THE CIP REPORT

CENTER FOR INFRASTRUCTURE PROTECTION VOLUME 10 NUMBER 9
AND HOMELAND SECURITY

MARCH 2012
CRITICAL MANUFACTURING

EDITORIAL STAFF

EDITORS
Devon Hardy
Olivia Pacheco

STAFF WRITERS
M. Hasan Aijaz
Shahin Saloom

JMU COORDINATORS
Ben Delp
Ken Newbold

PUBLISHER
Liz Hale-Salice

Contact: dhardy1@gmu.edu
703.993.8591

Click **here** to subscribe. Visit us online for this and other issues at
http://cip.gmu.edu

This month's issue of *The CIP Report* features the most recent addition to the U.S. Department of Homeland Security's Critical Infrastructure Sectors: Critical Manufacturing.

GEORGE MASON UNIVERSITY
School of Law
CENTER for INFRASTRUCTURE PROTECTION and HOMELAND SECURITY

First, we provide a brief overview of the Critical Manufacturing Sector. Then, we examine the current status of American manufacturing. A project manager and researcher from the University of Turku's Centre for Maritime Studies in Finland discusses the results of her analysis of a strike at public ports in March 2010 and its impact on Finnish critical manufacturing and foreign trade. Finally, an adjunst professor at George Mason University's School of Public Policy describes the critical infrastrucure transporation topics that were discussed at the annual conference of the Transportation Research Board (TRB) and the solutions that were proposed to protect the global supply chain.

This month's *Legal Insights* assesses the challenges involved with preventing the theft of copper, an important element in the power and communications sectors.

We would like to take this opportunity to thank the contributors of this month's issue. We truly appreciate your valuable insight.

We hope you enjoy this issue of *The CIP Report* and find it useful and informative. Thank you for your support and feedback.

Mick Kicklighter
Director, CIP/HS
George Mason University, School of Law

Legal Insights

Substations & Cell Towers: Stopping Copper Theft on a Budget

by Len Friedman, Ph.D.,
President and Founder,
Ultimate Security Products

The term "Critical Infrastructure Protection" has typically meant "expensive." This is no longer true. Affordable technology is proving effective and large scale deployment has become both necessary and economical. Critical infrastructure is already being targeted and destroyed — a victim of copper theft. Each year thousands of substations and cell towers are hit and stripped of their copper superstructure, grounding rods, and signal and power cables — threatening both the power and communications grid. The problem is simple: when substations and cell towers were built, copper prices were pennies per pound and it was not worth the effort to either steal it or secure it. Times have changed; copper is nearly $4/pound and the plague of copper theft is overwhelming utilities with substations unsecured and unprepared for the epidemic. The same issue is afflicting communications infrastructure, especially mobile phone networks, as each and every cell tower depends upon copper grounding cables to protect their expensive switching gear from lighting strikes. The grounding cables and copper bus-bars used to ground switching equipment are a literal gold mine to copper thieves — a problem demanding a solution that can be widely deployed to protect these remote assets.

Substations

It is not an exaggeration to claim that physical security at most of our Nation's substations consists of a simple padlock. That is why they are such wonderful targets. Once a crook learns how to avoid being electrocuted, the rest is easy. Unfortunately, the results for the power grid can be catastrophic, far beyond the gravel surface of a single substation. Substations interact with the grid through cables running in lightly covered cable troughs protected by a short chain link fence. Figure 1 illustrates a thief removing the top covers to gain access to the exposed cables. These signal/sensor cables relay information to the utility over the supervisory control and data acquisition (SCADA) network in real-time to manage the grid. If copper thieves unknowingly (or worse — perhaps some group actually understands the cause/effect) cut the signal cables and the sensor cables in their search for copper, overburdened transmission lines and transformers can fail and take down large sections of the power grid. Power transmission is based upon alternating current; if the grid is put out of phase,

(Continued on Page 9)

Legal Insights *(Cont. from 8)*

very bad and expensive things happen. A YouTube search for the "aurora project" shows what happens when "phase" is disrupted in a simulated cyber-attack; a massive generator is literally torn apart before the cameras. While high tech cyber-attacks inducing phase shifts may be complicated, jumping a chain link fence is not. This is literally all that it would currently take. Low level thugs selectively vandalizing the signal/sensor cables in unsecured substations can induce the same phase issues that will destroy even the largest generators that power our cities. If this happens to the grid, it could be months or even years before it was operational again. These critical points of vulnerability are located in remote areas, hidden from prying eyes and only protected by the proverbial padlock and swinging gate — a recipe for disaster. Based upon the current infrastructure, in a very real way cybersecurity is only as good as the physical security that protects the cables in the troughs. NERC (National Electric Reliability Corporation) has already looked into the subject, as we will see later.

The problem is one of economics. In today's economy, utilities simply cannot afford to spend tens of thousands of dollars to secure every substation — there are tens of thousands of substations in every area of the country. Cost is a key consideration for the investor owned utilities and even more so for the regional co-ops. To be effective, the typical closed-circuit television, or CCTV, surveillance systems demand prohibitively expensive operators monitoring the cameras 24x7; far too expensive for mass deployment beyond a few large sites. Other proposed solutions like "capacitive fences" that detect a body's mass as it approaches the fence create a tsunami of false alarms that make them impractical in real life. Every deer, raccoon, and dog that approaches the fence triggers an alarm. The old fashioned alarm systems no longer work for the same reasons — in many areas of the United States, police no longer respond to unverified alarms because of reduced budgets and resources. The local first responders need better actionable data before they deploy their resources.

The press and the utility regulators are beginning to recognize, however, that there is an affordable solution that is already proving effective. Videofied cordless intrusion alarms were developed specifically to deliver immediate police response to protect outdoor assets. *Transmission and Distribution World* (T&D World) ran a cover story on copper theft in their April 2010 issue, relating how the large investor-owned utilities had begun experimenting with MotionViewers, a wireless outdoor sensor/camera that detected crooks and sent the video clips over the cell network for immediate police response. Progress Energy and Northeast Utilities each reported that these video intrusion alarms were helping them make arrests and catch crooks before they were able to remove the copper. In a follow up article in October 2011, *T&D World* reported how a local co-op in the Carolinas, Blue Ridge Electric, installed the systems and were able to catch a gang that had been targeting their remote substations.

NERC provides oversight for utilities and develops "best practices" to address pressing issues. NERC recently sponsored a webinar on substation physical security at the end of November 2011.[1] The entire seminar underscored the threat that copper theft poses to our critical infrastructure and affordable video intrusion alarms were a proven solution. Brian Smith of Duke Energy (who had just acquired Progress Energy) presented on their successes using Videofied to make arrests at their substations. One big reason for the effectiveness of the MotionViewers is that law enforcement gives priority response to video verified alarms — police caught the crooks red handed. Successful protection in this example depended upon local law enforcement and low cost technology — not a massive billion dollar program. The International Assosiation of Chiefs of Police underscored this trend towards increasing the effectiveness of first responders with affordable technology. A recent case study in *The Police Chief Magazine* described how Detroit had installed wireless video alarms to protect vacant schools; over the 2011 school year they delivered a 70 percent arrest rate instead of the typical 12 percent. These systems

(Continued on Page 10)

[1] http://www.nerc.com/files/Physical%20Security%20Webinar%20Presentation.pdf.

Legal Insights *(Cont. from 9)*

cost 1/30th of the price of a typical surveillance system and were many more times effective in making arrests. Detroit secured 30 schools for the price of equipping a single school with unmonitored surveillance cameras. These are the same systems used to protect substations.

Cell Towers

Cell tower protection follows a similar pattern. Remote towers with elaborate copper grounding systems are an easy target for thieves. Many towers have been hit multiple times, bringing down the network and creating havoc with communications. Again, the primary physical security consists of a chain link fence and a padlock around the tower with a standard locked door on the shelter housing the switching gear. Figure 2 shows a thief breaking into a shelter to steal the copper grounding bars. Companies like AT&T, T-Mobile, Metro PCS, and Verizon have all turned to video verified alarms to solve the problem and make arrests, catching the crooks in the act. AT&T has literally hundreds of arrests and was instrumental in a case study published in *Above Ground Level* magazine. Like the substations, priority police response was a crucial element of the success. Local police response is the foundation to securing remote critical infrastructure.

Unfortunately, police response to traditional alarms is actually disappearing and people responsible for homeland security policies are not aware of this fact. Municipal and county budget cuts mean that police simply do not respond to traditional alarms in many areas of the country. Detroit is a good example. When hit with budget cuts, Detroit Police joined the growing trend and decided to end response to "blind" alarms because there simply were not enough officers to go around anymore. On August 16, 2011, in a *Detroit Free Press* feature article, Detroit Police Chief Ralph Godbee Jr. declared that any triggered alarm will require a verified response before dispatch sends a cruiser to the location. Godbee cited a U.S. Department of Justice report supporting verified response as a reliable practice towards eliminating waste and improving public service. Abandoning traditional alarms, Chief Godbee sees video verified alarms as the solution to more effective policing — using video to verify that the alarm is an actual crime. Detroit Police Commander Todd Bettison stated, "[o]ur main goal is to respond to crime, and if we can utilize modern technology, then so much the better. We feel very passionate about this. We've been looking at this for a long time and from what we've observed this is definitely the way to go."[2] It is also important to note that in many other areas, police have simply relegated alarm response to such a low priority that the response time is measured in hours not minutes. Video alarms that verify a crime-in-progress is different because police remain motivated to make arrests. In any case, affordable protection must still deliver law enforcement to be effective in securing critical infrastructure. In fact, local police response is probably the most crucial part of a real solution.

Even if it were the same cost, expensive video surveillance is not the answer. Most surveillance is NOT monitored in real-time. While it is true that high definition CCTV surveillance cameras and a video recorder can document an incident in high resolution for later

(Continued on Page 13)

2. This article is archived; however, a portion of this article can be found at http://www.securitysystemsnews.com/blog/detroit-no-longer-responding-unverified-alarms.

Legal Insights *(Cont. from 10)*

review by law enforcement, for the utility and the community, the crime has already happened, the power grid is already damaged, and it is already too late. Movie-quality video without real-time monitoring and immediate police response is a solution, but for other problems. Video quality is not the key issue; once a monitoring operator can tell that there is an actual crime and sends the police — that is sufficient, effective as well as less expensive. There are hundreds of video clips of arrests on YouTube taken outdoors and in difficult low-light conditions that prove the point. "Adequate video quality" means affordability and the good news is that video intrusion alarms themselves are a small fraction of the price of a high definition surveillance system. Police do not need Hollywood quality to make arrests; what they need is instant notification of a crime-in-progress. This is the best protection we can provide for our critical infrastructure, and it is affordable.

Conclusion

The success of these wireless video alarms has not gone unnoticed by law enforcement. The National Sheriffs Association recently took the unprecedented step and endorsed the Videofied outdoor intrusion alarm because it delivers more arrests, especially in the rural areas the sheriffs patrol. Cordless video verified alarm systems are an affordable effective option for mass deployment that will not break the bank — a reasonable and cost effective alternative to the padlock and the fence that we now depend upon to keep our power on and our communications networks operating. In conclusion, while it is true that securing critical infrastructure at every level may be an expensive proposition, delivering police protection to remote substations and cell towers is affordable enough to implement immediately and provide significant protection that is currently lacking — exposing our power grid to massive failure.

To view actual videos of these systems catching crooks visit: http://videos.tdworld.com/video/Catching-Copper-Thieves-in-the;Substations. ❖