# From Sea Power to Cyber Power

## Learning from the Past to Craft a Strategy for the Future

*By* KRIS E. BARCOMB


U.S. Navy (Gary Nichols)

**U.S. Navy cryptologic technicians preview Integrated System for Language Education and Training program at Center for Language, Regional Expertise, and Culture, Pensacola, Florida**

*Naval strength involves, unquestionably, the possession of strategic points.*

—Alfred Thayer Mahan

Alfred Thayer Mahan saw the ocean for what it is. While it spans the globe and covers a predominant portion of the Earth, not all parts of it are equally important. Mahan offered a focused naval strategy in an era when America was struggling to define itself as either isolated from, or an integral part of, the larger international community. The force structure of the U.S. Navy hinged upon leaders deciding between protectionism and expansionism. Rather than simply a mechanism to defend the coasts, Mahan envisioned the Navy as a powerful means for promoting American economic prosperity. In one sense, his strategy allowed the Nation to achieve both objectives simultaneously. By projecting naval power at key points around the globe, Mahan's approach allowed for economic expansion and had the second-order effect of pushing conflict away from U.S. shores.

Cyberspace represents a similar challenge. The United States now faces a contemporary struggle between expansionism and protectionism in this domain. We can learn a great deal from Mahan's methodology for delineating and prioritizing the sea domain into actionable terms. Thus, this article identifies strategic categories in cyberspace by adopting Mahan's approach. In doing so, it seeks to identify similarities and differences between sea power and cyber power. The aim is to provide senior leaders with a better understanding of the salient aspects of cyberspace, offer insights for securing those points, and suggest a new paradigm for the proper role of the military in this domain. This tailored expansionist strategy for cyberspace should provide the United States with both economic growth and security akin to Mahan's approach to sea power a century ago.

**Major Kris E. Barcomb, USAF, is a Cyberspace Strategist for 24th Air Force at Lackland Air Force Base, Texas.**

## A Mahanian Approach to Cyberspace

Mahan did not view the Navy as an end unto itself, but as a key component of the larger economic welfare of the Nation. He tied the very existence of the Navy to commerce when he wrote, "The necessity of a navy, in the restricted sense of the word, springs, therefore, from the existence of a peaceful shipping, and disappears with it."[1] Similarly, while cyberspace originated through U.S. Government investment, the domain owes its rapid expansion and modern character to commerce. In this sense, sea power and cyber power share a common objective. They both primarily exist to protect economic interests within their respective domains.

*sea power and cyber power both primarily exist to protect economic interests within their respective domains*

Two principles guided Mahan's analysis. First, Mahan looked for strategic points of convergence and concentration. He stated, "In general . . . it will be found that by sea, as by land, useful strategic points will be where highways pass, and especially where they cross and converge."[2] As a result of his foresight and the willingness of key U.S. leaders to act on it, such as President Theodore Roosevelt, American influence secured the Hawaiian Islands, the Philippines, Guantanamo Bay, Puerto Rico, and the Panama Canal, to name a few. Despite both the realities and perceptions of the decentralized nature of cyberspace, careful inspection reveals several points of concentration.

Second, Mahan emphasized the need to minimize the total number of points considered important to communicate priorities and overcome resource constraints: "The search for and establishment of leading principles—always few—around which considerations of detail group themselves, will tend to reduce confusion of impression to simplicity and directness of thought, with consequent facility of comprehension."[3] In accordance with these two principles, this article identifies seven strategic points of concentration in cyberspace: operating systems (OSs), search engines, physical communications infrastructure, cloud computing, governance forums, cryptography, and Internet Protocol version 6 (IPv6).

Each of these categories has unique challenges, and some are more established than others. Fortunately, the United States holds dominant roles in many of these categories, such as operating systems and search engines, and it must define strategies to maintain those positions. In others, such as physical communications infrastructure and cloud computing, the United States has played a leading role in their early development, but the future share of influence is still uncertain. Here, more proactive measures must be taken to help assert U.S. influence.

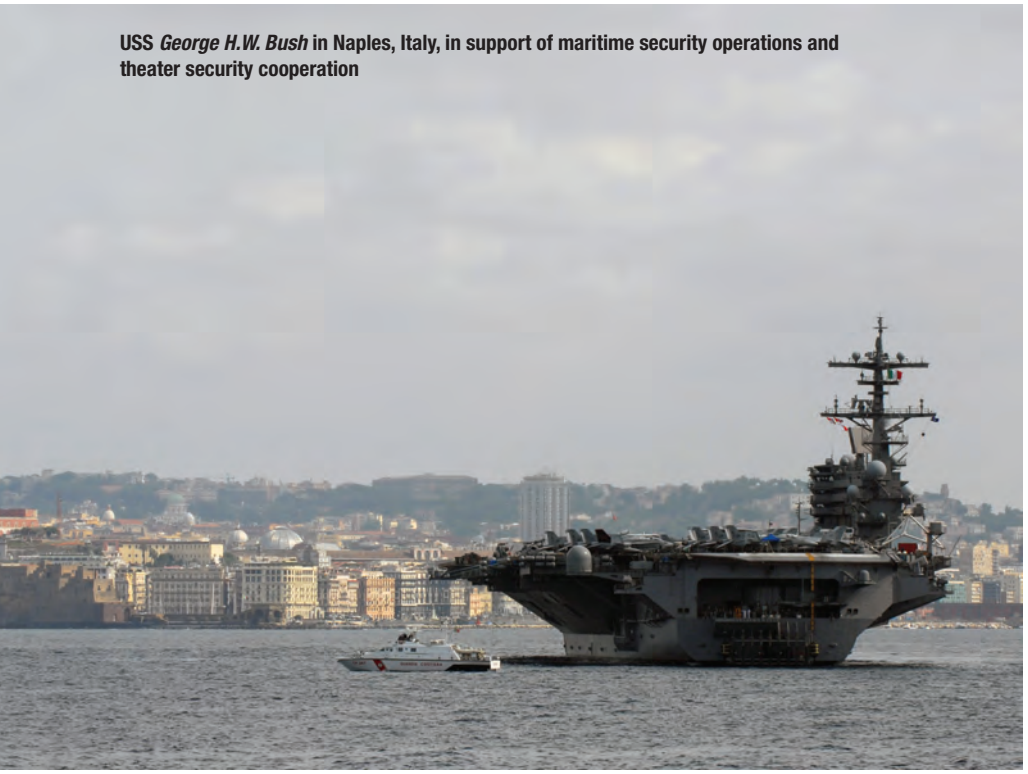
## Key Differences

Before continuing with a detailed review of each category, it is important to evaluate the salient differences between the nature of the sea and the essence of cyberspace. First, while the government played a key role in helping establish the technological foundations of the Internet, commercial interest quickly surpassed the government in terms of influence over the domain. Martin Libicki, a senior policy analyst at the RAND

Corporation, succinctly described the current state of government influence: "As it is, the days when governments were leading-edge consumers and manipulators of information technology are long past. . . . Man for man, it cannot compete with Microsoft."[4]

The second important difference is the relationship between hard and soft power in each domain. Mahan emphasized hard power, and he viewed the threat or use of force as foundational to protecting maritime interests. He also tied sea power to command when he asserted, "These national and international functions can be discharged, certainly, only by command of the sea."[5] Yet his view of command and the role of force do not translate well into cyberspace, where soft power plays a predominant role. In cyberspace, strategies centered on relationship-building, performance, and legitimacy will be more effective than those based on force. In contrast to Mahan, Joseph Nye stated, "To succeed in a networked world requires leaders to think in terms of attraction and co-option rather than command."[6]

The final differentiator is ease of access. Cyberspace has much lower barriers to entry than the sea. Perhaps this key difference will lead to a devolution of norms with respect to the proper role of government and military in protecting private interests in cyberspace.



USS *George H.W. Bush* in Naples, Italy, in support of maritime security operations and theater security cooperation

U.S. Navy (Betsy Lynn Knapper)

While Western navies were expanding the sphere of European influence, events in the East were unfolding differently. In 1433, in an attempt to inhibit the link between military and commercial enterprises, the Chinese imperial court halted naval expeditions. Then, in 1436, the Chinese government banned the construction of new seagoing ships.[8] Because the Chinese economy was only allowed to function within the narrow limits defined by the government, commerce failed to expand, thereby allowing European interests to dominate the global economy for centuries.[9] Europeans recognized that they could not control the outcome of the economy as a whole. Instead, they established policies to facilitate economic growth. In contrast, China's attempt to control its economy too tightly led to its decline. Given that commercial interests dominate cyberspace, and influence is based largely on merit, the United States must act more like the Europeans than the Chinese of the middle ages.

So far, we have established convergence and simplicity as key components of a Mahanian-style analysis for cyberspace. We have also established how the proper employment of both sea power and cyber power is intimately linked to promoting economic growth. Yet the two also have important differences. Commercial entities wield more influence over cyberspace technology than governments, power and influence in cyberspace are based on attraction and cooperation rather than command, and low barriers to entry into cyberspace likely require a decentralized security model.

## Seven Strategic Points in Cyberspace

The first strategic point is operating systems. While cyberspace is distributed and lacks a centralized authority, a single company has tremendous influence over nearly every desktop computer on the planet. Microsoft Windows commands 92 percent of the global market share, followed by Apple's Mac OS at a distant 6 percent, and Linux trailing at only slightly more than 1 percent.[10] In real numbers, this equates to over 1.25 billion computers running versions of the Windows OS.[11] Despite the complaints about security flaws and functionality restrictions in Microsoft product offerings, the United States can be thankful that Microsoft is a U.S.-based company subject to its own laws and cultural norms.

Similarly, U.S. companies currently dominate the global market share of mobile operating systems, although not to the degree of concentration seen in the desktop market. The breakdown of the top four companies is Google Android at 43 percent, Nokia Symbian 22 percent, Apple iOS at 18 percent, and Research in Motion at 12 percent (Microsoft carries less than a 2-percent share).[12] The U.S. position in the mobile OS space is a relatively recent development. Nokia ceded the top spot in 2010 as a result of the transformation of cellular phones from simple voice communication devices to "smart phones."[13]

From a national security standpoint, even if the government or military cannot directly control the software powering the bulk of the world's desktop and mobile devices, it is far better to at least have the preponderance of software come from a U.S.-based company. Imagine if we woke up tomorrow and 92 percent of the world's personal computers ran on an operating system designed by a strategic competitor to the United States. We would quickly wish for the good old days of Microsoft.

Search engines are the second strategic point in cyberspace. While operating systems define the technical performance characteristics of systems, search engines exert tremendous influence over ideas. In many ways, they embody Nye's concept of soft power; they must attract users through superior performance, and the results they return are a powerful form of agenda-setting and preference-shaping. Most users can easily switch from one search engine to another, yet they often choose only one: Google. The company commands 91 percent of the global market share for search.[14] Google's search algorithm returns what it believes are the most relevant matches to a user's request from its index of over 1 trillion unique URLs.[15] Since people generally only review the top three to five results, the company wields historically unprecedented ability to shape preferences. Over 1 billion times every day, Google decides what is and is not important across the Internet.[16] *That* is power.

The struggle for control of this strategic point in cyberspace has already begun. For example, China and Google have had a public dispute over the Chinese government's efforts to censor Google's search results within its borders and the government's attempts to hack into Google's infrastructure.[17] In a demonstration of corporate soft power, Google withdrew its search services from mainland China in 2010 and rehosted them in Hong Kong. Google's absence in mainland China opened the door for the government to increase its own authority over Internet searching. The state-run search engine Baidu became a de facto monopoly over the country's 400 million Internet users.[18] Prior to pulling its search engine out of the mainland, Google had over 35 percent of the Chinese market share. As of June 2011, Google's dispute caused them to slip to an 11 percent share, while Baidu rose to over 83 percent of the Chinese search engine market.[19]

To maintain its dominant position in both operating systems and search engines, the United States must continue to adhere to economic principles that promote growth and innovation. It must also be extremely cautious in exerting hard power in either of these categories. For example, antitrust regulation that fostered U.S. competition in the industrial era may now open a door for global competitors to rise to the top. The United States should also guard against mandating controls or censorship within either of these areas. Too much government interference could delegitimize companies such as Microsoft, Apple, and Google and subsequently facilitate the ability of non-U.S. companies to take their place.

*antitrust regulation that fostered U.S. competition in the industrial era may now open a door for global competitors to rise to the top*

A third strategic point in cyberspace is physical communications infrastructure. In particular, this category relates to those physical systems supporting the backbone of the Internet. Only a handful of companies, known as Tier 1 Internet Service Providers, control the bulk of the communications passing through cyberspace. The United States has historically held the majority stake in this category, and until recently, nearly all Internet traffic has been routed through U.S.-owned infrastructure. In an address to Congress in 2006, former Central Intelligence Agency Director Michael Hayden acknowledged this point: "Because of the nature of global telecommunications, we are playing with a tremendous home-field advantage, and we need to exploit that edge."[20]

Unfortunately, from a national security standpoint, this situation is rapidly changing as information technology costs decrease and the legal environment governing the protection of electronic communications grows more uncertain. In this environment, lawmakers must be mindful of unintended effects as nations become increasingly willing to recreate their own communications backbones to reduce the need to pass through U.S. infrastructure. For example, Congress passed the USA PATRIOT Act in part to help monitor nefarious cyber activity, but the law had the unintended consequence of driving that traffic to infrastructure outside of U.S. control.[21]

Additionally, some U.S. companies have been shortsighted with regard to expanding their services. After the dot-com bubble of 2000 burst, these companies were either not in a financial position to invest in physical communications infrastructure or were unwilling to take another chance on risky technology. This myopic stance allowed non-U.S. interests to attain those resources and open independently owned and operated communications paths.[22] A more farsighted investment strategy combined with targeted financial incentives could have helped the United States retain the preponderance of ownership.

The fourth strategic point is cloud computing. While physical communications infrastructure established the need to maintain influence over the global communications paths, this category deals with maintaining similar influence over the current trend to centralize processing and storage on the Web. Cloud computing providers such as Amazon, Microsoft, and Google allow users to rent storage and processing capacity on hosted infrastructures. While the current market for this category is relatively small, it is an emerging aspect of cyberspace that will be important in the near future. As the market for cloud services grows, more and more data will flow across the infrastructures of a handful of providers, making it a strategic concentration point in cyberspace.

For now, U.S. companies are the cloud computing market leaders, but that could change. If it does, it could mean that an increasing share of cyberspace data, including that of U.S. citizens, could be hosted on machines operating outside the boundaries of U.S. law. The United States should encourage the development of these services within regions covered by U.S. jurisdiction. It should incentivize U.S. cloud service providers through both appropriate fiscal policy and continue to participate in the governance bodies defining standards for this emerging capability. U.S. Government organizations such as the National Institute

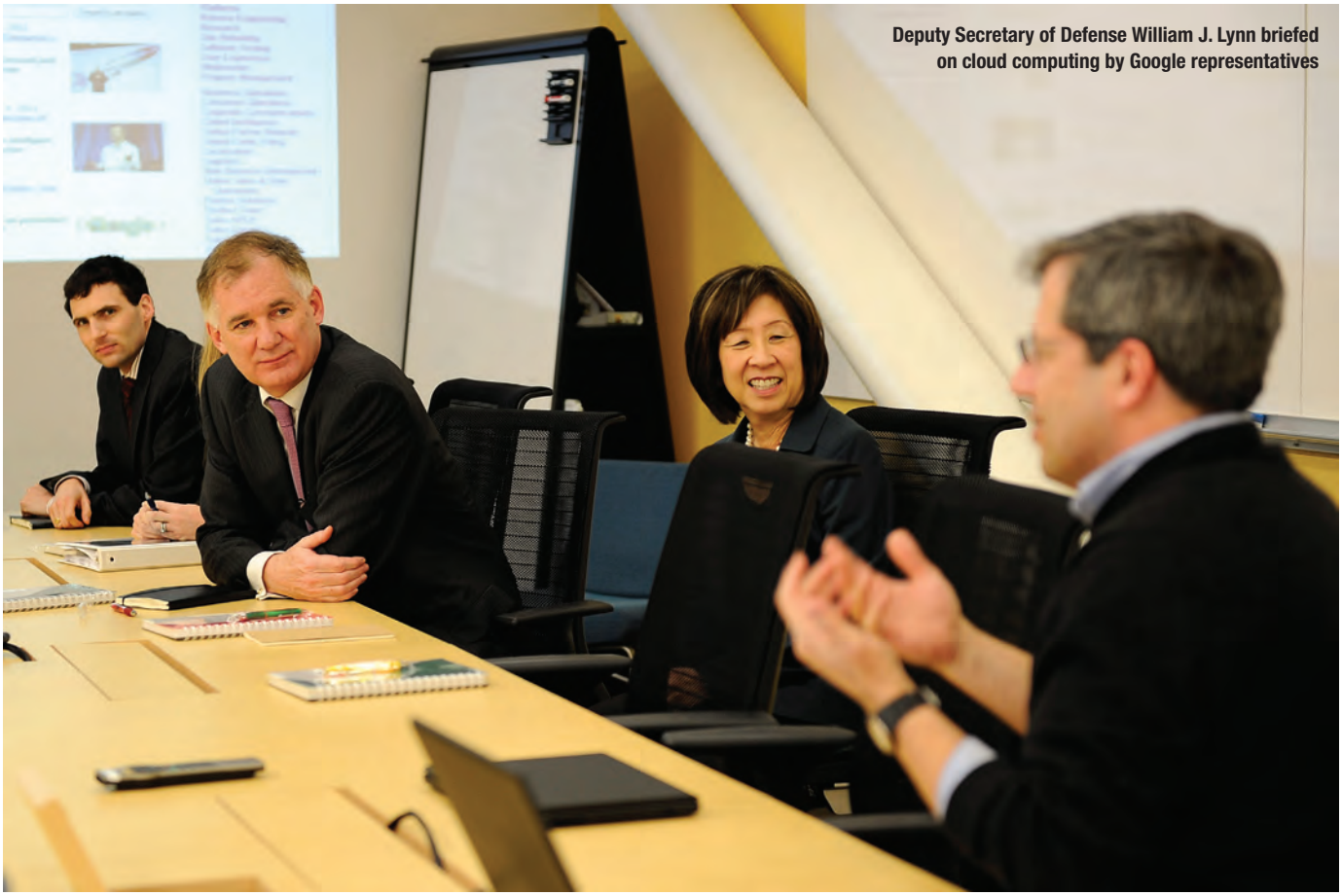
of Standards and Technology (NIST) have performed well in building a foundation of legitimacy and credibility in the cloud computing arena. These kinds of activities need encouragement.

The fifth strategic point is governance forums. Governance in cyberspace is more like a cultural phenomenon than a means of control. There are many consortiums made up of various interested parties that work together to decide the standards for communicating in cyberspace. The Institute of Electrical and Electronics Engineers, International Telecommunications Union, World Wide Web Consortium, Internet Assigned Numbers Authority, and many others play integral roles in shaping the characteristics of the cyber domain. A detailed description of each forum and its relevance to the cyberspace is beyond the scope of this article, but it is enough to emphasize that the United States must make a concerted effort to support, participate with, and help set the direction for these governing bodies.

Another area where NIST has been instrumental in exercising U.S. Government soft power in cyberspace has been in the sixth strategic point, cryptography. The mathematical underpinnings of cryptography provide the foundation of security in cyberspace. If the modern methods for securing data were broken, the entire economic engine of the Internet would crumble almost overnight. Fortunately, the odds of that happening are extremely low because of the NIST's transparent process for defining cryptographic standards. Since 1972, NIST, in coordination with the National Security Agency, has been instrumental in testing and certifying cryptographic standards and making them available to the general public. A 2001 economic assessment determined their efforts had improved the U.S. economy by $1.2 billion as of 2000.[23] While more recent data were not available, given the exponential growth of e-commerce, it seems clear that this number has grown tremendously since then.

The U.S. Government has an important role to play in this field because of the fragility of cryptography when poor practices or design implementations undercut its theoretical foundations. Enigma, the cypher machine used by the German military to encrypt communications during World War II, provides an excellent historical case study to support this point. R.A. Ratcliff describes the negative consequences of decentralizing the management of cryptography and how it undermined the German war effort.[24] A similar problem would arise if individual companies were left to define their own cryptography standards. Cryptography also represents the elements of soft power in cyberspace since the government cannot dictate its implementation outside its own networks. Yet NIST's open, competitive process for defining standards helps attract security conscious private entities that recognize the value of such a process.

The United States must also continue to support research and development efforts into quantum computing as a subset of the cryptography category. Quantum computers have the potential to undermine the fundamental security assumptions of modern encryption. Fortunately, quantum computers are currently too immature to achieve this feat, but when and if they do reach that level of complexity, it is in the best interest of the United States to be at the forefront of this next generation of computing technology.



**Deputy Secretary of Defense William J. Lynn briefed on cloud computing by Google representatives**

U.S. Air Force (Jerry Morrison)

The final strategic point, IPv6 (the next generation standard), is associated with the fundamental routing protocol of the Internet. The current standard, IPv4, was formally defined in 1981, and it has sufficient capacity to handle over 4 billion unique Internet addresses.[25] While this number sounds impressive, all of the available addresses were allocated as of February 3, 2011.[26] There are many economic barriers associated with adopting IPv6, which will dramatically increase the total number of unique Internet addresses. While there are financial incentives for adopting the new standard, many companies are concerned that if they are the first to move to the new space, they will also have to bear the cost of dealing with security or design flaws. This makes adopting IPv6 a classic example of a public good, and therefore the U.S. Government should play a role in helping overcome this critical hurdle.

Another pressing reason to facilitate IPv6 adoption in the United States is China's national push to do the same. China has already developed a substantial program to implement the standard across its next generation of Internet architecture.[27] With over 400 million users and a growing economy, China has the potential to wield significant influence over the IPv6 standard, its hardware implementations, and its governance forums. The United States must take a more proactive role in helping its own commercial interests overcome the adoption hurdles and curtail the possibility of losing the preponderance of influence over this critical piece of the Internet.

## Conclusion

While the United States cannot dictate the direction of the overall global economy, it can take steps to facilitate the growth of American private enterprise in cyberspace and thereby maintain or improve U.S. leadership in the key strategic points of this domain. Securing the ocean's concentration points with sea power helped foster American economic dominance for decades. Similarly, purposefully selecting, prioritizing, and capitalizing on the strategic "locations" of the electronic world could secure American influence in cyberspace. Like coastal defense, tactical security in cyberspace will emerge as a function of projecting cyber power at these key points, while also facilitating economic growth.

Hard power will be secondary to soft power in cyberspace for the foreseeable future. Strategies aimed at attracting and co-opting will be more successful than those attempting to control through force. This limits the role the military will play in cyberspace, but it does not invalidate the need for tailored government programs and policies. The United States must resist the current trend toward protectionism in an effort to maintain the status quo. Excessive attempts to control or exert hard power will likely do more harm than good. Like Mahan's strategy for sea power, if the United States exerts soft power appropriately in these seven strategic points of cyberspace, it will be able to achieve both expansionism and security simultaneously. Through tailored fiscal policy, partnership with private enterprise, and prioritized research and development, the United States will continue to wield cyberspace power in the 21st century. **JFQ**

## NOTES

[1] Alfred Thayer Mahan, *Mahan on Naval Strategy: Selections from the Writings of Rear Admiral Alfred Thayer Mahan*, ed. John B. Hattendorf (Annapolis: Naval Institute Press, 1991), 28.

[2] Ibid., 118.

[3] Ibid., 97.

[4] Martin C. Libicki, *Conquest in Cyberspace: National Security and Information Warfare* (New York: Cambridge University Press, 2007), 281.

[5] Mahan, xx.

[6] Joseph S. Nye, *The Future of Power* (New York: PublicAffairs, 2011), 101.

[7] William H. McNeill, *The Pursuit of Power: Technology, Armed Force, and Society Since A.D. 1000* (Chicago: University of Chicago Press, 1984), 102.

[8] Ibid., 45.

[9] Ibid., 49.

[10] NetMarketShare, "Desktop Operating System Market Share," available at <http://marketshare.hitslink.com>.

[11] Matt Rosoff, "Right Now, There Are 1.25 Billion Windows PCs Worldwide," *Business Insider*, December 6, 2011, available at <http://articles.businessinsider.com/2011-12-06/tech/30481049_1_android-apps-ios>.

[12] "Gartner Says Sales of Mobile Devices in Second Quarter of 2011 Grew 16.5 Percent Year-on-Year; Smartphone Sales Grew 74 Percent," Gartner, August 11, 2011, available at <www.gartner.com/it/page.jsp?id=1764714>.

[13] "The Nokia Story," *Nokia.com*, available at <www.nokia.com/global/about-nokia/company/about-us/story/the-nokia-story/>.

[14] "Browser, OS, Search Engine including Mobile Market Share," *Statcounter.com*, available at <http://gs.statcounter.com/>.

[15] "Our history in depth," *Google.com*, available at <www.google.com/about/company/history.html>.

[16] Steve Lohr, "Google Schools Its Algorithm," *The New York Times*, March 6, 2011, available at <www.nytimes.com/2011/03/06/weekinreview/06lohr.html>.

[17] Nye, 140.

[18] Ibid., 115.

[19] Viet Hoang, "Baidu vs. Google: Is the battle already lost for Google?" February 21, 2012, available at <http://digimind.com/blog/market-industries/infographic-baidu-vs-google-is-the-battle-already-lost-for-google/>.

[20] John Markoff, "Internet Traffic Begins to Bypass the U.S.," *The New York Times*, August 29, 2008, available at <www.nytimes.com/2008/08/30/business/30pipes.html?pagewanted=all>.

[21] Ibid.

[22] Ibid.

[23] National Institute of Standards and Technology, "Planning Report 01-2: The Economic Impacts of NIST's Data Encryption Standard (DES) Program," October 2001, ES-1, ES-3.

[24] R.A. Ratcliff, *Delusions of Intelligence: Enigma, Ultra, and the End of Secure Ciphers* (New York: Cambridge University Press, 2008), 215.

[25] Internet Engineering Task Force, "Internet Protocol: DARPA Internet Program Protocol Specification," September 1981, 7.

[26] ICANN, "Available Pool of Unallocated IPv4 Internet Addresses Now Completely Emptied," February 3, 2011, available at <www.icann.org/en/news/press/releases/release-03feb11-en.pdf>.

[27] Ben Worthen, "Internet Strategy: China's Next Generation Internet CIO.com," *CIO.com*, July 15, 2006, available at <www.cio.com/article/22985/Internet_Strategy_China_s_Next_Generation_Internet>.