CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

The Electrical Grid as a Target for Cyber Attack

James Andrew Lewis
Center for Strategic and International Studies
March 2010

The electrical power grid has gotten much attention in the last few years as a potential target for cyber attack. Here are the reasons why.

The electrical power system has always been a high priority target for military and insurgents. It is cheap and easy for insurgents to blow up or simply pull down pylons and transmission lines or to attack power plants and substations. This is a normal part of guerrilla warfare. Militaries also normally plan to attack power plants, substations or hydroelectric facilities as part of a bombing campaign. British air raids on the Ruhr dams are a classic example of this. The only time these plants are spared is when attackers believe they will have an easy victory and will soon be occupying the target country. Cyber attack is a new addition to the portfolio of possible attacks (missiles, aircraft, Special Forces, sabotage) that many militaries could use to attack an opponent's electrical industry. Cyber combines low cost and long range. We know that there has been discussion of such attacks in the military literature of potential opponents, and this may reflect their actual military doctrine and planning.

One trend that has increased vulnerability across the board in many industries is the move in the last decade from propriety software and communications systems using dedicated lines to IP- (internet protocol) based systems using commercial software (including Windows) over the public internet. There are sound economic reasons for moving to the IP-based approach, including lower costs of acquisition and of operations by using public networks and remote access to control systems, but this has essentially made targets less complex to attack. If an electrical company did not build security into the new, more efficient, IP-based system, the result is increased vulnerability.

The Aurora tests conducted at Idaho National Labs a few years ago showed it is possible to exploit remote access to send commands to large generators that cause them to damage or destroy themselves. Researchers were able to remotely change the operating cycle of the generator, sending it out of control. A video of the incident shows that the target generator shakes, emits smokes, and then stops. A simple analogy would be to consider the effect of randomly changing the firing order of spark pugs in your car – the engine would soon render itself nonoperational.

The 2003 Northeast power blackout, although in no way connected to a cyber attack, showed that a failure at even a small part of the grid (in this case, a small power company in northern Ohio) can have cascading effects. CIA officials have publicly identified one incident in Brazil as a cyber attack that caused a blackout.

There is evidence that unknown foreign entities have probed the computer networks of the power grid. Some electrical companies report thousands of probes every month, although we do not

know (and it may not make much difference) whether these were cyber crime or part of a military reconnaissance effort. There is also anecdotal reporting that potential military opponents have done the reconnaissance necessary for a cyber attack on the power grid, mapping the underlying network infrastructure and locating potential vulnerabilities.

It seems unlikely, as part of its reconnaissance, that foreign powers have left behind some kind of cyber time bomb that could be triggered at some later date. Networks are dynamic, almost organic in their constant change and reconfiguration, with equipment being added or changed, patches or new software being installed, usernames changing as personnel leave or are added. A "time bomb" planted in January could not reliably be expected to work in March or April.

Also, while reconnaissance of potential targets by itself is not an act of war (and is carried out routinely by all parties), planting a destructive device on an opponent's territory could itself be considered an act of war. It comes too close, and may even cross, a threshold that no one has been willing to cross in cyber war. Why risk planting something that might not work a month or so later? If we were to discover that a cyber "time bomb" has been installed, it is a good indicator that conflict is imminent.

This constraint, which brings with it a degree of caution in launching a cyber attack, applies mainly to governments. Non-state actors like terrorists are unlikely to worry about whether their action violates the international laws of war. It seems safe to assume that terrorists do not yet have the capability to launch cyber attacks against the power grid, or we would have seen such attacks in countries with active insurgencies (Colombia, for example) or against the United States. That they likely do not have the capabilities now to launch cyber attack does not mean that terrorist will not eventually acquire them.

Military precedent, foreign military publications, and new vulnerabilities combine to suggest that foreign opponents have added cyber attack on the power gird to their portfolio of possible actions in a conflict with the United States. Perhaps a better way to express this is that the United States cannot safely assume that it is not vulnerable to cyber attacks on its electrical grid, and should consider how it might improve its ability to defend theses networks

This conclusion is different from the strategic consequences on a cyber attack on the power grid. The United States routinely suffers blackouts. The nation does not collapse. In the short term, military power and economic strength are not noticeably affected - a good example for opponents to consider is Hurricane Katrina, which caused massive damage but did not degrade U.S. military power in or even long-term economic performance. Is there any cyber attack that could match the hurricane?

The United States is a very large collection of targets with many different pieces making up its electrical infrastructure. While a single attack could interrupt service, the large size and complexity of the American economy make it more resilient. Even without a Federal response plan, the ability of electrical companies to work quickly together to restore service is impressive and we should not underestimate the ingenuity of targets to recover much more rapidly than expected. This is a routine occurrence in aerial bombing: impressive damage is quickly rectified by a determined opponent.

Conflict and warfare always entail a high degree of uncertainty. The kind of proof needed for legal proceedings will always be lacking. Precedents from previous conflicts and assessments of an opponent's intentions and capabilities and our own vulnerabilities must guide planning. Based on precedent and what we know of opponent intentions, electrical grids will be a target for cyber attack in any future conflict.