Are Terrorists Training at Nuclear Plant? NRC Probes Indian Point Security

Posted: 21 Nov 2013 06:55 PM PST

By Roger Witherspoon

The Nuclear Regulatory Commission is investigating possibly major lapses in security at the Indian Point nuclear power plants, including the prospect that criminal elements are using parts of the plants' emergency drills for their own terrorist training.

Records show that for more than a decade, officials at Indian Point have largely ignored instances where their internal security communications system was compromised and blocked by outside individuals. Whether the deliberate jamming of security communications is a decade-long prank or the result of individuals or groups using Indian Point safety drills as opportunities to test their own ability to cause mayhem during a terrorist attack is not known.

But the fact that deliberate jamming by "an individual or group of individuals" was first reported in 2003 by James Lee Witt in his analysis of emergency planning on behalf of the State of New York and has continued intermittently to the point where it forced the cancellation of emergency drills in November 2012 has prompted an investigation by the NRC.

Indeed, those who have hacked into Indian point's security have lately become so brazen that they have recorded instructions made by plant security officials at the beginning of drills, and then jammed the network's receivers by replaying those instructions over and over, according to participants, thus blocking any further use of the compromised security network. And the electronic intruders were apparently operating within a mile or two of the plant site.

The latest allegations were the most potentially explosive in a series of failures outlined by two former security officers – Lt. Skip Travis and Lt. Jason Hettler – in a suit filed in U.S. District Court in August against Entergy Nuclear , which owns the twin Indian Point plants in Westchester County some 25 miles from Manhattan. A spokesman for Entergy declined to discuss the subject.

There is no evidence in the public NRC record that there have been any problems with security operations or drills at the plant site in bucolic Buchanan, along the banks of the Hudson River about 10 miles south of West Point. The agency's January, 2013 evaluation of Indian Point 2 and 3 gave the plants "green" or top ratings in every category, including security. (**http://www.nrc.gov/NRR/OVERSIGHT/ASSESS/pim_summary.html**)

Indeed, despite a litany of complaints against the security operation at the plant, the NRC has noted but done little about problems delineated in the suit, including:

- The falsification of work logs and fitness for duty reports, thus allowing security personnel to exceed the maximum permitted work hours per week despite being fatigued.
- Jeopardizing the effectiveness of Force on Force drills by informing the security personnel of what routes the "invaders" would take to attack the plant.
- A faulty perimeter detection system, which made it impossible for defenders to know where "terrorists" were breaking into the plant site and where they were on the grounds. As a result of being technologically blind during a drill monitored by the NRC on October 11, 2011, the suit states "all of the 'terrorists' successfully breached the perimeter and the identified target sets located inside of Indian Point and succeeded in causing a total nuclear meltdown. Not one terrorist was killed by any security personnel during the drill."
- A combination of faulty detection equipment and internal communications allowed "terrorists" to succeed in in reaching all of their targets in an NRC-monitored, Force on Force drill in April, 2013. Hettler and Travis contend that had the April drill "been an actual terrorist attack, the 20 million individuals who live and work in the 50-mile radius meltdown zone would have perished."

- An absence of backup power for the internal communications system. As a result, the security force could not communicate during station blackout conditions.

Agency spokesman Neil Sheehan said in an email note that "the NRC is aware of the issues raised in the filing. The agency is evaluating all of the plant safety and security issues described in the lawsuit that are under our jurisdiction. The NRC has an extensive plant oversight program to ensure that facility's owner adequately adheres to federal safety and security requirements."

Ever since the 9/11 terrorist attacks the NRC has had strict rules regarding what is public and what is considered "safeguard" information that cannot be released. According to the official 9/11 Report, Indian Point was scouted and selected as a backup target to the twin towers of the World Trade Center, whose upper floors may have been obscured had the region been blanketed with rain or fog. The Hudson River Flyway serving the region's airports, on the other hand, begins just 500 feet above the water. The twin domes of Indian Point, jutting more than 300 feet in the air in the middle of a bend in the river, would be hard to miss even in bad weather.

Security issues in general and cyber security in particular are subjects that are not discussed with the public by NRC officials. Sheehan added, however, that "I would just note that part of our Reactor Oversight Process involves cyber security reviews. Via those reviews, we would be able to follow up on any earlier problems, including a company's root cause evaluation of an issue."

He could not, however, comment on whether or not the FBI or any other federal law enforcement or security agency had been consulted about the issues raised at Indian Point. A spokeswoman for the FBI said the agency does not confirm or deny participation in any investigations.

There has never been public acknowledgement of any NRC probe into the jamming revealed by the 2003 Witt Report (http://bit.ly/gQjdK3) . There was widespread criticism at the time of Entergy's response that the jamming was irrelevant because the leaders of the

radiation detection teams had a roll of quarters and could find pay phones to call in their findings. That low tech work-around is no longer available.

Andrew Spano

Andrew Spano, who was the Westchester County Executive at the time, said in an interview this week that "Entergy has always handled these drills as if they were just something the company had to do. I don't think they ever took them seriously. I'm not surprised at their current equipment problems. You can never underestimate either incompetency or equipment failure."

The most extensively documented evidence of jamming disrupted a three-day drill held November, 2012 and monitored by NRC security evaluators. Part of the problem, recalled Hettler and Travis during a lengthy interview, lay in the fact that Entergy devises the scenario for the "surprise attacks" and the NRC monitors how well the teams react to the script as it unfolds. Under NRC rules, the participants are not to have any advance knowledge of the script, including where the attackers will break in, how many there are, or what their targets are.

"The drill was messed up from the start," said Travis. "The operators had the script with all of the events, and they kept jumping the gun and getting ahead of the script by sending us to defend an area before the 'attack' had occurred. We had to start over three times."

It was during the fourth try at defending Indian Point from an invading team of terrorists that the jamming began. "Someone was going over the frequency and playing back the drill sergeant's voice," said Travis. "Someone had recorded our earlier conversations and was playing the traffic back on our frequency. They halted the drill and did radio checks, thinking someone on the post was playing fictitious voices over the radio.

"But someone taped those checks and then played it back, jamming us again. Obviously the person was hearing our entire drill in real time and knew everything that was happening. They looked at the electronic identifier of the incoming signal, and could not identify it. It

was not coming from anyone on the base. So we cancelled the drill."

This wasn't the first time signals had been jammed. It has occurred frequently enough that Entergy security officials have their own name for it: "spoofing."

The problem lay with the antiquated equipment used by the security teams. "I have been on many shifts where there was jamming," explained Travis, a 25-year security veteran and a crew leader at Indian Point. "You can't tell anyone where to move because the system is jammed. Our consoles were not the type where you could hit a button and override the incoming signal. The radio communications in our bay stations are the originals that were installed when they built the plants 40 years ago.

"As a result, whoever is on the air owns the airwaves. If an individual opens his mike and tapes it open he owns the frequency till the battery goes dead. You can't cut in. You can't cut him off."

Entergy updated some of the communications equipment towards the end of 2012, added Hettler. "But we continued to have bleeding, where one radio's frequency bleeds over into another frequency. As a result, anyone with a 1,000 Megahertz Jammer – the kind you can buy publicly – can drown out all of the security frequencies at Indian Point. And you don't even have to be onsite to do it."

The problem of outside jamming is compounded by the failure of the plant site's ARINCS detection system, the former security officers said.

"Within the first 15 minutes of going 'hot' the system crashed 14 times," said Travis, "and it has been a failed system since that first night. It crashes whenever there is inclement weather – it's a nonstop problem with respect to that."

In their suit, the two security officers state that "between February 2011 and May 2013, ARINCS has had tens of thousands of 'total failures' wherein the ARINCS computer system froze, surveillance cameras froze, alarms failed to detect movement on the perimeter fence, alarms failed to sound, etc. and ARINCS continues to fail on a regular basis presently."

The combination leaves security guards at Indian Point effectively deaf and blind.

Phil Musegaas

Phil Musegaas, program director for Riverkeeper, an environmental group seeking to close the twin reactors, said Entergy's tolerance of continued jamming is a serious issue that needs to be immediately addressed.

"It's appalling," Musegaas said. "This is a situation where you should assume the worst and get to the bottom of it as quickly as possible when you consider the stakes we are dealing with.

"In any other industry, if there were similar problems in their critical infrastructure, the plant would be shut down and an independent investigation would be conducted and they wouldn't be allowed to operate until their security was proven to be effective. At this point, what is going on there sounds like a laughable situation.

"It would be laughable if it weren't so serious and so dangerous."