Physical security and the vulnerabilities of critical infrastructure to physical attack

(Executive Summary)

By Stefan Skinner

Cybersecurity for critical infrastructure is improving, while physical security of critical infrastructure is not as high a priority, but it should be. For all the talk of worms, viruses, and Advanced Persistent Threats (APTs), not as much talk or money is focused on preventing, or preparing to quickly recover from, outright physical attacks by people who have the tools, expertise, and will to carry out such attacks.

The problem is not new, but the tactic it facilitates may be. For time immemorial, people have built walls, tunnels, moats, and other contrivances to thwart physical attack by adversaries. However, the physical security at some key infrastructure sites. e.g., water, is so bad that people have been known to simply wander around these facilities at will. In a gray-zone world, this level of non-security could be the opening for a series of hits that the United States takes, each of which being below the threshold of war, but which collectively will cause more damage than what we think of today as an act of war.

It is a paradox that the better the security is, the less likely it will be needed, as low hanging fruit abound elsewhere. So, in a capitalist system, spending a fortune on security that doesn’t appear to have been needed is something that bean counters will resist making into a habit at every turn; this is the reason for regulation that demands serious physical security, e.g., at nuclear power facilities. The absence of regulation often means leaving security to bean counters instead of security professionals, and that makes the failure of the security more likely, especially if it is tested by professional attackers.

A case in point is the Metcalf power substation in San Jose, California. The substation was attacked in the early morning hours of April 16, 2013, by an unknown group of individuals who cut communications and fired a relatively high number of rifle rounds at the substation’s transformers, draining the cooling oil and causing the system to shutdown due to an overheating condition. The mission was a complete success from the attackers’ point of view, as the substation was off-line for 27 days. If this type of attack were to occur at key substations across the United States simultaneously, the results could be catastrophic for this country.

The number of ways to attack critical infrastructure appear to be limited only by the imagination. Some people seem to think it an impossible mission to defend it all, but that doesn’t mean that we can’t make it as difficult, dangerous, and expensive as possible for attackers, and those funding and supporting them. The United States is about to make huge investments in critical infrastructure throughout the country; one can only hope that, where it is most applicable and most critical, physical security is a primary consideration in the construction and operations plans.