ieee.es
Instituto Español de Estudios Estratégicos

Documento
Análisis

33/2013 29 mayo de 2013

María José Caro Bejarano

PODER BLANDO FRENTE A PODER DURO EN EL CIBERESPACIO

PODER BLANDO FRENTE A PODER DURO EN EL CIBERESPACIO

Resumen:

El predominio del ciberespacio se puede hacer mediante su control aplicando estrategia del poder duro o mediante estrategias de poder blando. Ningún país puede imponerse en Internet fuera de sus fronteras. Existe un debate sobre aplicar expansionismo o proteccionismo en el ciberespacio, como medio de poder que también sirva para promocionar la prosperidad económica de un país.

Abstract:

Cyberspace dominance may be achieved applying control through strategies of hard power or soft power. No country can impose on the Internet outside its borders. There is debate over applying expansionism or protectionism in cyberspace as a means of power that also serves to promote the national economic prosperity.

Palabras clave:

Ciberespacio, poder duro, poder blando, expansionismo, proteccionismo, tecnologías de la información y la comunicación.

Keywords:

Cyberspace, hard power, soft power, expansionism, protectionism, communication and information technologies.

PODER DURO O PODER BLANDO EN EL CIBERESPACIO

Las estrategias de seguridad en los distintos espacios comunes o global commons como tierra, mar, aire y espacio se han debatido entre aplicar una u otra alternativa: hard power o soft power, es decir, emplear el control de un dominio o espacio por la fuerza o usar el llamado poder blando para dominarlo. En el caso del dominio del ciberespacio se plantea el dilema de cuál de los poderes utilizar.

Algunos autores han buscado una similitud entre los dominios del mar y el ciberespacio[1] a la hora de aplicar estrategias sobre un dominio pasado, el mar, a otro emergente, el ciberespacio.

De igual manera que en el pasado la fuerza naval se debatió entre aplicar el proteccionismo y el expansionismo, este dilema también puede aplicarse al ciberespacio. En el caso de EE.UU. la estrategia naval de Mahan[2] consideraba la misma como un mecanismo, no sólo de defensa de las costas, sino como un medio de poder para promocionar la prosperidad económica del país. Su estrategia permitió a este país alcanzar ambos objetivos simultáneamente, este enfoque permitió la expansión económica y como segundo efecto alejó el conflicto de las costas de EE.UU.

Al ciberespacio se le puede aplicar un desafío similar: el dilema entre el expansionismo y el proteccionismo. Una estrategia expansionista para el ciberespacio podría proporcionar un crecimiento económico y una seguridad similar a la obtenida con el enfoque de Mahan de poderío marítimo hace un siglo.

El origen tecnológico del ciberespacio radica en el interés y la inversión gubernamental de EE.UU. El embrión del ciberespacio fue la red Arpanet creada por encargo del Departamento de Defensa (DOD) y que comenzó como un medio de comunicación dentro de la Universidad de California y que años después fue el origen de la red Internet. Sin embargo, de este espacio gubernamental, este nuevo dominio saltó y se expansionó rápidamente hacia el ámbito comercial y de negocios. El interés y la defensa de los intereses económicos en el ciberespacio es un objetivo compartido con el dominio marítimo.

[1] *From Sea Power to Cyber Power. Learning from the Past to Craft a Strategy for the Future*. By Kris E. Barcomb.
[2] Alfred Thayer Mahan, historiador y estratega naval estadounidense. Sirvió en la Marina durante la Guerra de Secesión, presidente del Colegio de Guerra Naval de Newport en Rhode Island. Influyó en la doctrina marítima de Estados Unidos con su obra de 1890: *The Influence of Sea Power upon History*, *1660-1783* para el desarrollo de una Armada potente y muy operativa.

La aplicación del poder duro al ciberespacio, como defendía Mahan para el dominio marítimo, no es claramente trasladable a este nuevo espacio, donde se aplica más el poder blando. En el ciberespacio las estrategias que se centran en el establecimiento de relaciones, el funcionamiento y la legitimidad son más efectivas que las basadas en el empleo de la fuerza. Para triunfar en un mundo interconectado hay que pensar en términos de atracción y cooptación en lugar de órdenes.

El ciberespacio también ofrece una facilidad de acceso mayor que cualquier de los cuatro dominios mencionados anteriormente. Los intereses comerciales dominan el ciberespacio, donde ejercen una influencia basada en el mérito. Por tanto, la convergencia y la simplicidad son componentes clave en un análisis del ciberespacio. En ambos casos, el poder marítimo y el poder cibernético están íntimamente ligados a la promoción del crecimiento económico. Sin embargo, también existen diferencias. Las entidades comerciales ejercen mayor influencia sobre la tecnología del ciberespacio que los gobiernos, y el poder y la influencia en el ciberespacio se basa en la atracción y cooperación, más que en el dominio, y el fácil acceso al ciberespacio precisa un modelo de seguridad descentralizado.

PUNTOS ESTRATÉGICOS A APLICAR AL CIBERESPACIO

Ahora bien, aunque Mahan aplicaba al poder marítimo dos principios estratégicos de convergencia y concentración, el ciberespacio es descentralizado por su propia naturaleza, aunque también posee algunos aspectos de concentración.

En este sentido se recogen siete puntos estratégicos de concentración a aplicar al ciberespacio: sistemas operativos, motores de búsquedas, infraestructuras de comunicaciones físicas, informática en la nube, foros de gobernanza, criptografía y protocolo de Internet versión 6 IPv6.

El sistema operativo a utilizar es el primer punto estratégico. Aunque el ciberespacio es un dominio distribuido y carece de una autoridad centralizada, una única compañía ejerce una tremenda influencia mundial en el campo de los ordenadores. El sistema operativo Microsoft Windows domina el 92% del mercado mundial, mientras que Mac OS de Apple abarca un 6% y Linux se contenta con un escaso 1%[3]. Y a pesar de las quejas sobre fallos de seguridad y restricciones de funcionalidad de los productos de Microsoft, es una compañía

[3] Según datos del informe "Desktop Operating System Market Share, disponible en http://marketshare.hitslink.com

estadounidense la que lidera este mercado, y sujeta a las leyes y normas culturales de ese país.

También las compañías de esta nacionalidad dominan el mercado global en el campo de los sistemas operativos de los teléfonos móviles: Google Android 70%, Apple iOS 21%, Research in Motion 3%, Microsoft 3%, Nokia Symbian 1%[4], etc. Desde el punto de vista de la seguridad, se da una preponderancia del software procedente de compañías estadounidenses.

El segundo punto estratégico se centra en los motores de búsqueda o buscadores, que ejercen una enorme influencia sobre las ideas. Es una forma de ejercer el poder blando que mencionaba Joseph Nye. Estos motores atraen a los usuarios por su rendimiento superior y aunque se pueden usar muchos y diferentes buscadores hay uno que predomina: Google. Una única compañía domina el 83% del mercado mundial, seguido de lejos por Yahoo, Bind y el chino Baidu[5]. Los algoritmos de búsqueda de Google devuelven resultados para los usuarios indexando sobre un billón de direcciones de internet. Como la gente generalmente solo revisa los primeros tres a cinco resultados, esto permite a Google ejercer una capacidad, sin precedentes históricos, de moldear las preferencias. Más de 1.000 millones de veces al día decide Google lo que es o no es importante en Internet. Esto es una muestra del poder blando. De esto se percató China cuando mantuvo una disputa con la compañía. China quería censurar los resultados de las búsquedas de Google en territorio chino y se iniciaron ataques a las infraestructuras de Google, que cedió y reubicó sus servidores en Hong Kong, a costa de perder poder de influencia en beneficio del buscador gubernamental Baidu que sirve a una comunidad de 400 millones de usuarios chinos y domina el mercado de buscadores en China.

Esta posición dominante de EE.UU. en sistemas operativos y buscadores se mantiene por los principios económicos que promueven el crecimiento y la innovación.

El tercer punto estratégico son las infraestructuras de comunicaciones físicas, en concreto, aquellos sistemas que soportan la red troncal de Internet. Un puñado de empresas o proveedores de servicios de Internet, controlan el núcleo de las comunicaciones del ciberespacio. Hasta hace poco todo el tráfico de Internet pasaba por las infraestructuras de EE.UU. Desde el punto de vista de la seguridad esta situación está cambiando rápidamente

[4] Según datos del informe "Gartner Says Worldwide Mobile Phone Sales Declined 1.7 Percent in 2012" de febrero de 2013, disponible en http://www.gartner.com/newsroom/id/2335616.
[5] Según datos del informe "Desktop Search Engine Market Share" de abril de 2013, disponible en http://www.netmarketshare.com/search-engine-market-share.aspx?qprid=4&qpcustomd=0

debido al menor coste de las tecnologías de la información y a la mayor preocupación por la protección de las comunicaciones electrónicas. Esto hace que otras naciones tengan sus propias redes troncales de comunicaciones para evitar el paso por las infraestructuras de EE.UU. En este sentido el Patriot Act aprobado por el Congreso que permita monitorizar las ciberactividades de carácter perverso, ha tenido como efecto colateral el desvío del tráfico fuera del control de EE.UU. con lo que disminuye la influencia sobre las rutas de las comunicaciones mundiales.

El cuarto punto estratégico es la informática en la nube. Esta infraestructura permite ejercer cierta influencia sobre la tendencia actual de centralizar el procesamiento y almacenamiento en la web. Los proveedores de servicios en la nube como Amazon, Microsoft y Google permiten a los usuarios ubicar estos servicios en servidores externos. Se trata de un mercado emergente en el ciberespacio, pero creciente; cada vez más datos viajarán a las infraestructuras de unos pocos proveedores, lo que supone un punto de concentración estratégico. Las compañías líderes actuales también son estadounidenses, pero en un futuro cercano datos de ciudadanos estadounidenses podrían estar ubicados en servidores fuera de sus fronteras legislativas, como ya sucede con ciudadanos de otros países. En este sentido, EE.UU. aboga por desarrollar estos servicios en regiones que estén cubiertas por la jurisdicción nacional, incentivar la política fiscal y continuar participando en organismos elaboradores de estándares, como el NIST, National Institute of Standards and Technology.

El quinto punto estratégico es la gobernanza. Esta es más una cuestión cultural que un medio de control, o no, según se mire. Existen distintos consorcios constituidos por las partes interesadas que trabajan juntos para elaborar los estándares de comunicación en el ciberespacio, algunos de ellos son el IEEE (Electrical and Electronics Engineers), ITU (International Telecommunications Union), W3C (World Wide Web Consortium), IANA (Internet Assigned Numbers Authority) y otros muchos que desarrollan un papel integral en moldear las características del ciberdominio. La participación en estos foros ayuda a establecer la dirección de estos organismos de gobierno.

El sexto punto estratégico es la criptografía. La matemática subyacente está en los fundamentos de la seguridad del ciberespacio. Si fallaran los modernos métodos de asegurar los datos, el motor completo de la economía se vendría abajo. Desde 1972 el NIST coordinado con la NSA, National Security Agency, prueban y certifican los estándares criptográficos que dejan a disposición pública. Esta actividad tiene también un impacto económico que se valoraba ya en 1200 millones de dólares en 2001[6]. Con el crecimiento

[6] Véase National Institute of Standards and Technology, "Planning Report 01-2: The Economic Impacts of NIST's Data Encryption Standard (DES) Program," October 2001, disponible en www.nist.gov/director/planning/upload/report01-2.pdf

exponencial del comercio electrónico sin duda esta cifra se ha superado con creces. La criptografía representa por tanto, otro elemento de poder blando en el ciberespacio puesto que ningún gobierno puede dictar la implementación fuera de sus propias redes. El proceso abierto y competitivo del NIST al definir los estándares atrae a las entidades privadas de seguridad que reconocen el valor de este proceso.

El desarrollo de la informática cuántica se enclava dentro de la categoría criptográfica que está en proceso de investigación y desarrollo. Los ordenadores cuánticos podrían debilitar las bases fundamentales de seguridad del cifrado moderno. Esta tecnología aún está inmadura pero a cualquier país le conviene estar a la cabeza de esta próxima generación de tecnología informática.

El séptimo y último punto estratégico es el protocolo de Internet versión 6, IPv6, siguiente generación del protocolo actual IPv4, fundamento del enrutamiento en Internet. IPv4 comenzó en 1981 y puede gestionar hasta 4.000 millones de direcciones de Internet. Aunque es una cifra considerable, ya se sobrepasó en febrero de 2011. Existen barreras económicas para adoptar IPv6 aunque haya incentivos financieros para adoptar este nuevo estándar. China presiona para hacer lo mismo. Ya ha desarrollado un programa para implementar el estándar en su próxima generación de arquitectura de Internet. Con el potencial de más de 400 millones de usuarios de Internet, China puede ejercer una influencia importante sobre el estándar, las implementaciones hardware y los foros de gobierno. Está en juego el papel preponderante de EE.UU. para influir en esta pieza crítica de Internet.

CONCLUSIÓN

Aunque un país no puede dictar la dirección de la economía global general, sí que puede dar pasos para facilitar el crecimiento de las empresas privadas en el ciberespacio y por ello, mantener o mejorar su liderazgo en puntos clave estratégicos de este dominio.

Al seleccionar, priorizar y capitalizar los sitios estratégicos del mundo electrónico se podría asegurar la influencia de un país en el ciberespacio, en este caso, de EE.UU. como sucedía en la defensa de las costas de un país; la seguridad táctica en el ciberespacio puede emerger como una función de proyectar el ciberpoder en esos puntos claves, al tiempo que se facilita el crecimiento económico.

El poder blando se antepondrá al poder duro en el ciberespacio en el futuro previsible. Tendrán más éxito las estrategias dirigidas a atraer y cooperar que las que intenten controlar

mediante la fuerza. Esto limita el papel del poder militar en el ciberespacio pero no invalida la necesidad de programas y políticas gubernamentales adaptadas. Un excesivo intento de controlar puede hacer más daño que beneficio. Si se ejerce el poder blando en los siete puntos estratégicos del ciberespacio, se podrá alcanzar el expansionismo y la seguridad al mismo tiempo. Para ello se necesita una política fiscal adaptada, la colaboración con la empresa privada y la investigación y desarrollo priorizados para ejercer el poder en el ciberespacio en el siglo XXI.

María José Caro Bejarano
Analista Principal IEEE