Securing the Bulk Electric System

Patrick Brown, MBA, SCPM
Chair, Energy Security Committee
The Homeland Security Foundation of America

Introduction

Let’s start off with a simple statement of fact; we live in an insecure world. This truth has been demonstrated a number of times in recent years, with the attacks of 9-11, the London and Madrid bombings, and a wide range of other terrorist type attacks against military and civilian targets. We routinely see these events repeated and replayed in our newspapers, 24 hour newscasts, and discussed in our workplaces, schools, and homes.

In many ways, we have reached a point where we’ve become resigned to the risk and accept these events, if not as routine than as unavoidable, and, to a certain extent, desensitized to the potential severity and impact of these types of events. These days, we even include terrorist type attacks in popular video games, further desensitizing our youth, and our wider culture, to these events.

The ‘enemy’, defined in this case as anyone who plans, aids, or executes attacks against American personnel or interests both domestic and international, whether part of a terrorist group or as an agent of a foreign power, is aware of this desensitization of our culture to their efforts. They realize that in order to make a greater, lasting impact on our activities and interests, they will need to escalate the severity and reach of their attacks in order to gain our attention, and to instill the level of fear and anxiety in the American people necessary to further the attacker’s objectives.

With this in mind, it’s the responsibility of our security and defense community to anticipate the enemy’s future attacks, and their targets. In order to accomplish this, they must put themselves in the shoes of the attacker; what is their objective? Where are we most vulnerable? What type of attack would have the greatest impact? What resources does the enemy have at its disposal? How do we eliminate or mitigate the risk?

The question I ask is, what is the one system on which all others are based? What could simultaneously cripple our transportation systems, communications, and basic control systems? What one system, if compromised, could severely limit our ability to respond to further attacks? The obvious answer to me, as someone who has worked in the industry for the last decade, is the bulk electric system. Destroy or compromise this system, and all others will be crippled or severely limited.

The Threat of Cyber Attack

Although a physical attack on the bulk electric system is always possible, the scope of the operation necessary to make a large scale impact falls outside the capabilities of the most likely attackers; it would simply be too difficult and resource intensive to mount a physical attack of any significance.

Compromising a single or limited number of generation or transmission assets would most likely only have a local or limited regional impact, and could be mitigated in a reasonable amount of time. The operators of the bulk electric system are prepared for all single as well as the most likely multiple facility losses of this nature, and are well prepared to respond.

America's fleet of nuclear power stations are heavily fortified and protected by well-trained security forces, making them an unattractive target for physical attack.

There are a number of High Impact Low Frequency (HILF) events that are currently being examined, such as the use of an Electro-Magnetic Pulse (EMP) to compromise the digital control components of the electric system, but again, this type of attack is outside the reach of the most likely attackers.

That leaves a cyber attack as the most likely means of compromising our bulk electric system. Cyber warfare has become a 'legitimate' means of waging war, along with the use of conventional and unconventional military and paramilitary forces, and one that is readily available to the majority of our potential enemies. The United States and other developed nations have spent the last couple of decades building and refining their cyber warfare capabilities, and this has seeped out to the less developed communities as well as to terrorist organizations.

Unlike a conventional, or even unconventional military force, waging cyber warfare is relatively cheap and can be quickly implemented. In most cases there is no need to have physical access to the target, or place any personnel or other assets at risk, making it less resource intensive and an easier 'sell' to potential supporters.

I imagine it would be much easier to find someone to conduct a cyber attack on a facility on the other side of the world, with minimal risk to the perpetrator, than it would be to find someone that would be willing to strap a bomb to their chest or fly a plane into a building. This opens up a whole new source of potential supporters for our most likely enemies.

Imagine the damage a knowledgeable hacker could do to our bulk electric system if they gained access to a regional transmission or generation operator's Energy Management System (EMS), the computer system used in the real-time control of the electric grid. At the very least, they could gain information on the system's critical assets and vulnerabilities, gathering intelligence for future operations or attacks. An attacker could also provide operator's with false data and alarms, causing them to take action that could potentially place the system in jeopardy. In the worst possible case, an attacker could take complete control of system assets and wreak havoc on the electric grid.

There are many other control systems associated with the grid as well, providing an attacker with multiple potential access points. These include communications networks that allow relay protection systems to talk with one another, as well as recently developed 'smart grid' systems that allow communication between multiple elements of the system, from the power plant to the end-user's meter.

With 33 million 'smart meters' projected to be installed by the end of 2011, and a total of 230 million by the end of 2015, we could be exponentially increasing the risk to the bulk electric system.

Securing the Electric System

On November 8, 2009, the CBS News show '60 Minutes' presented a report titled 'Sabotaging the System', highlighting many of the threats to the electric grid, as well as to other critical systems. There is no doubt that the threat is real, and the potential impact extreme. However, '60 Minutes' implication that the electric industry is doing nothing to address the issue is false.

There are many agencies currently evaluating the potential threats, and developing standard methods for addressing these threats; The US Department of Energy, the Federal Energy Regulatory Commission, the North American Electric Reliability Corporation, the North American Energy Standards Board, the National Institute of Science & Technology, and the wider industry itself, all realize the seriousness and urgency of the issue and are working diligently to develop mandatory standards and business practices that will tighten the security of the system.

However, the reality is that we will never be able to completely eliminate the cyber threat to the electric grid. Cyber security experts readily admit that hackers can overcome most security protocols within a short period of time, forcing security professionals to quickly modify their systems. This results in a continuous game of cat -and-mouse, one which exposes the system to a certain amount of risk.

This highlights the need for the industry to develop standard operating procedures and protocols for an operational response to successful cyber attacks. These plans must consider a number of important elements;

1. All cyber attacks will not be the same, therefore any response plan needs to be flexible enough to be used for a broad range of attacks.
2. Cyber security professionals & intelligence agencies must provide and continuously update industry planners with the most likely attack scenarios in order to ensure current and future response plans are effective.
3. Planners must determine the minimum level of acceptable operational control, and which critical assets and load centers must be included to regain and maintain that control.
4. Response plans must be coordinated between adjacent utilities and regions to ensure an effective recovery of the overall system.
5. Industry system operators must be trained to recognize potential cyber attacks, and on the implementation of the appropriate response plans.

The development of flexible, comprehensive response plans will shorten the downtime of the effected elements of the bulk electric system and ensure that our most critical systems, such as defense and emergency response facilities, are given first priority in the restoration of the grid. Failure to develop these plans could potentially expose the system and our wider infrastructure to further, more severe attacks.

Conclusion

The bottom line is that the cyber threat to the bulk electric system is real, but the appropriate agencies and the industry itself are working to mitigate the threats. However, this effort will require wider support in order to be successful, from political support at the National, State, and local level, down to the end users of the system.

Without the political will power to develop and enforce mandatory cyber security standards, there is no guarantee that everyone will take the steps necessary to secure their portion of the system. Without end user support and their willingness to accept higher electricity rates in order to fund the necessary security enhancements, the system will remain vulnerable.

Securing America’s energy future is everyone’s responsibility, and one we cannot fall short on.