

# China's cyberwar

By Editorial Board

**CHINA IS waging a quiet, mostly invisible but massive cyberwar against the United States, aimed at stealing its most sensitive military and economic secrets and obtaining the ability to sabotage vital infrastructure.** This is, by now, relatively well known in Washington, but relatively little is being done about it, considering the enormous stakes involved.

What exactly is happening? Hackers mostly backed by the People's Liberation Army are trying daily to penetrate the computer systems of U.S. government agencies, defense contractors, technology firms, and utilities such as power and water companies — not to mention the private e-mail accounts of thousands of Americans. To an alarming degree, they are succeeding. In recent years hacks have been reported of the State, Defense and Commerce departments; Lockheed Martin; Google, which said its source code and the e-mail accounts of senior government officials were targeted; and the computer security company RSA, which protects critical networks through the SecureID system.

“The computer networks of a broad array of U.S. government agencies, private companies, universities and other institutions — all holding large volumes of sensitive economic information — were targeted by cyber espionage,” said a report issued in October by the Office of the National Counterintelligence Executive. “Much of this activity appears to have originated in China.”

As in the case of other novel and slowly developing threats — international terrorism in the 1990s comes to mind — the U.S. response has been slowed by bureaucratic infighting, poor information-sharing and a failure to prioritize the problem above more familiar business with Beijing. The Pentagon has set up a cyber command, but it has the authority to protect only military networks; the Department of Homeland Security jealously guards its prerogative to guard domestic civilian targets. Government agencies often don't share sensitive intelligence with companies, while many companies are reluctant to report on penetrations of their networks; Google has been a rare exception.

A further difficulty is identifying exactly where cyberattacks originate and connecting them to their government sponsors. Predictably enough, the Chinese government aggressively denies any involvement in the attacks on U.S. agencies and companies — which makes it difficult for diplomats to pressure for a cease-fire. But an encouraging report in the Wall Street Journal this week said that U.S. intelligence agencies had

**managed to identify many of the Chinese groups, and even individuals, involved in the cyberoffensive, including a dozen cells connected to the People’s Liberation Army.**

**This should provide an opportunity for the Obama administration to more directly confront the problem. It should demand that Beijing shut down the military-backed groups; if it does not do so, they could be subjected to countermeasures, including sanctions against individuals. Congress could also consider legislation punishing companies connected to the Chinese military if the cyberwar does not cease. Yes, such responses have the potential to roil relations between Washington and Beijing. But the Chinese offensive — and the economic and national security threats it poses — is simply too important to ignore.**