Iranian Cyber Attack on New York Dam Shows Future of War

By Mark Thompson

Published: 2016-03-24 · Archived: 2026-04-06 02:01:50 UTC

The first nationstate warfare took place between soldiers on the ground, and then ships at sea. In the 20th Century, the battles moved into the skies. On Thursday, the Justice Department claimed Iran had attacked U.S. infrastructure online, by infiltrating the computerized controls of a small dam 25 miles north of New York City, heralding a new way of war on American soil.

“We can tell the world that hackers affiliated with the Iranian government attacked U.S. systems, and we seek to bring them to justice for their crimes,” Assistant Attorney General John P. Carlin said, unveiling charges against seven Iranians for cyber attacks. The hackers, members of the Iran’s Islamic Revolutionary Guards Corps, also targeted several financial institutions, the New York Stock Exchange and AT&T with barrages of incoming emails designed to slow or shut down some of their computers, according to the indictment.

Hackers broke into the command and control system of the dam in 2013, apparently through a cellular modem. While 34-year-old Hamid Firoozi should have been able to release water from behind the dam given his remote access, he “did not have that capability because the sluice gate had been manually disconnected for maintenance at the time of the intrusion,” the U.S. government said.

FBI

While insignificant in the overall scheme—the 20-foot, flood-control dam is on Blind Brook in Rye Brook, N.Y.—it signals the desire of some foreign nations to infect, and potentially operate, U.S. infrastructure. “They were sending a shot across our bow,” Senator Charles Schumer, D-N.Y., said of the Iranian probing of the dam earlier

this month. “They were saying that we can damage, seriously damage, our critical infrastructure and put the lives and property of people at risk.”

There is next to no chance the Iranians will end up in U.S. courts. But U.S. officials say the “name and shame” effort is designed to make clear the U.S. knows what happened, and to deter those involved from traveling overseas, where they could be arrested.

The intrusion happened as the U.S. and Iran readied to negotiate a deal curbing Tehran’s nuclear-development program, and followed by two years a massive U.S.-Israeli cyber attack dubbed Stuxnet on Iran’s nuclear centrifuges designed to thwart its atomic ambitions. Some U.S. officials believe the Iranian attacks were in retaliation for the Stuxnet assault.

This isn’t the first time the U.S. has linked cyber attacks to foreign nations. In recent years, the U.S. government publicly accused North Korea of hacking into Sony Pictures Entertainment’s computers and the Chinese military of cyber-attacking several U.S. companies. “The infiltration of the Bowman Avenue dam represents a frightening new frontier in cybercrime,” U.S. Attorney Preet Bharara of the Southern District of New York said Thursday. “These were no ordinary crimes, but calculated attacks by groups with ties to Iran’s Islamic Revolutionary Guard and designed specifically to harm America and its people.”

Much U.S. infrastructure is privately owned and poorly defended, given the lack of a major attack and the resulting reluctance to spend money defending against a putative threat. “These sectors may be particularly vulnerable to cyberattack because they rely on open-source software or hardware, third-party utilities, and interconnected networks,” the Congressional Research Service warns.

The ability to run such systems remotely, as well as conduct maintenance and update software via the web itself, offers hackers all the access they need. Such networks are particularly tempting because they often control operations, and not merely information, potentially magnifying the impact of any attack on them. “Attacks against operations technology are different than information technology attacks because OT attacks can produce kinetic effects”—physical destruction—that CRS report noted with studied understatement.

Given the success of Stuxnet, it should come as little surprise that Iran is engaging in cyber warfare. Tehran is believed to be targeting the controls “that operate and monitor our electrical grid,” a report by the cyber-security firm Norse Corp. and the American Enterprise Institute warned in a 2015 report. “It seems clear that elements within Iran are working to build a database of vulnerable systems in the U.S., damage to which could cause severe harm to the U.S. economy and citizens.”
