ieee.es
Instituto Español de Estudios Estratégicos

Analysis
Report

33/2013 29th May 2013

María José Caro Bejarano

CYBERSPACE: HARD POWER VS. SOFT POWER

This document has been translated by a Translation and Interpreting Degree student doing work experience, IGNACIO CUEVAS MARTÍNEZ, under the auspices of the Collaboration Agreement between the Universidad Pontificia Comillas, Madrid, and the Spanish Institute of Strategic Studies.

CYBERSPACE: HARD POWER VS. SOFT POWER

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.

Keywords:

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

CYBERSPACE: HARD POWER VS. SOFT POWER

The security strategies in the various spaces or global commons as land, sea, air and space have been discussed between applying one or another alternative: hard power and soft power, i.e. employ control over one domain or space through coercion or use the so-called soft power to dominate it. Regarding the control of cyberspace there is a dilemma on which of the powers to use.

Some authors have sought a similarity between the domains of sea and cyberspace[1] when applying strategies on this old domain, the sea, to an emerging one, the cyberspace.

Just as the navy was torn between applying protectionism and expansionism in the past, this dilemma also applies to cyberspace. In the case of U.S. Mahan's naval strategy [2], this was considered as a means not only of coastal defense, but also as a mean of power to promote economic prosperity. This strategy allowed the country to reach both goals simultaneously, this approach allowed for economic expansion and, as a second effect, it distanced the conflict away from U.S. shores.

We can take a similar approach in the case of cyberspace: the dilemma between expansionism and protectionism. An expansionist strategy in cyberspace could provide an economic increase and a similar security to that obtained with Mahan's approach over sea power a century ago.

The cyberspace technological origin lies in the interest and investment of the U.S. government. The embryo of cyberspace was the Arpanet network, commissioned by the Department of Defense (DOD), which began as a communication tool within the University of California and years later originated the beginning of the Internet. However, this government space, this new domain, expanded quickly to the commercial and business area. The interest and defense of economic interests in cyberspace is a shared goal with the maritime domain.

A hard power approach to cyberspace, as argued by Mahan for the maritime domain, is not clearly transferable to this new space, where soft power is generally applied. In cyberspace,

[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, a U.S. naval historian and strategist. He served in the Navy during the Civil War, President of the Naval War College in Newport Rhode Island. Influenced the U.S. maritime doctrine with his work, 1890: The Influence of Sea Power upon History, 1660-1783 for the development of a powerful and highly operational Navy.

the strategies that focus on relationship building, operating and legitimacy are more effective than those based on the use of force. To succeed in an interconnected world, we must think in terms of attraction and cooptation[3] rather than orders.

Cyberspace also provides easier access than any of the four domains mentioned above. Business interests dominate the cyberspace, where they have a considerable impact based on merit. Therefore, convergence and simplicity are key components in a cyberspace analysis. In both cases, the maritime power and cyber power are intimately linked to the promotion of economic growth. However, there are some differences. Commercial entities have greater influence over cyberspace technology than governments. Power and influence in cyberspace are based on attraction and cooperation, rather than in the domain, and easy access to cyberspace requires a decentralized security model.

KEYPOINTS APPLICABLE TO CYBERSPACE

Now, while Mahan applied two strategic principles of convergence and concentration to maritime power, cyberspace is decentralized by nature, while maintaining some aspects of concentration.

At this point, we regard seven concentration strategic points applicable to cyberspace: operating systems, search engines, physical communications infrastructure, cloud computing, governance forums, cryptography and Internet Protocol Version 6 IPv6.

The operating system used is the first strategic point. Although cyberspace is a distributed domain and lacks a centralized authority, a single company has a tremendous global influence in the field of computers. The Microsoft Windows operating system holds 92% of the world market, while Apple's Mac OS accounts for about 6% and Linux settles with a meager 1%[4]. Despite several complaints about security failures and limited functionality of Microsoft products, it is a U.S. company the one leading this market, along with the laws and cultural norms of this country.

Also, other U.S. companies dominate the global market in the field of mobile phones operating systems: Google Android 70%, Apple iOS 21%, Research in Motion 3%, 3%

[3] En el original en español, la palabra que aparecía era *cooptación,* aunque está palabra la he traducido como tal, me parece que la autora tenía la intención de referirse a la *cooperación*, ya que concuerda con el sentido del texto y se repite en lo sucesivo. En este caso, la formulación de la oración no variaría, este sería el resultado: "we must think in terms of attraction and cooperation rather than orders."

[4] According to the report "Desktop Operating System Market Share", available at http://marketshare.hitslink.com

Microsoft, Nokia Symbian 1%, etc.… From a security point of view, there is preponderance of software coming from U.S. companies.

The second strategic point focuses on the search engines, which have an enormous influence on the ideas. It is a way of applying the soft power that Joseph Nye mentioned. These engines attract users for its superior performance and although there is a vast range of search engines, there is one that stands out: Google. A single company holds 83% of the world market share, followed distantly by Yahoo, Bind and the Chinese Baidu[5]. The Google search algorithms return results to the users by indexing over one trillion Internet addresses. Since people generally only go through the first three or five search results, this allows Google to shape the preferences, a feature with no historical precedent. Over 1,000 million times a day, Google decides what is or is not important on the Internet. This is an example of soft power. China realized this when they held a dispute with the company. China wanted to censor Google search results in Chinese territory and launched attacks against Google infrastructure. The company relinquished and relocated its servers in Hong Kong. The cost of this action was the loss of power to influence in favor of government sponsored search engine Baidu, which provides service to a community of 400 million users and leads the search engine market in China.

The economic principles that promote growth and innovation are the major causes for the U.S.'s dominant position in the operating systems and search engines market.

The third strategic point is physical communications infrastructures, in particular, those systems that support the Internet backbone. Just a handful of companies or Internet service providers, control the communications core of cyberspace. Not that long ago, all Internet traffic passed through the U.S. infrastructure. From a security point of view, this situation is shifting quite rapidly due to the lower cost of information technologies and the increasing concern for the protection of electronic communications. In consequence, other nations create their own communications backbones to prevent their Internet traffic from going through the U.S. infrastructure. In this sense, the Patriot Act passed by Congress, that allows the monitoring of cyber activities of vicious character, has had the side effect of diverting traffic away from the U.S. control thereby decreasing influence over global communications routes.

Cloud computing is the fourth strategic point. There is a current trend to centralize the processing and online storage, cloud computing infrastructure allows to hold some influence over this kind of activities. Providers of cloud services such as Amazon, Microsoft and Google

[5] According to the report "Desktop Search Engine Market Share", April2013, available at http://www.netmarketshare.com/search-engine-market-share.aspx?qprid=4&qpcustomd=0

allow users to locate these services on external servers.

This is an emerging market in the cyberspace, but also a growing one; more and more data infrastructures will travel to a few suppliers, which is a strategic rallying point. The current leading companies are also American, but in the near future data of U.S. citizens could be located on a server outside legal boundaries, as it already happens with citizens in other countries. In this sense, the U.S. supports developing these services in regions that are covered by the national jurisdiction, encourages fiscal policy and continue to participate in organisms responsible for standards, such as NIST, National Institute of Standards and Technology.

The fifth strategic point is governing. It is more of a cultural matter than a form of control, or not, depending on the point of view. There are various consortiums set up by concerned parties that work together to develop communication standards in cyberspace, some of them are the IEEE (Electrical and Electronics Engineers), ITU (International Telecommunications Union), W3C (World Wide Web Consortium), IANA (Internet Assigned Numbers Authority) and many others that develop and integral role in molding the features of the cyber domain. Participation in these forums helps establish the direction of these government bodies.

The sixth strategic point is cryptography. The underlying mathematics is found in the foundation of cyberspace security. If the modern methods of securing data failed, the whole engine of the economy would collapse. Since 1972 NIST, in collaboration with NSA, National Security Agency, test and certify the cryptographic standards available to the public. This activity also has an economic impact that was already valued at 1200 million dollars in 2001[6]. With the exponential growth of e-commerce this figure has undoubtedly exceeded. Therefore, cryptography represents another element of soft power in cyberspace since no government can dictate the implementation outside their own networks. The open and competitive process in NIST when defining standards attracts security private entities that recognize the value of this process.

The development of quantum computing is nestled within the cryptographic category that is under research and development. Quantum computers could weaken the fundamental bases of security of the modern encryption. This technology is still undeveloped, however, it is in a country's best interest to lead this next generation of computer technology.

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

The seventh and final strategic point is the Internet protocol version 6, IPv6, subsequent generation of the current protocol IPv4, the basis of Internet routing. IPv4 began in 1981 and can manage up to 4,000 million Internet addresses. In spite being a considerable amount, it was surpassed in February 2011. There are economic barriers to adopt IPv6 although there are financial incentives to implement this new standard. China is pressuring to do the same. It has developed a program to implement the standard in the next generation of their Internet infrastructure. With the potential of more than 400 million Internet users, China can exert an important influence over the standard, the hardware implementations and the government forums. At stake is the prevailing role of the U.S. to influence this critical piece of Internet.

CONCLUSSIONS

Although a country cannot dictate the direction of the global economy, it can take steps to enable the growth of private enterprises in cyberspace and thus maintain or improve their leadership in strategic key points of this domain.

By selecting, prioritizing and capitalizing the strategic points of the electronic world, it becomes clear the influence of one country in cyberspace, in this case, the U.S. As in a country's coast defense, tactical security in cyberspace may come from the projection of cyber power on these key points, while enabling economic growth.

Soft power will succeed over hard power in cyberspace in the foreseeable future. Attraction and cooperation strategies will overcome those that apply force in order to control. This limits the role of military power in cyberspace while maintaining the need for adapted government policy and programs. Attempting to exert an excessive control may cause more harm than good. If soft power is applied in these seven strategic areas of cyberspace, expansionism and security will be reachable at the same time. This requires an adapted fiscal policy, collaboration with private companies and the prioritization of research and development priority to exercise power in cyberspace in the XXI century.

María José Caro Bejarano
Analista Principal IEEE