THE WALL STREET JOURNAL.
WSJ.com

INFORMATION AGE

February 10, 2013, 4:54 p.m. ET

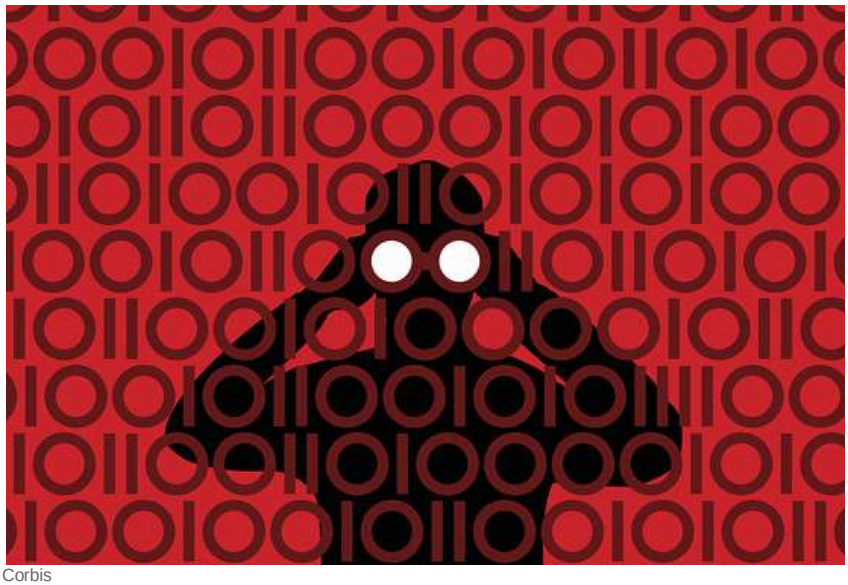
# Confronting Cyber Barbary Pirates

*Secure digital networks are equivalent to the open sea lanes that made global free trade possible.*

By L. GORDON CROVITZ

The Wall Street Journal, New York Times and Washington Post all recently disclosed that their computer systems had been infiltrated by cyber espionage from China. While it's refreshing that Beijing still views newspapers as important enough to hack, they're only the latest targets of such attacks. Foreign governments have worked their way into U.S. communications systems, doing everything from hacking Pentagon plans to stealing corporate intellectual property.

Defense Secretary Leon Panetta warned in October of a "cyber Pearl Harbor" that could endanger the U.S. power grid, transportation network and financial services. In recent years, companies from Google and Yahoo to Lockheed Martin and Northrop Grumman have acknowledged being on the receiving end of attacks. The U.S. Chamber of Commerce in 2011 was surprised when one of its printers began producing Chinese characters. Iran last year hacked Aramco in Saudi Arabia, taking down most of the company's workstations. Russia used cyber warfare against Estonia and Georgia. Last week, cyber spies infiltrated hundreds of thousands of Twitter accounts, getting access to names, email addresses and passwords.



Corbis

Despite years of cyber attacks, the U.S. has done little to confront perpetrators, as Hillary Clinton acknowledges. "We have to begin making it clear to the Chinese," she said in a recent interview

summarizing her time as secretary of state, "that the U.S. is going to have to take action to protect not only our government but our private sector from this kind of intrusion."

The phrase "begin making it clear" underscores the question of what Washington has been saying or doing about years of cyber attacks led or encouraged by foreign governments. Adam Segal wrote last week on the Council on Foreign Relations blog: "It seems fair to say that both sides agree the 'naming and shaming' approach to the problem is not working. The United States can call China out, but it has no real effect on behavior."

Instead of looking for ways to raise diplomatic costs on countries that abuse the Internet by attacking American targets, the first instinct of the White House was to expand Washington's power. That included proposing a "kill switch" that would enable bureaucrats to shut down the Internet. Congress said no.

The lawmakers also balked at regulators mandating security procedures for private companies. Mandates can't keep pace with technological change and would pre-empt innovations to block increasingly sophisticated cyber attacks. Republicans have proposed sensible legislation to make it easier for companies and the government to share information about cyber attacks, including a reduction of the litigation risk when companies acknowledge being victims of break-ins.

So far, most of the attacks have been to subvert communications systems rather than to endanger lives or physical facilities, but because there is no central clearinghouse tracking attacks, the full extent of the problem is unknown. President Obama recently issued directives encouraging federal agencies to help companies when they're attacked, but the top priority should be preventing it from happening in the first place.

It's time for the U.S. to raise the stakes by elevating the importance of secure digital networks and the open Internet. In their 2008 essay "Freedom of the Cyber Seas," published in CSO Magazine, a security trade publication, Energy Department officials Aaron Turner and Michael Assante argued that the U.S. should make open digital networks as much a national priority as open sea lanes.

"In modern times, the nearly ubiquitous availability of powerful computing systems, along with the proliferation of high-speed networks, have converged to create a new version of the high seas—the cyber seas," they wrote. "Nevertheless, for the last decade, U.S. cyber security policy has been inconsistent and reactionary. The private sector has often been left to fend for itself, and sporadic policy statements have left U.S. government organizations, private enterprises and allies uncertain of which tack the nation will take to secure the cyber frontier."

As this column has noted, there's a strong analogy between the open Internet and the open seas. The first time the U.S. military went abroad was to enforce freedom of the seas. President Thomas Jefferson refused to pay the tribute demanded by the Barbary states of what are now Libya and Morocco. The bribe for safe passage of U.S. ships was $1 million, one-tenth of the federal budget. Following a policy of "millions for defense, not one cent for tribute," Jefferson dispatched the Navy,

and the Barbary pirates were defeated. The U.S. Marines still sing about fighting on "the shores of Tripoli."

Global trade across open sea lanes made the Industrial Age possible. In the Information Age, digital networks are the seas. The increasing volume of data carried on these networks has become as critical as goods moved by ship.

No company can act on its own to protect the global digital network any more than clipper ships could force 19th-century pirates to respect freedom of the seas. It will take decisive action by Washington to deter rogue governments from breaching digital networks to read email, steal corporate information or identify news sources.