Physical security and the vulnerabilities of critical infrastructure to physical attack

By **Stefan Skinner**

(short form – 1,586 words)

Table of Contents

It starts -

In 2013 a watershed moment occurred on American soil that would wake up some in the world of Critical Infrastructure and Key Resource (CIKR) protection, and it has been called “the most significant incident of domestic terrorism involving the [power] grid that has ever occurred”[1]. An armed attack against an electrical substation occurred outside San Jose, California, that took 17 transformers off-line for 27 days[2]. The Metcalf substation, owned by Pacific Gas and Electric (PG&E), is situated near highway 101, and in the early hours of April 16, 2013, a section of AT&T fiber-optic cables near the substation was cut in such a way as to make repair difficult and time consuming, but most importantly, from a tactical perspective, it temporarily cut local communications[1]. A flashlight, being used as a signal, was recorded on one of Metcalf's security cameras immediately followed “by the muzzle flash of rifles and sparks from bullets hitting the [chain link] fence”[2]. The gunmen's targets were the “transformers’ oil-filled cooling systems” which leaked their oil, overheated, and caused the system to shut down. Police arrived at 0115 hrs, one minute after the shooting stopped according to the security cameras, saw and heard nothing out of the ordinary, and left[2].

The Metcalf incident shows just how easy it can be for professional operators to take an entire substation off-line for a month. Imagine, though, if multiple substations were hit simultaneously. It is just such a scenario that the Federal Energy Regulatory Commission (FERC) has been studying; they found that if just nine highly critical substations were attacked simultaneously in all three U.S. grid sections (East, West, and Texas), the U.S. could see a nationwide blackout that could take months to repair[3].

Kinetic attacks upon critical infrastructure will likely become a common feature of the threat landscape going forward, as it is an integral part of “gray-zone warfare”[4]. As actions in the gray-zone are acts “below the threshold of war”[4], and often unattributable, then until the next great war gets underway, one should expect this type of activity to increase continuously.

For example -

During the Metcalf incident shooters intentionally fired at the radiator fins of the transformers, ensuring that the cooling oil would drain out, which it did, whereby all 17 transformers overheated and caused a system shutdown[2].

The Metcalf incident shows what is possible, and because most substations are not attended and are only controlled remotely by Supervisory Control And Data Acquisition (SCADA), it leaves them wide open to physical attack[5].

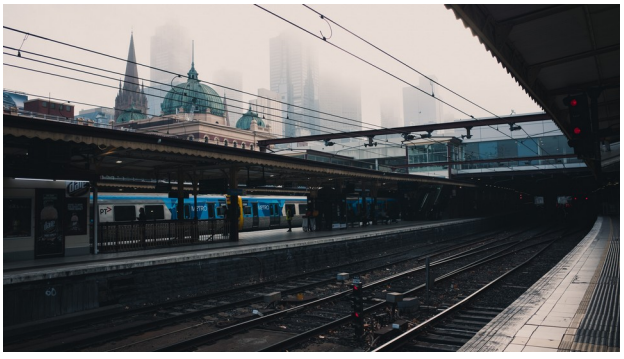
With enemies like these, who needs… wait a minute -

The energy sector isn't the only sector with such vulnerabilities to physical attack. Drinking-water and waste-water plants are targets that any terrorist would love to hit, and they are just as susceptible as the Metcalf substation to attack.

As far back as 1941, then director of the Federal Bureau of Investigation, J. Edgar Hoover stated: "It has long been recognized that among public utilities, water supply facilities offer a particularly vulnerable point of attack [...], due to the strategic position they occupy in keeping the wheels of industry turning and in preserving the health and morale of the American populace"[6].

In 2012, "two drunken people" entered a waste-water treatment plant in Sacramento through a gate; not only did they not set off any alarms, it is possible that no one would even have known they were there had they not "called for help" because they couldn't find their way out of the facility once inside[7]. Right next to the water treatment plant is a drinking-water plant that is one of two water plants providing water to the entire city of Sacramento [California's capital city] and is a known terrorist target[7]. Obviously if two intoxicated people can just wander in, a serious team could have wreaked havoc. The waste-water treatment plant had been a part of upgrades since 9/11 money was allocated to improve security ($216,000), and the city later paid even more money for security ($1.6 million), and the results were abysmal[7]. A relative few "number of large drinking water and waste-water utilities located primarily in urban areas […] provide water services to more than 75% of the U.S. population"[18]. This clearly makes the water sector a key target for terrorism.

The threats to the rail system by physical attack are just as ominous as the attacks on electric and water. Considering that the U.S. has 100,000 miles of rail, the ways to attack it are likely limited only by imagination[8]. Some of the glaring vulnerabilities of trains to physical attack are: 1) lack of serious train station security; 2) existence of train schedule databases which are a prime target, either by hacking the computer(s) that house the database table data, or by co-opting people with access to the data, in order to know, with high precision, where trains are and what cargo they contain, including sensitive cargo such as chemicals or military shipments; 3) a train that has chemical, petroleum, or other dangerous loads could simply be blown up at a location where it would cause the most damage; 4) passenger trains offer outstanding possibilities for ransom; and so on[8].



Of course, it's a sliding scale -

Only five days after the Metcalf incident, a nuclear power plant in Tennessee, the Watts Bar Nuclear Power Plant, had an intruder; the intruder was challenged by security only to begin shooting at security, who then returned fire before the intruder made his getaway by boat[9].

Imagine if there had been no guard at the nuclear facility. The prime reason there was a guard there is the Nuclear Regulatory Commission mandates armed guards at nuclear facilities[10]. Unfortunately, it appears that only government can properly induce private industry to make investments that have no guarantee of a return, such as defenses, because ironically, the better the defenses are the less likely it is there will be an attack to justify those very expenses.

Where there's a will, or a contract -

The likelihood of attack at any given site is lowered in the presence of strong defenses, because they increase the cost and decrease the likelihood of success of an attack. Dedicated people on a mission, though, can find ways to press through whatever defenses are in place. For example, Chapo Guzman is a notorious former drug lord who operated in Mexico as the head of the Sinaloa cartel[11]. He was spirited out of prison in one of the most spectacular prison escapes ever; the high-risk prisoner was able to escape a maximum-security prison by riding a motorcycle through a mile long tunnel constructed 30 feet below the Earth's surface[12]. Those digging the tunnel were able to go up 30 feet from the tunnel and come out precisely in the cell's in-room shower, which was a semi-private space in the cell[12].

The fact that engineers could construct a tunnel of this length, remove 3,250 tonnes of earth, and come out in a space 2 feet by 2 feet, is extraordinary, and portends of major security issues in defense against creative critical infrastructure attackers[12]. In the motion picture Victory (1981), WWII American POW's are playing an exhibition football/soccer match against a German team, and a tunnel was dug for them to escape[13]. The tunnel came up to the floor of a very large bath in the locker room, and at half-time the tunneler punched through the floor to rapidly drain out the bath

water to clear a path to the tunnel[13]. Imagine, then, a group tunneling under a nuclear power facility and coming up to the cooling pool, punching a hole through, and rapidly draining it; this in turn would cause a melt-down and possibly even explosions that would send radioactive material into the wind. The end result would be similar to what happened at the Fukushima Daiichi nuclear power plant when the cooling pools became inoperable after a massive earthquake and tsunami caused tremendous damage to the facility[14]. A moat could be a help in protection from tunneling due to the tendency of the weight of the water to collapse a tunnel underneath it. It is possible, though, that the Guzman tunnel, at thirty feet below ground surface, may be able to go under a moat unaffected.

The world is gray -

The blurring of boundaries brought about by gray zone conflict, causes the difficulty of defense planning to increase in step. Similar to the Battle of Kadesh between the armies of Ramses II and Muwatalli II[15], a war without boundaries and the emergent qualities[16] found within one, ensures that the war we end up fighting may be different than the one we, or our enemies, can foresee. In the gray zone that means that “the boundary between the battlefield and what is not the battlefield, between what is a weapon and what is not, between soldier and noncombatant, between state and non-state or supra-state”[17] will continue its path to dissolution.

As for the near-term, the gray zone will be the primary zone of operation for the world’s military and intelligence services (public and private), and it will be full and busy. Critical infrastructure must be constructed, or re-built, with this fact in mind, otherwise all the investments the United States federal government is about to make in critical infrastructure will be for nothing. If the ‘lowest-bidder wins’ mentality of yesterday remains the mentality of tomorrow, coupled with the laisez-faire attitude of private industry toward expensive security, we in the United States are doomed; that much, at least, we can foresee.

References:
****ALL IMAGES ARE CLICKABLE *****

Aldrich, I. (2015). *Joaquín "El Chapo" Guzmán Loera Biography*. http://www.biography.com/people/el-chapo-joaquin-guzman-loera

Baverstock, A. & Calderwood, I. (2015). *First picture of motorbike kingpin el chapo used to escape prison*. http://www.dailymail.co.uk/news/article-3160913/El-Chapo-s-ride-freedom-pictures-motorbike-rails-Mexican-drugs-lord-used-tunnel-escape-prison-paid-50m-bribes.html

CBS. (2012). *Water Treatment Plant Security Breach Raises Serious Questions.* http://sacramento.cbslocal.com/2012/03/28/water-treatment-plant-security-breach-raises-serious-questions/

Copeland, C. (2010). CRS report for congress prepared for members and committees of congress terrorism and security issues facing the water infrastructure sector. http://fas.org/sgp/crs/terror/RL32189.pdf

Hoover, J. E. (1941). Water Supply Facilities and National Defense. *Journal (American Water Works Association)*, *33*(11), 1861–1865. http://www.jstor.org/stable/41232575

Dostri, O. (2020). *The Reemergence of Gray-Zone Warfare in Modern Conflicts.* https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/January-February-2020/Dostri-Gray-Zone/

Fields, F. (Producer), & Huston, J. (Director). (1981). *Victory* [Motion Picture]. US/UK: Paramount Pictures

Holt, M. (2014). *Nuclear power plant security and vulnerabilities*. http://fas.org/sgp/crs/homesec/RL34331.pdf

Huotari, J. (2013). *TVA: Suspect shoots at security officer at watts bar nuclear plant, officer shoots back***.** http://oakridgetoday.com/2013/04/21/gunshots-fired-at-watts-bar-nuclear-plant-involve-tva-nuclear-security-officer/

Liang, Q. & Xiangsui, W. (1999). *Unrestriced warfare*. https://archive.org/details/Unrestricted_Warfare_Qiao_Liang_and_Wang_Xiangsui

mrsghistory. (2017). *History Channel Decisive Battles E05 Ramses II*. https://www.youtube.com/watch?v=N9WszW3hzzo

Nelson, D. (2018). *What Are Emergent Properties? Definition And Examples*. https://sciencetrends.com/what-are-emergent-properties-definition-and-examples/

Penn State University. (n.d.). *Major vulnerabilities to railway security.* http://www.personal.psu.edu/staff/r/p/rpt117/sra211/vulnerabilities.htm

Smith, R. (2014 -a). *Assault on California Power Station Raises Alarm on Potential for Terrorism* . https://www.wsj.com/articles/SB10001424052702304851104579359141941621778

Smith, R. (2014 -b). *U.S. Risks National Blackout From Small-Scale Attack.* https://www.wsj.com/articles/SB10001424052702304020104579433670284061220

Wikipedia. (n.d. -a). *Metcalf sniper attack*. https://en.wikipedia.org/wiki/Metcalf_sniper_attack

Wikipedia. (n.d. -b). *Electrical substation*. https://en.wikipedia.org/wiki/Electrical_substation

World Nuclear Association. (2015). *Fukushima Daiichi Accident*. https://www.world-nuclear.org/information-library/safety-and-security/safety-of-plants/fukush%0Aima-daiichi-accident.aspx