Physical security and the vulnerabilities of critical infrastructure to physical attack

By **Stefan Skinner**

(long form - 2,635 words)

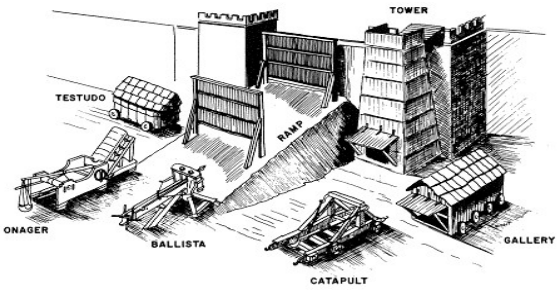
Table of Contents

A brief history -

The history of physical security and its attendant use of weapons is as old as humanity itself. Spears are some of the oldest known weapons to exist, with some specimens as old as 500,000 years[1]. Complete spears were found in the 1990s in a “coal mine in Schöningen, near Hannover, Germany [that] are the oldest complete hunting weapons ever found [at] 380,000 to 400,000 years old”[2]. The use of the bow goes back to 10,000 BCE and it is “unlikely that animals were its only targets”[3] any more than it is likely that animals were the only targets of spears before them.

People long ago began to band together for division of labor and mutual defense, and these human centers often included walls. The city of Jericho had, by 7,000 BCE, a wall made of stone that was 13 feet high and 10 feet thick at the base[3]. As urbanization began in Mesopotamia around 4,500 BCE, cities began to wall themselves in with walls that included gates, watchtowers, and moats[4]. The gates, watchtowers, and moats would remain the hallmarks of “military architecture”[3] until the arrival of the “widespread use of cannons”[3].

Prior to the arrival of cannons, the primary attack against walled cities was the siege. Initially sieges were used as a means of forcing capitulation by an enemy through starvation, the routes in and out would be sealed and eventually the city behind the wall would surrender[5].



ROMAN SIEGECRAFT AND WORKS

This form of siege could take quite some time to be successful, so as time went on new methods were devised to expedite the besieged cities surrender: catapults for launching fire, stones, or even diseased dead animals over a wall and into the city behind it; battering rams to smash doors or even parts of the wall; and the use of tunneling to infiltrate a walled city or to collapse part of the outer wall structure[5].

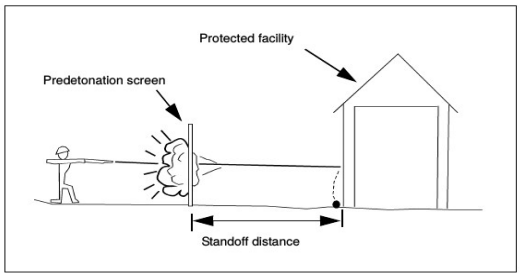
The only constant is change -

With the advent of gunpowder and cannons, however, the face of sieges would begin to change. The walls which had proven relatively effective against the siege up to this point, were now wholly inadequate to meet the challenges posed by the new technology[5]. Where breaching of the outer walls by way of tunneling underneath it was moderately effective, with gunpowder mines, the wall did not stand a chance if a mine was successfully detonated below it[6].

As a defense for castle and city walls, moats were invented. Moats filled with water create an obvious impediment to attack, as it prevents the use of battering rams, and it decreased the accuracy

of launched items[7]. Even if a wall were breached by cannon fire, the attackers would still have to cross the moat, which would leave them terribly exposed. Even dry moats provide protection by creating what is called a stand-off distance[8]. The stand-off distance is the distance between a fence or natural barrier, and the structure being protected, this area is well lit and monitored by security personnel that are able to physically respond to intruders in the stand-off area[8]. Alas, stand-off distance does little against direct gunfire.

One layer good, many layers better -



Stand-off distance is part of what is called “defense in depth”, which is a layered approach to security: perimeter fencing, stand-off distance, lights, cameras, security personnel, and access control mechanisms[8]. A perimeter fence provides: a clear demarcation line, a psychological and physical barrier, and some level of protection from shoulder launched weapons, e.g., an anti-tank weapon, by acting as a “pre-detonation screen”[8].

Buckle up -

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”[9]. An armed attack against an electrical substation occurred outside San Jose, California, that took 17 transformers off-line for 27 days[10]. 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[9]. 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”[10]. 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[10].

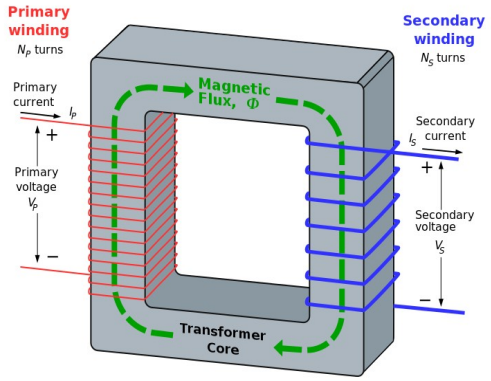
The Metcalf incident shows just how easy it can be for professional operators to take an entire substation off-line for a month. Imagine, though, if multiple substations were hit simultaneously. It

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[11].

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"[12]. As actions in the gray-zone are acts "below the threshold of war"[12], and often unattributable, then until the next great war gets underway, one should expect this type of activity to increase continuously.

Modernity's Achilles heel -

Electrical substations are an integral part of the electric grid, as they provide the mechanism needed for the long-distance transmission of power from power generation sources to end users[13]. Long distance transmission of power is accomplished by the use of transformers, and these transformers are located at substations[13]. A substation uses its transformers to increase voltage on one end of the line, the supply side, and decrease it on the other end, the demand side[14]. A transformer basically consists of copper winding's around a transformer core[14]; the core for a large transformer can be made of laminated steel or iron, and the winding's are made of electrically insulated conducting material[15].



The overall purpose of a transformer is to both efficiently and rapidly transfer power from a power producer to power users[16]. Large transformers are immersed in a special cooling oil that remains stable at high heat and provides electrical insulation as well[17].

Back to point -

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[10].

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[13].

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"[18].

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[19]. 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[19]. 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[19]. 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[20]. 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[20].

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[21].

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[22]. 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[23]. 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[24]. 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[24].

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[24]. 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[25]. 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[25]. 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[26]. 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.

Fight fire with fire -

The new threat on the horizon, for secure installations in particular, are unmanned aerial vehicle's (UAV's). Much of physical security is based on the idea that whatever attacks the installations will be at ground level, and UAV's clearly are able to circumvent those defenses. In addition, UAV's are becoming weaponized with guns and/or explosives[27]. Combine the weaponization of UAV's with the swarming capabilities being programmed into them, and attacks by armed swarming UAV's should send a shudder through most security professionals[28]. Some ways of protecting against UAV's currently are: radio jamming, lasers, guns, or counter-swarms[29] [30]. Radio jamming can be effective if the swarm is counting on “communications for its coordination”[30]. Another UAV defense is from “low cost per shot” weapons such as lasers and rail-guns, as well as machine guns such as the Counter - Rockets, Artillery and Mortars weapons system (C-RAM)[30].

One defense that looks promising is the “counter-swarm”[30]. The counter swarm could mix in with an attacking swarm and self-detonate, causing large losses of UAV's in the attacking swarm. A variation on the theme is to program the UAV's to go “head-to-head”[31] and fight each other in similar fashion to manned fighter aircraft[30].

The more things change, the more they stay the same -

In 1999, a paper was released by two Chinese People’s Liberation Army (PLA) generals discussing the future of warfare[32]. In the paper, the authors point out that focusing on one type of technology may result in an

“electronic Maginot line”[32] that leaves those who become dependent on any one technology virtually doomed to be defeated[32]. Therefore, it is imperative that no one technology, or even a related group of technologies, be made a silver bullet. Were that to happen, it's less a silver bullet and more a path to failure.

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[33], a war without boundaries and the emergent qualities[34] 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”[32] 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

allthereddimensions. (2014). Officials believe 2013 attack on pg&e metcalf substation a "dress rehearsal" for a larger electric-grid attack to come. http://altereddimensions.net/2014/pge-metcalf-substation-vandalism-terrorist-attack-dress-rehearsal-larger-attack

Ancient Military. (n.d.). *Ancient Weapons*. http://www.ancientmilitary.com/ancient-weapons.htm

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

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/

exploring-castles. (n.d.). *Defending a medieval castle: The formidable features of some of britain's strongest castles*. http://www.exploring-castles.com/medieval_castle_defence.html

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

FPSRussia. (2012). *Prototype quadrotor with machine gun!*. https://www.youtube.com/watch?v=SNPJMk2fgJU

Gallagher, S. (2013). *German chancellor's drone "attack" shows the threat of weaponized uavs*. http://arstechnica.com/information-technology/2013/09/german-chancellors-drone-attack-shows-the-threat-of-weaponized-uavs/

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

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/

Kouwenhoven, A. P. (1997). *World's oldest spears*. http://archive.archaeology.org/9705/newsbriefs/spears.html

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

Mark, J. J. (2009). *Wall*. https://www.worldhistory.org/wall/

Meier, A. V. (2006). *Electric power systems: A conceptual introduction*. U.S.: Wiley Inter-Science

Meistrich, I. (2005). *Military history: The birthplace of war*. http://www.historynet.com/military-history-the-birthplace-of-war.htm

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

Rawley, C. (2015). *The future of naval warfare is swarming, or… distribute everything.* http://www.informationdissemination.net/2015/01/the-future-of-naval-warfare-is-swarming.html

Scharre, P. (2014). *Robotics on the battlefield part II The coming swarm*. https://www.cnas.org/publications/reports/robotics-on-the-battlefield-part-ii-the-coming-swarm

Simpson, D. & Bruckheimer, J. (Producers), & Scott, T. (Director). (1986). *Top Gun*. U.S. : Paramount Pictures

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

Texas Instruments. (2001). *Section 4 – power transformer design*. http://www.ti.com/lit/ml/slup126/slup126.pdf

U.S. Army. (2010). *Physical security*. http://fas.org/irp/doddir/army/attp3-39-32.pdf

Wikipedia. (n.d. -a). *Siege*. https://en.wikipedia.org/wiki/Siege

Wikipedia. (n.d. -b). *Tunnel warfare*. https://en.wikipedia.org/wiki/Tunnel_warfare

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

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

Wikipedia. (n.d. -e). *Transformer*. https://en.wikipedia.org/wiki/Transformer

Wikipedia. (n.d. -f). *Transformer oil*. https://en.wikipedia.org/wiki/Transformer_oil

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