

The New York Times

By RICK GLADSTONE



Iran reported a number of new cyberattacks on Tuesday, saying foreign enemy hackers tried in recent months to disrupt computer systems at a power plant and other industries in a strategically important southern coastal province as well as at a Culture Ministry information center.

Accounts of the attacks in the official press did not specify who was responsible, when they were carried out or how they were thwarted. But they strongly suggested that the attacks had originated in the United States and Israel, which have been engaged in a shadowy struggle of computer sabotage with Iran in a broader dispute over whether Iran's nuclear energy program is for peaceful or military use.

Iran has been on heightened alert against such sabotage since a computer worm known as Stuxnet was used to attack its uranium enrichment centrifuges more than two years ago, which American intelligence officials believe caused many of the machines to spin out of control and self-destruct, slowing the Iranian program's progress.

Stuxnet and other forms of computer malware have also been used in attacks on Iran's oil industry and Science Ministry under a covert United States effort, first revealed in January 2009, that was meant to subvert Iran's nuclear program because of suspicions that the Iranians were using it to develop the ability to make atomic bombs. Iran has repeatedly denied these suspicions.

The latest Iranian sabotage reports raised the possibility that the attacks had been carried out in retaliation for others that crippled computers in the Saudi Arabian oil industry and some financial institutions in the United States a few months ago. American intelligence officials have said they believe that Iranian specialists in cybersabotage were responsible for those attacks, which erased thousands of Saudi files and temporarily prevented some American banking customers from gaining access to their accounts.

Defense Secretary Leon E. Panetta cited those attacks in an Oct. 11 speech in which he warned of America's vulnerability to a coordinated computer warfare attack, calling such a possibility a "cyber-Pearl Harbor."

The Iranian Students' News Agency said the country's Passive Defense Organization, the military unit responsible for guarding against cyberattacks, had battled a computer virus infection of an electric utility and other unspecified manufacturing industries in southern Hormozgan Province, home to a large oil refinery and container port in the provincial capital of Bandar Abbas.

The news agency quoted Ali Akbar Akhavan, the head of the Passive Defense Organization's provincial branch, as saying that "with timely measures and the cooperation of skilled hackers in the province, the progress of this virus was halted." It was unclear whether any Iranian targets had been damaged.

Iran's Fars News Agency said a cyberattack had also been made against the information center of the Headquarters for Supporting and Protecting Works of Art and Culture, a part of the Culture Ministry, and that the attack had been "repelled by the headquarters' experts."

The Fars account said the attack originated in Dallas and was routed to Iran via Malaysia and Vietnam. It did not elaborate on the significance of that information, but noted that a broad array of Iranian targets had recently come under cyberattacks that were "widely believed to be designed and staged by the U.S. and Israel."

News of the latest cyberattacks came as Western economic sanctions on Iran have been tightening, while diplomatic negotiations aimed at resolving the nuclear dispute have remained basically stalled since June. There are expectations that a resumption of those negotiations will be announced soon, possibly next month.