New York Times
April 3, 2012

How China Steals Our Secrets

By Richard A. Clarke

FOR the last two months, senior government officials and private-sector experts have paraded before Congress and described in alarming terms a silent threat: cyberattacks carried out by foreign governments. Robert S. Mueller III, the director of the F.B.I., said cyberattacks would soon replace terrorism as the agency's No. 1 concern as foreign hackers, particularly from China, penetrate American firms' computers and steal huge amounts of valuable data and intellectual property.

It's not hard to imagine what happens when an American company pays for research and a Chinese firm gets the results free; it destroys our competitive edge. Shawn Henry, who retired last Friday as the executive assistant director of the F.B.I. (and its lead agent on cybercrime), told Congress last week of an American company that had all of its data from a 10-year, $1 billion research program copied by hackers in one night. Gen. Keith B. Alexander, head of the military's Cyber Command, called the continuing, rampant cybertheft "the greatest transfer of wealth in history."

Yet the same Congress that has heard all of this disturbing testimony is mired in disagreements about a proposed cybersecurity bill that does little to address the problem of Chinese cyberespionage. The bill, which would establish noncompulsory industry cybersecurity standards, is bogged down in ideological disputes. Senator John McCain, who dismissed it as a form of unnecessary regulation, has proposed an alternative bill that fails to address the inadequate cyberdefenses of companies running the nation's critical infrastructure. Since Congress appears unable and unwilling to address the threat, the executive branch must do something to stop it.

In the past, F.B.I. agents parked outside banks they thought were likely to be robbed and then grabbed the robbers and the loot as they left. Catching the robbers in cyberspace is not as easy, but snatching the loot is possible.

General Alexander testified last week that his organization saw an inbound attack that aimed to steal sensitive files from an American arms manufacturer. The Pentagon warned the company, which had to act on its own. The government did not directly intervene to stop the attack because no federal agency believes it currently has the authority or mission to do so.

If given the proper authorization, the United States government could stop files in the process of being stolen from getting to the Chinese hackers. If government agencies were authorized to create a major program to grab stolen data leaving the country, they could drastically reduce today's wholesale theft of American corporate secrets.

Many companies do not even know when they have been hacked. According to Congressional testimony last week, 94 percent of companies served by the computer-security firm Mandiant were unaware that they had been victimized. And although the Securities and Exchange Commission has urged companies to reveal when they have been victims of cyberespionage, most do not. Some, including Sony, Citibank, Lockheed, Booz

Allen, Google, EMC and the Nasdaq have admitted to being victims. The government-owned National Laboratories and federally funded research centers have also been penetrated.

Because it is fearful that government monitoring would be seen as a cover for illegal snooping and a violation of citizens' privacy, the Obama administration has not even attempted to develop a proposal for spotting and stopping vast industrial espionage. It fears a negative reaction from privacy-rights and Internet-freedom advocates who do not want the government scanning Internet traffic. Others in the administration fear further damaging relations with China. Some officials also fear that standing up to China might trigger disruptive attacks on America's vulnerable computer-controlled infrastructure.

But by failing to act, Washington is effectively fulfilling China's research requirements while helping to put Americans out of work. Mr. Obama must confront the cyberthreat, and he does not even need any new authority from Congress to do so.

Under Customs authority, the Department of Homeland Security could inspect what enters and exits the United States in cyberspace. Customs already looks online for child pornography crossing our virtual borders. And under the Intelligence Act, the president could issue a finding that would authorize agencies to scan Internet traffic outside the United States and seize sensitive files stolen from within our borders.

And this does not have to endanger citizens' privacy rights. Indeed, Mr. Obama could build in protections like appointing an empowered privacy advocate who could stop abuses or any activity that went beyond halting the theft of important files.

If Congress will not act to protect America's companies from Chinese cyberthreats, President Obama must.

Richard A. Clarke, the special adviser to the president for cybersecurity from 2001 to 2003, is the author of "Cyber War: The Next Threat to National Security and What to Do About It."