de dominio económico y militar que posee Estados Unidos en la actualidad, los Estados que buscan coaccionar o disuadir a Estados Unidos, tienen un incentivo para ser creativos. Las dos ocasiones en que las fuerzas armadas convencionales de Iraq, cuya doctrina fue inspirada por la Unión Soviética, fueron rápidamente destruidas en un período de un poco más de una década, ofrecen una clara

lección a potenciales opositores del Estado: “No se enfrente a Estados Unidos a menos que cuente con armas nucleares”.¹⁷

Por lo tanto, sin dejar de desarrollar capacidades convencionales, algunos Estados miembros han decidido elaborar estrategias concebidas para aprovechar las claras fortalezas estadounidenses como reales vulnerabilidades. Como a menudo es el caso, el punto de vista resulta fundamental. Por ejemplo, un importante punto fuerte del país es la magia que permite a los Estados Unidos utilizar las redes de computadoras y los programas informáticos que le permite al país coordinar incursiones aéreas por todo el mundo con increíble precisión, desde centros de comando geográficamente distantes. Sin embargo, a los ojos de un adversario asimétrico, esta misma capacidad puede verse como una peligrosa dependencia, que deja la fastuosamente costosa fuerza armada estadounidense vulnerable a los relativamente menos costosos ataques cibernéticos. La relativa fortaleza de los adversarios de Estados Unidos en esta ecuación es irrelevante: la estrategia es asimétrica, independientemente si es empleada por un pequeño grupo de piratas informáticos, un débil actor regional o un poderoso adversario global.

Por lo tanto, no es de sorprender que una variedad de Estados hayan comenzado a ejecutar estrategias asimétricas contra Estados Unidos. Con esto, se está produciendo un tipo de evolución paralela. En los últimos dos décadas, actores asimétricos, cada vez más fuertes, han elaborado estrategias bastante similares. A continuación destacamos varias de ellas para ejemplificar la tesis central: que las estrategias asimétricas—adecuadamente comprendida, ya están siendo empleadas por actores cada vez más fuertes, incluso Estados, y no solamente por débiles actores no estatales.

Combate híbrido

Tal vez, la insurgencia es una estrategia asimétrica simbólica y ha demostrado ser muy eficaz en “invertir” los puntos fuertes, incluso, los de las fuerzas armadas más poderosas del mundo. Desde hace mucho tiempo, los Estados han apadrinado la insurgencia como un medio para acosar a un adversario; tales tácticas fueron comunes durante la guerra Fría y en la actualidad



Cuerpo de Infantería de Marina de EUA

Nube de humo del bombardeo cuartel estadounidense en el Aeropuerto Internacional de Beirut, donde perecieron más de 200 Infantes de Marina estadounidenses.

están siendo empleadas en distintos lugares. Como una estrategia para ser directamente empleada por un Estado en una confrontación militar típica, contra otro Estado, la insurgencia resulta poco atractiva. Una emergente pero aún incipiente mezcla de tácticas, técnicas y tecnologías, combina algunas de las ventajas asimétricas clave de la insurgencia con enfoques más convencionales para mantener y controlar un territorio. A menudo denominado “combate híbrido”, este enfoque evolutivo en combate terrestre pronto puede presentarle a los Estados una alternativa asimétrica viable contra Estados Unidos.¹⁸

Indudablemente, la insurgencia es un grave desafío asimétrico hasta para las más poderosas fuerzas armadas tales como la de Estados Unidos. La estrategia es asimétrica, según nuestra definición, en el sentido de que pretende convertir en desventajas las ventajas militares en masa y poder de fuego, agotando al enemigo en una campaña prolongada mientras lo incita al error o lo engaña, llevándolo contra la población civil. Las tropas convencionales tienden a participar en la obtención y mantenimiento de terrenos clave y centran su energía destructiva en la eliminación de las fuerzas armadas enemigas; mientras tanto, los insurgentes se enfocan en la población y en sus oponentes convencionales, cediendo regularmente terrenos clave y suelen concentrar sus esfuerzos en actos simbólicos de violencia, que cambian a su favor el equilibrio

del poder político. Entonces, en la mayoría de los casos, la insurgencia aprovecha los cambios favorables en el equilibrio político para cambiar a su favor el balance del poder militar. De no poder lograr tal cambio, sencillamente la insurgencia sigue sobreviviendo mientras agotan la voluntad para luchar del oponente, hasta tanto las fuerzas convencionales, debilitadas por la baja moral, decide retirarse de la región del conflicto.¹⁹

En los últimos cien años, la insurgencia ha demostrado ser una herramienta eficaz para los actores no estatales que participan en campañas contra un gobierno, ya sea nacional o extranjero, sin embargo, tiene serias limitaciones. Si bien la insurgencia es a menudo una estrategia ofensiva, políticamente hablando, en el sentido de que frecuentemente busca reemplazar a un gobierno por otro, la insurgencia es principalmente defensiva en términos geográficos.²⁰ Mao Zedong, el padre doctrinal de la moderna insurgencia, concibió de manera genial a los insurgentes como peces nadando en el “mar” en una población amigable. Evidentemente, este enfoque requiere que el insurgente sea parte de la población en la que nada, o por lo menos, contar con la lealtad de la misma.²¹

Incluso, como estrategia defensiva, la insurgencia representa el último recurso para los gobiernos, porque requiere que un gobierno permita que una fuerza hostil invada y ocupe su territorio, antes que la insurgencia pueda incluso comenzar. Mao, describió sus planes para la insurgencia contra el ejército japonés acertadamente de la siguiente manera: la estrategia del invasor debe ser una de guerra tipo relámpago. Si podemos aguantar por tres o más años, será muy difícil que ellos lo soporten bajo tensión”.²² Para la mayoría de los líderes nacionales, tomar las colinas y los callejones durante tres o más años mientras las fuerzas armadas extranjeras ocupan su país, es definitivamente una opción defensiva poco atractiva, incluso, cuando la probabilidad de éxito de una campaña convencional de defensa territorial es mínima. Aún cuando finalmente el enemigo es derrotado, resulta probable que el país anfitrión quede devastado y el sistema político que existía antes de la guerra, apenas sobreviva. De ahí que, para un Estado, la insurgencia es poco atractiva porque la base de la propia estrategia es la renuencia a luchar por su integridad territorial.

El combate híbrido puede, parcialmente, remediar esa falla, mientras conserva muchas de las ventajas asimétricas de la insurgencia. En teoría, el combate híbrido combina las estructuras de liderazgo y comunicaciones sumamente descentralizadas, la logística reducida y la sinergia con la población civil, con tácticas concebidas para mantener el terreno y destruir la fuerza de oposición, en lugar de solo acosarla. Análogo a la insurgencia, el combate híbrido, a menudo, se basa en el modelo de “infantería ligera”, que mayormente evita emplear grandes sistemas de armamento, fáciles de detectar, tales como tanques y artillería de alto calibre.²³ A diferencia, las fuerzas híbridas emplean misiles antitanques portátiles, cohetes, proyectiles y morteros. La proliferación de armas de precisión guiada sigue haciendo a las mismas, cada vez más poderosas contra las formaciones blindadas convencionales, hasta el punto de que una fuerza de infantería descentralizada pero bien equipada, que puede infiltrarse en la población civil, es, cada vez más capaz de resistir el ataque. Una fuerza como esta presenta algunas de las vulnerabilidades defensivas que suelen caracterizar a las fuerzas convencionales. Por ejemplo, si bien las fuerzas armadas estadounidenses típicamente pueden adquirir el objetivo y destruir una red de comunicación y logística del enemigo antes de iniciar un ataque, tal infraestructura es difícil de identificar y es imperceptible en los sistemas civiles si el oponente es una fuerza híbrida descentralizada que mantiene fuertes lazos con la población.

Si bien el combate híbrido sigue siendo una amenaza emergente, algunos analistas de defensa creen que la experiencia de Israel contra Hezbolá en el sur del Líbano, en 2006, puede revelar algo de lo que está por venir. El conflicto es digno de señalar porque la Fuerza de Defensa Israelí (FDI, por sus siglas en español) está equipada predominantemente con tecnología militar estadounidense y utiliza tácticas al estilo de Estados Unidos, tuvo dificultad para dominar las fuerzas irregulares de un adversario en la campaña israelí de conquistar y mantener terreno.²⁴ De alguna manera, el mismo Hezbolá es híbrido, ya que es un actor no estatal, con orígenes de organización insurgente y terrorista, que también controla territorio y realiza muchas de las

funciones tradicionales de un Estado. Durante sus 24 años de historia, hasta el enfrentamiento con las FDI, en 2006, Hezbolá parece haber desarrollado un enfoque híbrido equivalente para luchar contra su convencional, bien entrenado y equipado oponente. Por un lado, Hezbolá continúa haciendo énfasis en una estructura organizacional con base en células tipo insurgente descentralizada y autónoma, prácticamente sin ningún “caudal” logístico y, frecuentemente, hace uso de tácticas de “ataque sorpresa” que pretende causar más provocación política que algún efecto militar. Sin embargo, las fuerzas de Hezbolá simultáneamente defendieron el sur del Líbano en 2006, con el uso de una compleja serie de refugios antiaéreos preparados y ocultos, diseñados y equipados para mantener una defensa prolongada y emplearon una serie de sistemas guiados de armas de tecnología avanzada, contra blancos israelíes en tierra e incluso en el mar.²⁶ A diferencia de los insurgentes tradicionales, los combatientes de Hezbolá, en 2006, consistentemente lucharon para mantener el terreno contra un determinado ataque de las formaciones blindadas israelíes, a veces con éxito.²⁷

Durante la incursión terrestre israelí que duró 33 días, la fuerza híbrida de Hezbolá, de guerra convencional y no convencional, le permitió infligir más bajas israelíes en comparación con las bajas árabes, que cualquiera de los tradicionales adversarios de Israel, en la guerra árabe-israelí de los años 1956, 1967, 1973 o 1982.²⁸ Dadas las similitudes entre las formas de librar guerras de Israel y Estados Unidos, este hecho no pasó desapercibido por potenciales adversarios de Estados Unidos, Irán, y en particular, pudo haber usado el conflicto de 2006 como una prueba de las estrategias concebidas para defenderse contra una posible invasión estadounidense, y directamente proporcionar la mayor parte del arsenal de Hezbolá. Según lo planteó un observador del conflicto: “Hezbolá entrena a Irán, no lo contrario”.²⁹ Originalmente, Rusia desarrolló y fabricó la gran mayoría de los sistemas de armas de tecnología avanzada de Hezbolá, y sin duda alguna, los planificadores militares rusos prestaron gran atención a su empleo y efectividad.³⁰ Mientras tanto, China está desarrollando su propia estrategia para negar el Pacífico Occidental a las fuerzas estadounidenses,

en parte, por el amplio uso de misiles guiados, empleados de manera descentralizada, un enfoque que se denomina “*Assassin’s Mace*” (Laberinto del Asesino).³¹ Los observadores estadounidenses, inmediatamente se han dado cuenta de la amenaza que presentan tales tácticas.³²

Potencialmente, el combate híbrido permite a los Estados disfrutar de algunas ventajas de la insurgencia y, al mismo tiempo, evitar significativos costes, especialmente, la renuncia a terrenos clave. Esta estrategia presenta una ventaja asimétrica, ya que permite a un adversario transformar la ventaja del oponente con respecto a las costosas armas de tecnología avanzada en una vulnerabilidad, mientras que simultáneamente convierten la debilidad en cuanto a armas y número de tropas, en fortaleza. Después de que Estados Unidos entrara en Afganistán y luego en Irak, los Estados interesados en defender sus fronteras contra una posible invasión estadounidense, tales como Irán y Corea del Norte, comenzaron a considerar las armas nucleares como su alternativa de defensa principal. Sin embargo, en un futuro cercano, las guerras híbridas pueden permitir que estos opositores organicen una defensa convencional más efectiva contra la manera de hacer la guerra de Estados Unidos.

La ciberguerra

En los últimos años, la ciberguerra ha emergido como un grave desafío para los países que poseen la tecnología más avanzada del mundo, incluyendo a Estados Unidos. La estructura descentralizada y compleja de la propia Internet agrava esta amenaza, ya que es cada vez más factible para los Estados y actores no estatales desarrollar y emplear, anónimamente, las capacidades de guerra cibernética o través del potencial uso inconsciente, lo que hace difícil proponer una forma de contrarrestarlo. Considerando que es posible nivelar las condiciones a través de la interrupción o desactivación de las capacidades de tecnología de punta del oponente, y tal vez, incluso haciéndolo con una negación plausible, es comprensible que los Estados grandes y pequeños hayan dedicado cada vez más recursos para el fomento de una capacidad de guerra cibernética.

La lista de países que activamente buscan desarrollar capacidades de guerra cibernética es extensa e incluye a varios potenciales adversarios

de Estados Unidos. China ha desarrollado una doctrina militar oficial para la guerra cibernética, ha entrenado un gran número de oficiales militares para llevar a cabo operaciones ofensivas en Internet y ha llevado a cabo una extensa serie de ejercicios y simulacros.³³ Rusia ha desarrollado una fuerte capacidad de guerra cibernética, en parte, en consulta con China.³⁴ Además, Rusia ha demostrado gran interés por la guerra cibernética ofensiva durante la última década, llevando a cabo ataques de este tipo contra sitios de Chechenia desde 2002.³⁵ Utilizando grupos criminales como ejecutantes, Rusia empleó los ataques cibernéticos para paralizar las redes de Georgia antes del ataque militar convencional de Rusia en 2008, después de haber confirmado su utilidad en un enfrentamiento anterior con Estonia.³⁶ En ambos casos, fue el actor más fuerte, Rusia, quien adoptó una estrategia asimétrica. Además, se sabe que Irán, India, Pakistán y Corea del Norte están desarrollando capacidades de guerra cibernética con distintos grados de complejidad y efectividad, a veces en coordinación con organizaciones delictivas.³⁷

Como han señalado algunos observadores, la guerra cibernética se comprende mejor no como una plataforma para tácticas completamente nuevas sino como un nuevo entorno en donde los conflictos ocurrirán en formas más o menos similares a las utilizadas en tierra, mar, aire o espacio.³⁸ En este nuevo y evolutivo entorno, así como ocurre en los entornos de combate tradicionales, veremos elaborarse muchas estrategias que combinan y encajan en los métodos directos e indirectos, así como la coerción y el engaño. Muchas estrategias de guerra cibernética parecen intrínsecamente asimétricas, cuando la infraestructura computarizada de un país sumamente desarrollado y poderoso, se vuelve más vulnerable por las consecuencias de un ataque cibernético con éxito. Sin embargo, vale la pena recordar, que la explotación de percepciones erróneas es una característica central de las estrategias asimétricas. En vista de que la guerra cibernética es una característica común del entorno estratégico global, los Estados que dependen de redes informáticas complejas estarán muy conscientes de su vulnerabilidad. Es posible prever que en un futuro cercano, las redes informáticas serán vistas a través del mismo

prisma utilizado por los portadores de aviones en la actualidad, herramientas tecnológicas poderosas pero vulnerables, que deben ser cuidadosamente protegidas contra ataques.

Al igual que en otros aspectos del conflicto humano, un pequeño subconjunto de las estrategias ciberespaciales serán verdaderamente asimétricas. Es probable que sea demasiado reciente en la historia de la guerra cibernética para sacar conclusiones definitivas acerca de cuáles estrategias serán empleadas, cómo evolucionarán y cómo será la guerra asimétrica en el ciberespacio. Sin embargo, se puede señalar algunas características un poco generales, pero útiles.

Imagínese a un oponente que ha desarrollado una vasta capacidad de guerra cibernética, empleando gran cantidad de militares y personal de inteligencia y sistemas computarizados, y utiliza dicha capacidad para lanzar un ataque de negación de servicio a gran escala contra las redes computarizadas de las fuerzas armadas de Estados Unidos. Presuma que el ataque cibernético es concebido para debilitar nuestra capacidad de mando y control durante una campaña aérea y naval que cubre grandes distancias, permitiendo a las fuerzas enemigas, de otra forma superadas, organizar una defensa más eficiente. Si bien, en sentido general, el ataque convertiría una fortaleza estadounidense en una debilidad, los medios de ataque en el ciberespacio son el equivalente a una penetración profunda de fuerzas blindadas en tierra, donde la fuerza se concentra y se utiliza contra un punto vulnerable cuidadosamente seleccionado. Un ataque como este puede lograr el efecto sorpresa y conmoción, sin embargo no es asimétrico.

En contraste con este tipo de ataque, otro tipo hipotético de ataque contra las redes estadounidenses, se lleva a cabo para lograr objetivos similares. Sin embargo, en este caso, suponga que el ataque se lleva a cabo usando una red de personal civil, empleados gubernamentales y computadoras militares de todo el mundo. En la mayoría de los casos, es probable que el objetivo no sepa que se está produciendo el ataque, asumiendo además que esta red es creada y controlada por un grupo de personas empleadas de forma clandestina por el Estado infractor. En este escenario, cuatro o cinco individuos podrían

ocasionar un serio daño al ejército más poderoso del mundo. Presentan varias debilidades aparentes: no están armados, conforman un pequeño grupo y cuentan relativamente con pocos recursos. Sin embargo, esas debilidades aparentes le proveen al atacante el anonimato y la posibilidad de negación de responsabilidad, indispensable para sobrevivir y ejecutar ataques. La eficacia de estos ataques cibernéticos surge de su capacidad para transformar un aparente punto fuerte estadounidense— las fuerzas armadas estadounidenses de tecnología avanzada, cuidadosamente sincronizada— en una debilidad.

El potencial para un ataque de este tipo es demostrado por la saga del infame gusano informático *Conficker* (también denominado *Downup*).³⁹ Al igual que otros programas maliciosos, el *Conficker* está concebido para insertarse en una computadora que da servicio a otras conectadas a ella sin revelar su presencia, haciendo pequeños cambios, necesarios para defenderse y evitar la detección y luego extenderse a otros sistemas. También se mantiene en constante comunicación por Internet con su creador anónimo y puede seguir instrucciones. Este programa malintencionado apareció por primera vez el 20 de noviembre de 2008 y desde entonces, ha sobrevivido con éxito varios intentos, sin precedentes, de destruirlo por parte de una red coordinada global de expertos en seguridad. Actualmente, este gusano controla una *botnet*— o red de equipos infectados, que posiblemente está compuesta de millones de computadoras de todo el mundo, operados en gran parte por usuarios completamente crédulos. Esta *botnet* da al gusano y a su controlador un enorme poder computarizado, el cual puede ser potencialmente usado para llevar a cabo ataques debilitantes hasta en las redes más grandes y seguras del mundo. Para cualquier organización, incluso un Estado, un *botnet* estable como el controlado por *Conficker* representa una poderosa capacidad ofensiva disponible.

El diseño y las adaptaciones subsiguientes de *Conficker* indican que fue concebida por un equipo de personas con gran experiencia en distintas disciplinas, incluso la criptografía y el diseño de *software*. Según los expertos en seguridad cibernética que han estudiado

Foto: Tnte 2º Chris Harper, 5º Regimiento/1ª División del Cuerpo de Inf. Mar. de EUA



Un infante saluda a niños de la región durante su patrulla junto con soldados del Ejército Nacional Afgano, 18 de diciembre de 2011.

este gusano, los creadores de *Conficker* son “ya sea criminales cibernéticos con tecnología increíblemente avanzada o un grupo que fue financiado por un Estado- Nación.⁴⁰ Los creadores de *Conficker* permanecen en el anonimato y no se sabe si el gusano está controlado por un Estado. Sin embargo, puede ser significativo señalar que la versión original de *Conficker* fue concebida para evitar infectar cualquier computadora con una dirección en Internet ucraniana.⁴¹

La combinación del potencial ofensivo y negación de responsabilidad ofrecidos por un *botnet* controlada anónimamente por *Conficker*, es sencillamente demasiado atractivo para que pase desapercibido por un actor estatal. Tales capacidades representan algunas de las amenazas peligrosas e importantes emergentes para Estados Unidos y sus aliados y de ninguna manera son armas exclusivas para el débil. Especialmente en combinación con la guerra híbrida y otras estrategias asimétricas tratadas en este artículo, la guerra cibernética puede ofrecer a los futuros adversarios de Estado Unidos una ventaja potencialmente transformadora. En manos de un fuerte actor estatal con acceso a gran caudal

intelectual y conocimientos técnicos, la guerra cibernética puede resultar devastadora.

Manipulación de los medios de comunicación

A menudo, los estadounidenses consideran sus robustos medios de comunicación como una ventaja estratégica; hasta los adversarios de Estados Unidos han llegado a percibir los medios de comunicación del mismo, como un beneficio estratégico. Por ejemplo, durante la guerra fría, la Unión Soviética emprendió la restricción al acceso de sus ciudadanos a los medios de comunicación occidentales, mientras que Estados Unidos intentó derrotar la censura soviética. Sin embargo, lo opuesto no fue el caso— los medios de comunicación soviéticos fueron muy ineficaces para influir en el público estadounidense y Estados Unidos no hizo grandes esfuerzos para censurarlo. Una dinámica generalmente similar persiste hoy en día entre Estados Unidos y varios de sus rivales, con la censura de los medios de comunicación estadounidenses que van desde extrema en el caso de Corea del Norte, hasta medidas más sutiles, en el caso de China.

Sin embargo, algunos opositores se han dado cuenta de que los medios de comunicación estadounidenses también pueden constituir una debilidad en determinadas condiciones. Los medios de comunicación de Estados Unidos están presentes en todo el mundo, transmitiendo un punto de vista estadounidense a las familias; sin embargo, el mismo alcance global y ambición por parte de los medios de comunicación con base en Estados Unidos, permite una perspectiva extranjera sobre la política exterior del país que llega a la audiencia estadounidense. Lo más importante es que la cobertura de los medios de comunicación estadounidenses provee a sus ciudadanos puntos de vista, a menudo, limitados pero sumamente irracionales del impacto inmediato diario que tienen las políticas de Estados Unidos, muchas de las cuales requieren un compromiso popular a largo plazo para lograr el éxito.

El efecto que surte es especialmente problemático para los líderes estadounidenses, cuando el país se involucra en un conflicto armado con un oponente más débil, una situación que el estatus de superpotencia de Estados Unidos hace muy probable. El problema es que un gran desequilibrio en la fuerza produce serios asuntos morales y éticos para la parte beligerante más fuerte, cuya fortaleza, confianza en sí mismo y voluntad para combatir, son continuamente socavados. De manera especial, Martin Van Creveld compara esta dinámica de “paradoja de fortaleza” con una situación en la que un hombre adulto enfrenta a un pequeño niño, quien lo ataca con un cuchillo— prácticamente, nada de lo que pueda hacer el adulto parecerá ser débil ni atroz para un observador.⁴² Cuando los ciudadanos estadounidenses observan a sus propias fuerzas armadas en situaciones similares, los mismos tienden a reaccionar de manera negativa.

A menudo, esta dinámica constituye más un simple hecho de la vida que una estrategia empleada por los adversarios de Estados Unidos. Por ejemplo, las reacciones ante la gráfica cobertura de los medios de comunicación acerca de los impactantes ataques aéreos de las fuerzas de la coalición contra las tropas iraquíes en retirada, en el año 1991, contribuyeron, en gran medida, al cese de fuego, lo que permitió que gran parte de la Guardia Republicana Iraquí se escapara. Tan beneficioso como resultó ser para el régimen

iraquí, no hay evidencia alguna que sugiera que los líderes del país pretendieron que sucediera o incluso, que supieran que estaba sucediendo. De manera similar, la formulación silenciosa y centralizada de la política exterior disfruta de cierta ventaja en cuanto a la cultura de Washington de constante filtración de información, incluso, sin que China haga algo para beneficiarse de este aspecto del proceso de formulación de política estadounidense.

Sin embargo, otros actores, han sido más calculadores en sus intentos de darle forma a la cobertura que reciben en Estados Unidos. El uso de celebridades estadounidenses como portavoces para Vietnam del Norte, a fin de destacar las supuestas atrocidades que comete Estados Unidos, es un ejemplo infame, sin embargo, las estrategias más recientes han sido tanto más sutiles como eficaces. Hubo momentos en que los insurgentes iraquíes modernos exhibieron una comprensión sumamente sofisticada de los medios de comunicación global, al coordinar ataques que coincidieran con la cobertura de los medios de la zona blanco y hasta sincronizaron los principales ataques para beneficiarse de la programación de los noticieros centrales estadounidenses. Muchos de los adversarios militares de Estados Unidos, incluyendo al ex Gobierno de Irak e insurgentes iraquíes, han demostrado una excepcional capacidad para dirigir las cámaras de televisión a incidentes de bajas civiles. Al mismo tiempo, Irán pareciera haber prestado suficiente atención a la cobertura de los medios estadounidenses y a la opinión pública para destacar su programa nuclear, alternándose entre una postura conciliadora y una actitud rebelde, para evitar provocar una fuerte reacción estadounidense o hacer concesiones legítimas. En total, lo que una vez pudo haber sido, un debilitamiento de Estados Unidos a través de la cobertura de sus medios de comunicación, cada vez más pareciera haberse convertido en una opción estratégica deliberada de los adversarios de Estados Unidos— y, en especial, una opción asimétrica que transforma un pilar de una sociedad libre en un elemento problemático de formulación de política exterior.

El hecho de que un Estado extranjero manipule la opinión pública estadounidense en cuanto a la política exterior influyendo a los medios de comunicación, resulta más fácil

decirlo que hacerlo. Sin embargo, cuando la estrategia funciona, los resultados pueden ser sumamente favorables para un adversario. Por ejemplo, fueron las imágenes televisadas de las bajas estadounidenses lo que condujo al retiro de las tropas estadounidenses de Somalia, a principio de los años 90 y no una victoria militar lograda por los comandantes militares de Mogadicio.⁴³ Los intentos de manipular a los medios de comunicación representan una estrategia asimétrica potencialmente poderosa, revirtiendo el poder de los influyentes medios de comunicación de EUA para afectar a los mismos estadounidenses.

Qué podemos considerar “hacerles”

Estados Unidos debe estar preparado para responder a las estrategias asimétricas utilizadas en su contra por una variedad de enemigos, desde insurgencias localizadas hasta insurgencias regionales potencialmente hegemónicas. Además, Estados Unidos debe considerar hacer algo menos reactivo y más innovador: necesita crear sus propias estrategias asimétricas. En general, esto no ha sido nuestro enfoque hasta el presente. Prácticamente, Estados Unidos ha asegurado a potenciales adversarios que responderá ante sus acciones solo de manera específica, bien definida, reaccionaria y muy controlada.⁴⁴ En algunos aspectos, esto es una consecuencia de la postura del país como el principal avalador de la estabilidad mundial. Sin embargo, Estados Unidos puede ir más allá de su habitual réplica simétrica y luego demostrar su superioridad sobre las capacidades de los opositores sin arriesgar el rol global que juega.

Las estrategias asimétricas ofrecen una serie de ventajas a Estados Unidos. Las mismas suelen ser económicas, ya que pueden eludir la necesidad de igualar las capacidades clave de un oponente con sus propias capacidades. A menudo, la asimetría produce considerables sorpresas estratégicas, por lo menos temporalmente, permitiendo que el usuario obtenga y explote la iniciativa, mientras que el oponente lucha para reevaluar la situación. Lo más fundamental es: el descubrimiento por parte de un oponente en cuanto a que su fortaleza también es, en cierto sentido, una debilidad paralizante que puede producir gran confusión.

La incertidumbre que suelen generar las estrategias asimétricas las hacen profundamente inquietantes para sus objetivos, lo que conlleva a la confusión acerca de las relativas fortalezas de los adversarios, la viabilidad de las actuales defensas, el uso de las actuales opciones de respuesta, e incluso, la validez de la base de su propio poder. Este poder para desestabilizar y confundir a un blanco, tal vez explica la frecuente asociación de las estrategias asimétricas con el terrorismo, ya que los efectos descritos son precisamente los que buscan los terroristas cuando emprenden sus ataques. Como hemos visto, no hay nada acerca de las motivaciones o debilidades relativas de los terroristas que los haga ser los usuarios exclusivos o hasta más eficaces de la estrategia asimétrica.

Así como un fuerte y calificado luchador puede emplear las técnicas de *jujutsu* para arrasar a un enemigo físicamente más débil, los Estados fuertes pueden emplear las estrategias asimétricas para obtener resultados decisivos contra adversarios más débiles. Tal vez, esto es más o menos lo que Thornton tiene en mente al decir: “queda mucho por decir en cuanto a la idea de que el poderoso tiene que parecerse más a los débiles para igualar sus capacidades”.⁴⁵ Lo que en este artículo proponemos no es que Estados Unidos elabore sus propias y singulares estrategias asimétricas. Estas estrategias surgirán de las propias capacidades singulares estadounidenses. Fundamentalmente, deben ser consecuentes con el carácter moral y posición de liderazgo global del país.

En un escenario mundial con un creciente número de adversarios fuertes y débiles, Estados Unidos haría bien examinar las ventajas del enfoque asimétrico. Evidentemente, no sugerimos que haya una solución asimétrica para todo problema estratégico, ni que la misma se considere una estrategia eficaz o razonable por el simple hecho de ser asimétrica. La actual adopción global de asimetría por actores estatales y no estatales deberá ofrecer a los estrategas estadounidenses, una pista de los posibles beneficios de tal pensamiento. De hecho, si bien el poder de Estados Unidos es enorme, no es infinito. A medida que busca complementar su propio poder mientras confronta una serie de rivales cada vez más fuertes, Estados Unidos haría bien en devolver las fortalezas de los opositores contra ellos mismos. **MR**

REFERENCIAS BIBLIOGRÁFICAS

1. Lambakis, Steven, Kiras, James y Kolet, Kristin, "Understanding 'Asymmetric' Threats to the United States." *Comparative Strategy* 21, núm. 4 (2002): págs. 241-277. Específicamente en la página 241: "'Asymmetry' is a term... [que] contribuye a la confusión en la comprensión de las actuales amenazas y distorsiona el pensamiento sobre los problemas de seguridad que encara el país".
2. Es importante distinguir entre los conflictos asimétricos, que son las interacciones cuya asimetría es un simple hecho derivado de algún tipo de discrepancia entre las partes beligerantes y las estrategias asimétricas, las cuales son deliberados intentos de moldear las interacciones. Estos últimos constituyen el foco de este artículo.
3. Norton-Taylor, Richard, "Asymmetric Warfare." *The Guardian*, 3 de octubre de 2001, <http://www.guardian.co.uk/world/2001/oct/03/afghanistan.socialsciences> (visitada el 16 de junio de 2011), y Gray, Colin S., "Thinking Asymmetrically in Times of Terror." *Parameters*. Vol. 32, núm. 1 (primavera de 2002): págs. 5-14. "Excluding the shared American and Soviet cold war concept of MAD—mutually assured destruction—all warfare has been asymmetric, says Phillip Wilkinson of King's College, London," Norton-Taylor (2001). Una declaración similar se encuentra Gray (2002), p. 14: "all of America's wars have been asymmetrical contests"; "all warfare is asymmetrical."
4. Meigs, Montgomery C., "Unorthodox Thoughts about Asymmetric Warfare." *Parameters* 33, núm. 2 (verano de 2003): págs. 4-18; Steven Metz y Douglas V. Johnson II, *Asymmetry and U.S. Military Strategy: Definition, Background, and Strategic Concepts* (Carlisle, PA: Strategic Studies Institute, 2001). Metz y Johnson, p. 1. La comparación con esta definición es similar, aunque más compleja, en Meigs, p. 4: "Asymmetry means the absence of a common basis of comparison in respect to a quality, or in operational terms, a capability."
5. Barnett, Roger W., *Asymmetrical Warfare: Today's Challenge to U.S. Military Power* (Washington, DC: Brassey's, 2003), p. 15.
6. Thornton, Rod, *Asymmetric Warfare: Threat and Response in the 21st Century* (Cambridge: Polity Press, 2007), p. 1.
7. Lambakis, Kiras, y Kolet, "Understanding 'Asymmetric,'" p. 242. Una definición similar propuesta por Lambakis, Steven J., "Reconsidering Asymmetric Warfare," *Joint Forces Quarterly*, núm. 36 (2004): págs. 102-108. En la página 102 Lambakis dice: "Asymmetry typically describes an enemy that thinks or acts differently from America, especially when faced with conventionally superior U.S. forces."
8. Thornton, *Asymmetric Warfare*, p. 55. Thornton se aproxima a esa formulación, pero —según lo discutido anteriormente— también ofrece otras variaciones: "The turning of strengths into vulnerabilities is obviously what the asymmetric warrior is looking for."
9. *Ibid.*, p. 3.
10. U.S. Joint Chiefs of Staff, *Joint Warfare of the Armed Forces of the United States* (Washington, D.C.: Joint Chiefs of Staff, 1995), IV-10.
11. Thornton, *Asymmetric Warfare*, p. 27.
12. Lambakis, Kiras, y Kolet, "Understanding 'Assymmetric,'" p. 253.
13. Thornton, *Asymmetric Warfare*, págs. 4-5. Thornton observa que vale la pena señalar que las técnicas asimétricas también pueden ser empleadas por el más fuerte, a continuación destaca que la importancia de la actual amenaza asimétrica notes —de tanto actores estatales como no estatales. También consulte la página 76: "The real threat... is from the weak state asymmetric adversary." Why is the "real threat" not from the strong state asymmetric adversary?
14. Liang, Qiao y Xiangsui, Wang, *Unrestricted Warfare: China's Master Plan to Destroy America* (Dehradun: Natraj Publishers, 2007), p. 115.
15. En la práctica, evidentemente, la fuerza relativa a veces está realmente correlacionada con los blancos de las estrategias asimétricas, a medida que los actores se debilitan junto a las dimensiones tradicionales deben buscar formas creativas para enfrentar a los rivales más fuertes, para tener alguna oportunidad de ganar. Sin embargo, además no hay una relación entre la debilidad objetiva del actor y su decisión de emplear una estrategia asimétrica, no hay nada intrínseco sobre la debilidad relativa en el concepto de asimetría: en su lugar, la asimetría se trata de revelar los puntos fuertes de un adversario como una debilidad, convirtiendo su propia aparente debilidad en una ventaja, incluso si en sí, uno es el partido más fuerte.
16. Thucydides, *The Landmark Thucydides: A Comprehensive Guide to the Peloponnesian War*. Robert B. Strassler, ed. (New York: The Free Press, 1976), p. 43.
17. Huntington, Samuel P., *The Clash of Civilizations and the Remaking of World Order* (New York: Simon & Schuster, 1996), p. 187.
18. Hoffman, Frank G., *Conflict in the 21st Century: The Rise of Hybrid Wars* (Arlington, VA: Potomac Institute for Policy Studies, 2007); Simpson, Erin M., "Thinking about Modern Conflict: Hybrid Wars, Strategy, and War Aims" Paper presented at the annual meeting of the Midwest Political Science Association, Palmer House Hilton, Chicago, Illinois, 7 de abril de 2005, p. 3. Disponible en http://www.allacademic.com/meta/p84945_index.html (visitada el 6 de junio de 2011). El término "Guerra híbrida" también ocasionalmente se utiliza para describir los conflictos que afectan tanto a la guerra intraestatal como a la interestatal, en lugar de una fusión de métodos convencionales e irregulares empleados por una de las partes beligerante.
19. Hammes, Thomas X., *The Sling and the Stone: On War in the 21st Century* (St. Paul, MN: Zenith, 2004); Smith, Rupert, *The Utility of Force: The Art of War in the Modern World* (London: Penguin Books, 2005); Kilcullen, David, *The Accidental Guerrilla: Fighting Small Wars in the Midst of a Big One* (Oxford: Oxford University Press, 2009). Estos libros proporcionan un análisis más detallado de la insurgencia y su dinámica evolución.
20. La insurgencia patrocinada por el Estado por medio de un representante, tal como la campaña de los norvietnamitas contra el Sur a través del Vietcong es otra cuestión. Además, cabe señalar que Vietnam del Sur terminó siendo derrotado por una invasión militar convencional y no por las actividades llevadas a cabo por la insurgencia.
21. Kilcullen, David, *The Accidental Guerrilla*. Campañas insurgentes expedicionarias del Che Guevara en América Latina y la estrategia de al-Qaeda para insertarse en las insurgencias locales y regionales, tal como los talibanes, pueden presentar una excepción a esta regla. Sin embargo, tanto el Che y al-Qaeda dependían fuertemente de interlocutores locales y utilizaron de forma masiva la mano de obra local en sus campañas.
22. Mao Tse-Tung, *On Guerrilla Warfare*, trans. S.B. Griffith (Chicago: University of Illinois Press, 1961).
23. Hoffman, Frank G., *Conflict in the 21st Century*, p. 8, p. 29. Hoffman define la guerra híbrida como aquellas en la que los métodos convencionales e irregulares son empleadas por las mismas fuerzas en el mismo teatro de operaciones, lo que permite un agama mucho más amplia de posibles estructuras de fuerza y métodos en su definición. Si bien el uso más directo del concepto es un modelo con base en una infantería descentralizada y ligera, hay otros ejemplos.
24. Exum, Andrew, *Hizballah at War: A Military Assessment* (Washington, DC: The Washington Institute for Near East Policy, 2006), p. 1, disponible en <http://www.washingtoninstitute.org/pubPDFs/PolicyFocus63.pdf> (visitada el 16 de junio de 2011).
25. *Ibid.*, p. 5. Resulta revelador que la guerra del 2006 estallara cuando Hezbolá tendió una emboscada a una patrulla israelí y secuestró a dos militares de las Fuerzas de Defensa Israeli; Biddle, Stephen y Friedman, Jeffrey A., *The 2006 Lebanon Campaign and the Future of Warfare: Implications for Army and Defense Policy* (Carlisle, PA: Strategic Studies Institute, 2008), p. 29.
26. Exum, Andrew, *Hizballah at War*, págs. 4-7.
27. Biddle y Friedman, *The 2006 Lebanon Campaign*, págs. 35-36. En este artículo se proporciona una útil "taxonomía" del comportamiento militar de Hezbolá durante el conflicto de 2006.
28. *Ibid.*, p. xv.
29. Andrew Exum, *Hizballah at War*, p. 7
30. *Ibid.*, p. 6.
31. Krepinevich, Andrew; Watts, Barry y Work Robert, *Meeting the Anti-Access and Area-Denial Challenges* (Washington DC: Center for Strategic and Budgetary Assessments, 2003). "Assassin's Mace" itself is essentially a cocktail of mutually supporting asymmetric strategies, including undersea mining, cyberattacks and anti-satellite strikes as well as guided missile attacks.
32. Rusling, Matthew, "Shifting Gears: For the Military, a Future of 'Hybrid' Wars." *National Defense* 93 (September 2008): págs. 32-34.
33. Billo, Charles; Welton, Chang. *Cyber Warfare An Analysis of the Means and Motivations of Selected Nation States* (Institute for Security Technology Studies at Dartmouth College, 2004), págs. 25-40, disponible en <http://www.ists.dartmouth.edu/docs/cyberwarfare.pdf> (visitada el 16 de junio de 2011).
34. *Ibid.*, p. 107-119.
35. *Ibid.*
36. Project Goose, Grey, *Russia/Georgia Cyber War – Findings and Analysis* (17 de octubre de 2008), disponible en <http://www.scribd.com/doc/6967393/Project-Grey-Goose-Phase-I-Report> (visitada el 16 de junio de 2011).
37. Billo y Chang, *Cyber Warfare*.
38. Gray, Colin S., "The 21st Century Security Environment and the Future of War." *Parameters* 38, núm. 4 (invierno de 2008), págs. 23-24.
39. Mark Bowden, "The Enemy Within," *The Atlantic*, June 2010, 72-83.
40. *Ibid.*, p. 82.
41. *Ibid.*, p. 77.
42. Van Creveld, Martin, *The Transformation of War* (New York: The Free Press, 1991), págs. 173-179.
43. Johnson, Dominic D. P. y Tierney, Dominic, *Failing to Win: Perceptions of Victory and Defeat in International Politics* (Cambridge: Harvard University Press, 2006), págs. 205-241.
44. Barnett, *Asymmetrical Warfare*, p. 154.
45. Thornton, *Asymmetric Warfare*, p. 148.