NCRIC | Northern California Regional Intelligence Center

Fusing Information, Talent And Training For A Safer Society.

NCRIC Advisory Bulletin

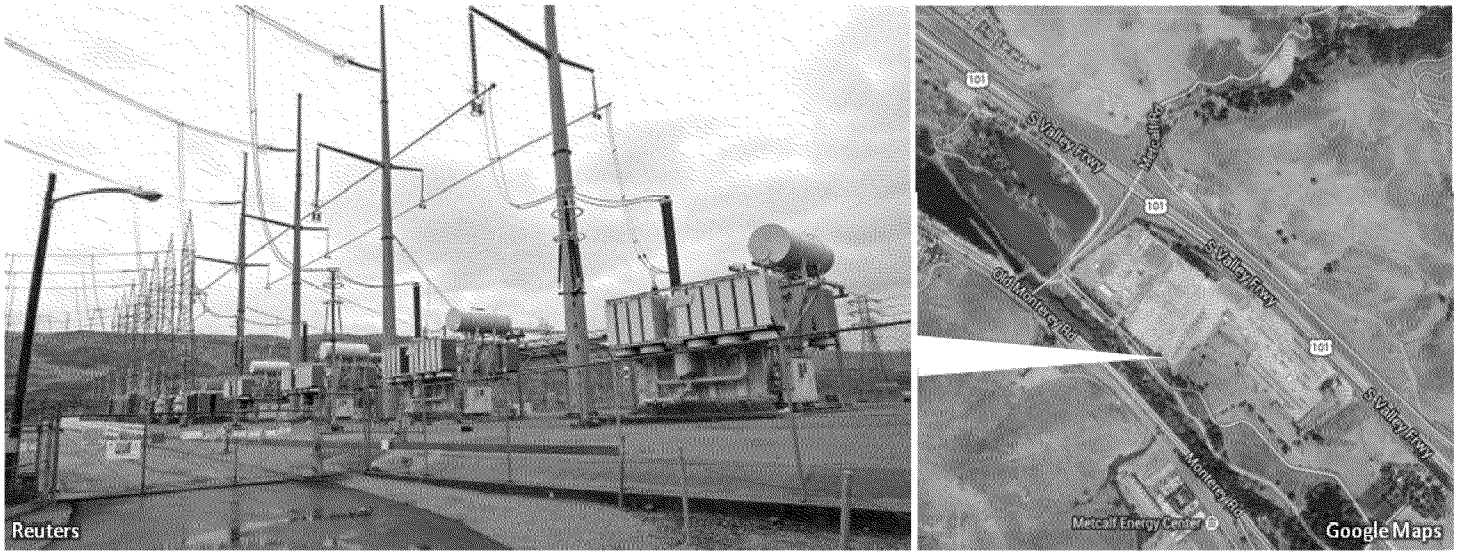
(U) SCOPE: NCRIC Advisories are intended to raise awareness of an emerging issue within the domain of critical infrastructure of interest to NCRIC partners. For comments and questions regarding this product, please contact the NCRIC at dutyofficer@ncric.org attention Risk Management Unit.

27 March 2014

(U) Sabotage Against Electricity and Telecommunications Targets

(U//FOUO) The 16 April 2013 sabotage[1] of optic cables and electricity transformers supplying Silicon Valley highlighted the vulnerability of critical infrastructure to deliberate, malicious harm. However, indications are lacking of a broader, sophisticated threat in the NCRIC area of responsibility for the following reasons.

- *The increase in suspicious activity reporting submitted to the NCRIC since the attack is consistent with heightened security awareness and does not signify a rise in nefarious activity.*
- *While the attack was preplanned, its execution was not sophisticated.*[2] Cutting the optic cables required the ability to lift manhole covers and use heavy wire cutters, and the radiators on the transformers presented a large, well-lit target that would be easy to hit.
- *Characterizing the perpetrators as 'snipers' overstates the capability demonstrated in the attack.*[3] The multiple rounds fired from short range to disable each of the large transformers do not point to the shooter(s) possessing advanced marksmanship skills.



(U) A bank of transformers struck by gunfire at the Metcalf electricity substation on 16 April 2013

(U//FOUO) **Increased suspicious activity reporting levels consistent with heightened awareness.** Following the Metcalf incident, the NCRIC received a significantly higher number of suspicious activity reports (SARs) relating to the electricity and telecommunications sectors, compared to previous months.[4] Allowing for weekly fluctuations, SARs from

these sectors have remained at consistently higher levels than before April 2013. No connections between individual SARs have emerged to indicate a specific trend of nefarious activity. Rather, the higher volume of reporting likely reflects heightened vigilance on the part of security personnel and law enforcement and greater sensitization to potential threats to these sectors.

(U//FOUO) **Preplanned attack.** Just before 1 a.m. on 16 April 2013, one or more individuals cut cables in separate underground vaults near the Metcalf electricity substation south of San Jose, CA. From there, they took up position outside the facility's perimeter fence and opened fire on the substation's transformers. They expended over 100 rounds of rifle ammunition, mostly striking the large radiators that cool the transformers. The punctured radiators leaked thousands of gallons of cooling oil, tripping alarms that prompted SCADA systems[5] to prevent overheating and reroute power. The nearby Metcalf Energy Center called 911 to report hearing shots fired. As law enforcement responded, the intruders left the scene. Four strands of barbed wire were cut on a pasture fence near where it met the substation's perimeter fence.

(U//FOUO) **Whodunit?** With the investigation of the Metcalf incident still ongoing, the motive for the sabotage and the affiliation or grievance of those who conducted it remains unknown. No one has claimed responsibility for the sabotage and nearly a year later, the motive is still unclear. The scale of the incident and the infrastructure targeted do not match the modus operandi of known threat actors. If the incident was indeed a terrorist attack, it is unusual that those responsible have not exploited media interest to advance their particular agenda. Criminals have targeted energy facilities for metal theft but typically do not go out of their way to take them offline. Environmental extremists and others with an antagonistic view of energy companies and large corporations have resorted to sabotage but rarely on so ambitious a scale. The significant damage caused at Metcalf would also be unusual for a disgruntled employee or frustrated customer. If the attackers' intention was to terrorize, then it was a failed attack. They were apparently too risk averse to engage responding law enforcement or to cause greater damage to the substation's components by entering the facility or to exploit the incident to further their social or political ideology.

(U) Electricity Infrastructure Threats and Vulnerabilities

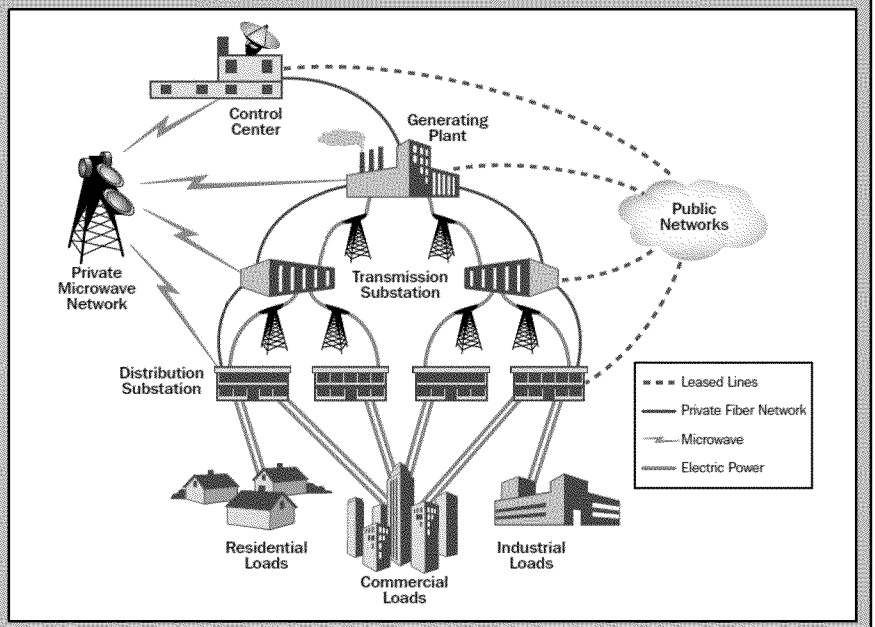
(U//FOUO) **Modes of Attack.** From a capabilities perspective, various modes of attack could be used to disable critical infrastructure. The Department of Homeland Security assesses that targeted shootings, intentional downing of power lines, and bombings are "the most likely high-profile and potentially consequential" tactics for electricity subsector infrastructure.[6] Depending on level of expertise and access to materials, potential adversaries could use small arms to damage components, as at Metcalf, or resort to improvised explosive devices, vehicle borne explosive devices, construction explosives (e.g., dynamite), grenades, destructive chemicals, introduction of hazardous materials, nuclear or radiological dispersion devices, arson, or sabotage of critical components of the electric infrastructure powering the site. In addition, cyber attacks present non-kinetic options for targeting critical infrastructure to disrupt the functionality of computerized control systems, infiltrate data processing, and cause severe economic and operational repercussions.

(U//FOUO) **Vulnerabilities of Electricity Infrastructure.** In recent media coverage of the sabotage at Metcalf, journalists have also noted the inherent vulnerability of electricity substations.[7] As illustrated on the next page, the electric power system requires that all segments function efficiently; attacks upon any of the components can impact the entire system and have the potential for cascading damage effects. DHS notes, however, that while targeted shootings can cause extensive damage, due to system resiliency, the effects may not result in significant impacts to customers.[8] Because of their size and function, substations are often located in sparsely-populated areas along freeways or major thoroughfares. They are not easily concealed within buildings or behind fences. Critical components, such as the transformer cooling tanks targeted in the April 2013 attack, present an easy target. At the opposite extreme, SCADA systems that are used to control essential functions of many electrical substation components could in theory be disabled by a sophisticated cyber attack. The system also has some resilience, as demonstrated by the rerouting of service via other substations after the Metcalf substation's transformers were taken offline. Although the sabotage at Metcalf was preceded by cutting optic cables in two nearby vaults, technicians at a remote location were still able to

monitor alarms on the transformers as they overheated and shut them down without further damage.

(U) Infrastructure Interdependencies

(U//FOUO) Effective operation of the electric power infrastructure is dependent upon several interconnected systems working together to generate and distribute electricity. Substations, such as Metcalf, are critical components of the electric power infrastructure. The figure below is a simplified illustration of the interconnectedness of the electric power system. It shows the complex interdependencies of the control center, the generating plant, transmission and distribution substations, and the necessary telecommunications components. Command and control of these various power system components relies heavily upon telecommunications lines.



Source: Department of Homeland Security, Electric Transmission Substations, Potential Indicators of Terrorist Activity, Common Vulnerabilities, and Protective Measures, 5 October 2007.

All law enforcement and media inquiries should be directed to the FBI San Francisco Field Office at 415-553-7400.

All federal agencies should contact FBI Headquarters, DTOU IA Erin Weller at 202-324-4070.

Report urgent threat information to local Law Enforcement or the FBI-JTFF at (415) 553-7400.

Report suspicious activity to the NCRIC online at http://www.ncric.org.

[1] (U) See Title 18 U.S. Code § 1366, Destruction of an energy facility. Text available from the Government Printing Office: http://www.gpo.gov/fdsys/pkg/USCODE-2011-title18/pdf/USCODE-2011-title18-partI-chap65-sec1366.pdf

[2] (U) Journalistic accounts have called the attack "sophisticated" and a "military-style raid." (*The Los Angeles Times*, Richard A. Serrano and Evan Halper, "Sophisticated but low-tech power grid attack baffles authorities," 11 February 2014, http://www.latimes.com/nation/la-na-grid-attack-20140211,0,7627269.story#ixzz2wuFwnSKe and *Foreign Policy Magazine*, Shane Harris, "Military-Style Raid on California Power Station Spooks U.S.," 27 December 2013. http://complex.foreignpolicy.com/posts/2013/12/24/power-station-military-assault)

[3] (U) The *Wall Street Journal* has used the term 'sniper' in two pieces: Rebecca Smith, "Assault on California Power Station Raises Alarm on Potential for Terrorism," 5 February 2014 (updated online on 18 February), and Peggy Noonan, "America's Power Is Under Threat," 7 February 2014. The

[4] (U) The increased volume of reports was highlighted in a "SAR Spotlight" in NCRIC Partner Update Brief 13-120, 18 June 2013.

[5] (U) Supervisory control and data acquisition (SCADA) is a type of industrial control system used to gather and analyze real-time data.

[6] (U) Department of Homeland Security Office of Cyber and Infrastructure Analysis (OCIA), *(U) IP Note: Most Significant Activity Surrounding Tactics, Techniques, and Procedures Against the Electricity Subsector*, 26 March 2014.

[7] (U) Rebecca Smith, "Transformers Expose Limits in Securing Power Grid," Wall Street Journal website, 4 March 2014. http://online.wsj.com/news/articles/SB10001424052702304680904579365412479185116

[8] (U) Department of Homeland Security Office of Cyber and Infrastructure Analysis (OCIA), *(U) IP Note: Most Significant Activity Surrounding Tactics, Techniques, and Procedures Against the Electricity Subsector*, 26 March 2014.