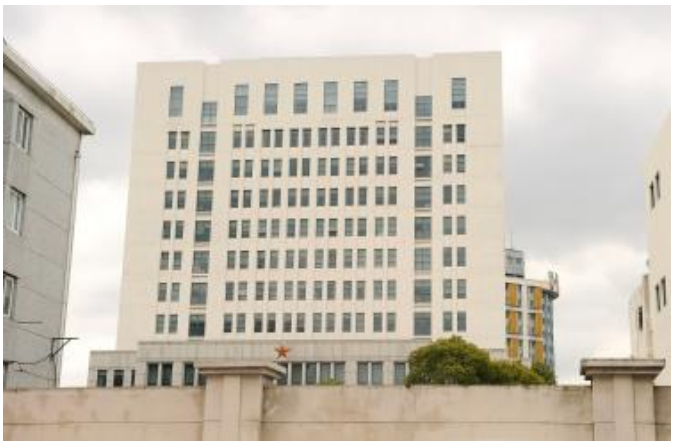

The Internet security firm Mandiant suspects that the white 12-story building photographed yesterday in a northern suburb of Shanghai, China, is the home of a People's Liberation Army-led hacking group.
**Photo: AFP**

China's army controls hundreds if not thousands of virulent and cutting-edge hackers, according to a report issued yesterday by a US Internet security firm that traced a host of cyberattacks to an anonymous building in Shanghai.

Mandiant said its hundreds of investigations showed that groups hacking into US newspapers, government agencies, and companies "are based primarily in China and that the Chinese government is aware of them."

The 74-page report focused on one group, which it called "APT1" from the initials "Advanced Persistent Threat." The *New York Times*, citing experts, said the group was targeting crucial infrastructure such as the US energy grid.

"We believe that APT1 is able to wage such a long-running and extensive cyber espionage campaign in large part because it receives direct government support," Mandiant said.

The group, it said, was believed to be a branch of the People's Liberation Army (PLA) called Unit 61398, and digital signatures from its cyberattacks were traced back to the direct vicinity of a nondescript, 12-story building on the outskirts of Shanghai.

“We believe the totality of the evidence we provide in this document bolsters the claim that APT1 is Unit 61398,” Mandiant said, estimating it is “staffed by hundreds, and perhaps thousands of people.”

China’s Ministry of Defense said its army had never supported any kind of hacking activity, adding: “Not only are reports that China’s army has been involved in hacking unprofessional, they do not fit with the facts.”

“Hacking attacks are a global problem. Like other countries, China also faces the threat of hacking attacks, and is one of the main countries falling victim to hacking attacks,” the ministry said.

The Chinese Ministry of Foreign Affairs also rejected “groundless accusations” of Chinese involvement in hacking.

In its report, Mandiant said that APT1 — known also as “Comment Crew” for its practice of planting viruses on the comment sections of Web sites — has stolen hundreds of terabytes of data from at least 141 organizations spanning 20 industries.

The *Times*, which was given early access to the report, said the researchers had found that the Comment Crew was increasingly focused on companies involved in US infrastructure, including in its electrical power grid, gas lines and water works. It said one target was a company with remote access to more than 60 percent of oil and gas pipelines in North America.

The Comment Crew was also among those that attacked the computer security firm RSA, whose computer codes protect confidential corporate and government databases, the *Times* said.

The building pinpointed as the hacking headquarters sits in the Shanghai suburb of Gaoqiao, near a petrochemical complex and surrounded by small shops. There is no name plate outside, but framed posters showing soldiers are displayed on a high wall surrounding the complex,

while the PLA's symbol of a red star is mounted over the main door of the building.

One soldier in camouflage uniform stood at the main gate yesterday. Another wearing a PLA overcoat was stationed in the guardhouse.

Source: Taipei Times - 2013/02/20