An Analysis of the Attack on the Metcalf Substation on April 16th, 2013

Anonymous

July 4th, 2022

Contents

Breaking down the timeline, methodology, investigation, and damage done

Location/date

- The Metcalf Substation is located outside of San Jose, CA in the small, unincorporated community of Coyote. Surrounded by little more than a chain link fence and accessible from only two roads–Monterey Highway and Metcalf Rd.–which intersect in front of the substation. The location is owned and operated by Pacific Gas and Electric (PG&E). This station provides a lot of energy to the Silicon Valley region.
- The attack occurred on April 16th, 2013, one day after the Boston Marathon Bombing. There is no evidence that these events are related, but it does seem the team may have been waiting for a sufficient media distraction, and they were able to mobilize within a day of the bombing.

Timeline

- 12:58am–fiber optic telecommunications cables are cut in an underground vault near the substation, not too far from US Route 101, just outside San Jose along Monterey Highway annd Coyote Ranch Rd. This act eliminates not only some landline and cell phone service in the area, but also shuts down the region's 911 emergency line system. HEAVY WIRE CUTTERS are used, making it harder to repair later on.

- 1:07am–additional cables used by Level 3 communications are cut in another vault near the Metcalf substation, causing customers in the area to lose internet service. To access both of these underground vaults, the culprits have to remove two manhole covers. It is speculated at least two people are involved in this part of the attack.

- 1:31am–surveillance cameras near Metcalf Substation record streaks of light, which investigators believe is a flashlight pointing out specific targets. The cameras are aimed inward, however, so no individuals are visible on the footage. Over the next few minutes, several sparks and flashes from gunfire are visible in the footage. The attack has commenced in earnest.

- The gunmen shoot at the transformer for 19 minutes, firing off more than 120 rounds of ammunition. Many shots missed their targets, but as many did not, hitting specific locations in the transformer banks, destroying at least 10 transformers in one area and three in another. By the end of the attack, 17 transformers have been destroyed.

- 1:37am–PG&E receives alarms from motion sensors along the fence.

- 1:41am–Santa Clara County Sheriff's Dept receives a 911 call from an employee at the Metcalf Energy Power Plant, just down the road from the substation. This employee still had cell service, meaning the initial fiber optic cables cut were not sufficiently enough to eliminate service entirely. The employee reports gunshots.

- 1:45am–Metcalf Substation transformers begin to overheat. After being riddled with bullet holes, the transformers are leaking approximately 52,000 gallons of cooling oil. This triggers a series of alarms at a PG&E control center 90 miles north. As a result, PG&E is able to divert power through other substations and prevent major blackouts.

- 1:50am–another streak of light, consistent with a flashlight being waved, is visible on security footage. This seems to mark the end of the attack. From this point on, no more gunshots are fired.
- 1:51am–less than a minute after the attack ends, police officers arrive. The officers find the gates to the location still locked.
- 3:15am–a utility technician with PG&E arrives at the substation to survey the damage.

Investigation

- Investigators discovered over 100 shell castings, belonging to a 7.62x39mm weapon - likely to be an SKS or AK variant
- No fingerprints were found on any of the shell casings or rounds. No bootprints or ire tracks from a potential getaway vehicle were found. Investigators were unable to find any evidence of the gunmen arriving or leaving in the video footage.
- Investigators believed at least 2 weapons had been fired, with as many as 4 being used during the shooting.
- The gunshots were targeted at the coolant fins on the transformers, which caused the cooling oil to leak, overheating the transformers.
- This caused irreparable harm to the transformers and attracted less attention as the coolant fins quietly leaked. If the gunmen had targeted different sections of the transformers, the damage could have resulted in extensive fire or explosions.
- The gunmen seemed proficient in shooting as they had been shooting from approximately 25 meters away.
- Small piles of rocks were discovered in the area, indicating the gunmen had visited the location beforehand to mark their shooting locations.
- It was also believed they used night-vision goggles
- The cutting of the fiber optic cables indicated that the gunmen had knowledge of the Metcalf Substation's systematic layout, which relied upon SCADA systems (Supervisory Control & Data Acquisition) not cellular networks, as others do. The attackers were able to eliminate any early warning systems that would alarm the PG&E control centers of the transformer failures.

Damage

- The damage to the substation took 27 days to repair and cost $15.4 Million. It caused a fluctuating level of power available to residents in the local area (not only southern San Jose, but throughout Gilroy and Morgan Hill as well). In the substation's 500kV yard, 10 transformers were damaged; In the 230kV yard, 7 transformers were damaged; In the 115kV yard, 6 circuit breakers were damaged. It was also claimed that a total of 52,000 gallons of mineral oil (used for cooling) leaked as a result of the bullet strikes.

- The damage to the fiber-optic telecommunications infrastructure was repaired within 24 hours. AT&T had six cables cut and needed to install new cables to work around the affected area. LEVEL 3 Communications had one cable cut, which was repaired within 10 hours.

- The attack did not disrupt much of the power grid since officials were able to reroute power around the Metcalf substation, and not only increase power plant production around Silicon Valley but asked residents to decrease their energy usage until midnight to help offset this destruction of property.

- *If this attack was carried out in the middle of winter or summer it could have resulted in blackouts throughout the San Jose area.*

- John Wellinghoof, the ten-chairman of Federal Energy Regulatory Commission (FERC) believed that a widespread replication of the attack could black out much of the country and potentially take down the U.S. electric grid. He also believed that America was woefully unprepared to deal with physical attacks entirely, having spent the past few years adapting to the emerging threat of cyberattacks, but ignoring the physical vulnerabilities of the power grid.

Other Attack

- On August 27, 2014, sometime in the middle of the night, the Metcalf substation was attacked again. An unknown number of individuals cut through the fences and ransacked the offices on the site, stealing items, paperwork, and files pertaining to the substation maintenance. This included a copy of the plans to improve and prevent a similar disaster as the 2013 attack from occurring. These copies were never recovered. The newly installed alarm system failed to go off during the 2014 attack or alert the authorities. No camera footage was captured of the intruders.

Anonymous
An Analysis of the Attack on the Metcalf Substation on April 16th, 2013
July 4th, 2022