THE CIP REPORT

CENTER FOR INFRASTRUCTURE PROTECTION VOLUME 10 NUMBER 9
AND HOMELAND SECURITY

MARCH 2012
CRITICAL MANUFACTURING

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

Critical Manufacturing Sector Overview

On March 3, 2008, the Critical Manufacturing Sector was established and became the newest of the 18 critical infrastructure sectors. The mission statement of the Sector is to "[r]educe risks to the Critical Manufacturing Sector through proactive prevention, preparation for and mitigation of natural and man-made threats leading to effective response and recovery through public-private partnership."[1] Sector members developed the following goals:

Goal 1: Achieve an understanding of the assets, systems, and networks that comprise the critical infrastructure of the Critical Manufacturing Sector.

Goal 2: Develop an up-to-date risk profile of the assets, systems, and networks within the Critical Manufacturing Sector that will enable a risk-based prioritization of protection activities.

Goal 3: Develop protective programs and resiliency strategies that consider the physical, human, and cyber elements of sector infrastructure and address sector risk without hindering economic viability.

Goal 4: Create a means of measuring the progress and effectiveness of Critical Manufacturing Sector CIKR protection activities.

Goal 5: Develop processes for ensuring appropriate and timely information sharing between government and private sector partners in the Critical Manufacturing Sector.[2]

In order to achieve these goals, the Sector is following the six-step process laid out in the National Infrastructure Protection Plan's (NIPP) risk management framework. The steps in this framework are to (1) set goals and objectives; (2) identify assets, systems, and networks; (3) assess risks; (4) prioritize; (5) implement protective programs and resiliency strategies; and (6) to measure effectiveness.[3] The application of the NIPP framework to the Sector is laid out in the Sector Specific Plan (SSP).

The SSP for critical manufacturing describes several features of the Sector that make it particularly challenging. One defining characteristic of the Sector is that modern manufacturing is a very interdependent process relying on large networks of distributors, contractors, and vendors that form a supply chain which crosses international borders. These long supply chains and the manufacturing process itself creates internal dependencies as well as external dependencies with the Transportation Systems, Energy, Emergency Services, Information Technology, Defense Industrial Base, Communications, and Chemical Sectors.

The great diversity of risk and the broad scattering of sector companies across the country makes an exhaustive vulnerability and risk assessment analysis of all facilities and systems infeasible. Instead, a three step process was adopted to efficiently assess risk across the Sector. The first step was to define functional areas. When this was completed, four broad categories were identified: (1) Primary Metal Manufacturing; (2) Machinery Manufacturing; (3) Electrical Equipment, Appliance and Component Manufacturing and; (4) Transportation, Equipment Manufacturing.

The next step is to analyze each functional area to determine if any organizations control enough of the market that their "incapacitation would result in nationally significant consequences."[4] Finally,

(Continued on Page 14)

1. *Critical Manufacturing Sector-Specific Plan (2010),* available at http://www.dhs.gov/xlibrary/assets/nipp-ssp-critical-manufacturing-2010.pdf.
2. Ibid.
3. *National Infrastructure Protection Plan* (2009), http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf.
4. *Critical Manufacturing Sector-Specific Plan (2010).* Available at http://www.dhs.gov/xlibrary/assets/nipp-ssp-critical-manufacturing-2010.pdf.

The Return of American Manufacturing

by Kendal Smith, J.D., CIP/HS Research Associate

When American companies began relocating their manufacturing operations overseas in the early 2000s, they cited lower costs as their primary motivation. Ten years later, the same reasoning is starting to bring many of them home. For anyone concerned about protecting our Nation's critical infrastructure, this reverse trend is good news.

Both business owners and government officials who previously extolled the economic benefit of cheap foreign labor are beginning to see the bigger picture. Namely, that labor cost is just one of many salient factors effecting production in an increasingly globalized world. Among other things, the loss of innovation, security risks, new technologies, and rising non-labor costs have necessitated a more comprehensive evaluation of foreign manufacturing.

When the offshoring craze first hit, its advocates claimed that outsourcing low-skill manufacturing jobs to low-wage economies would free up U.S. workers to focus on our greatest source of wealth creation — innovation. Thankfully, this lofty notion that research and development can be kept in-country while production occurs thousands of miles away has been debunked. Particularly in a world where "the interests of our global corporations and the interests of our country have diverged,"[1] it is evident that innovation follows manufacturing overseas, with the majority of the top U.S. R&D spending companies now maintaining R&D locations in China or India.[2] The result? America is fast-losing its innovative edge as design and operational facilities are emerging all over the globe.

This shift is not only economically detrimental, but has significant implications for national security. In a study evaluating the health of the U.S. defense industrial base, Dr. Michael Webber found that between 2001 and 2008, the height of the offshoring frenzy, 13 of 16 manufacturing sectors critical to U.S. military capabilities experienced significant "erosion."[3] Unlike the naturally occurring decline of industry due to technological advancement and decreasing demand, the products made in these sectors remain essential and are still experiencing demand growth.[4] While it might be cheaper to import goods manufactured overseas in the short run, an increased reliance on foreign manufacturing leads to a parallel increase of those nation's military and political influence within our borders and can leave us vulnerable in times of emergency.

Overseas manufacturing also results in greater risk to supply chains. Though globalization has reduced costs in many areas, it has generated a complex web of interdependent companies subjected to varying regulatory standards and responsible for differing aspects of the production process. The consequence is a security nightmare, with a multitude of opportunities for disruption — both accidental and intentional. As many of the international events of 2011 aptly demonstrated, whether it is political upheaval or the hand of Mother Nature, happenings abroad cause supply problems easily felt on American shores.

(Continued on Page 11)

1. *China's Five-Year Plan, Indigenous Innovation and Technology Transfers, and Outsourcing: Hearing Before the US-China Economic and Security Review Commission*, 112th Congress, (June 15, 2011), (Statement of Dr. Ralph Gormory, New York University Research Professor).
2. Ron Hira,. "The Globalization of Research, Development, and Innovation," in *Manufacturing a Better Future for America*, (ed.), Richard McCormack, (Alliance for American Manufacturing, 2009), Kindle edition.
3. Michael Webber, "Erosion of the U.S. Defense Industrial Support Base," in *Manufacturing a Better Future for America*, (ed.), Richard McCormack,. (Alliance for American Manufacturing, 2009), Kindle edition.
4. Ibid. These products include items such as circuit boards, batteries, optical instruments, semiconductors, and metal forming and cutting tools.

Critical Industries and a Port Strike: A Lesson for Preparedness

by Johanna Yliskylä-Peuralahti, Ph.D., University of Turku, Centre for Maritime Studies, Finland

Global trading networks could not exist without maritime transport. A majority of the goods we use every day are transported by the sea at some point of their product life cycle. For export-oriented countries and for countries whose industries are dependent on imported supplies, the role of maritime transport is fundamental. However, quite often only when problems occur, the true importance of the transports to companies and societies becomes visible. The volcanic eruption in Iceland in April 2010 stopping air traffic in Northern Europe, the United States and Canada, and the earthquake causing a tsunami in Japan in March 2011 are the most recent examples of severe disruptions stopping transports and causing considerable harm to societies and companies' supply chains worldwide. These disasters have been a wake-up call for many, and transport risk management is rising on the agenda for many companies and governments alike.[1]

In a networked world, companies face many threats that can cause negative consequences to their operations. These threats include environmental threats, such as natural disasters and pandemics; geopolitical matters, such as conflicts and political unrest, import/export restrictions, and terrorism; economic triggers, such as sudden demand shocks; and technological failures, such as information and communication disruptions and transport infrastructure failures. Many of these threats are beyond the control of individual companies alone. Companies have also become more vulnerable to transport risks now more than ever before because they have global and lean operating models with specialized and interconnected production networks.[2]

This article shows what happens when companies face a transport disruption caused by a strike. A strike at the public ports in March 2010 stopped approximately 80 percent of the Finnish foreign trade. The exporting companies estimated they suffered 100 million Euro (135,8 US dollar) lost foreign sales per day because of the strike.[3] As a result of the strike, Finnish companies could not export their products and/or import raw materials, components, and spare parts. They had to find other alternatives in order to be able to continue their operations.[4] Discussions with the representatives of the companies on the subject of how they managed to continue their operations during the strike and what problems they faced thus gave us very practical insights about companies' preparedness towards transport disruptions in general.

How were Companies able to Cope when Ports were Closed?

For a country like Finland, a strike closing ports is very harmful because nearly 80 percent of the country's foreign trade is transported by the sea and land transport options are limited. A majority of the Finnish maritime traffic is feeder traffic to and from the ocean ports in Antwerp, Rotterdam, and Hamburg in

(Continued on Page 5)

1. J. Evans, "Weathering the Storm," *The Wall Street Journal*, (February 7, 2011), http://online.wsj.com/article/SB10001424052748703296604576005060742737534.html?mod=WSJ_business_LeftSecondHighlights.
2. World Economic Forum, "New Models for Addressing Supply Chain and Transport Risks," (2012), http://www3.weforum.org/docs/WEF_SCT_RRN_NewModelsAddressingSupplyChainTransportRisk_IndustryAgenda_2012.pdf.
3. Reuters Helsinki, "Finnish Port Strike Negotiations Planned for Tuesday," (March 7th, 2010), http://www.reuters.com/article/2010/03/07/finland-strike-idUSLDE6260I820100307.
4. This article is based on the results of a study focusing on the importance of maritime transports on the security of supply in Finland, see Yliskylä-Peuralahti et. al, "Finnish Critical Industries, Maritime Transport Vulnerabilities and Societal Implications," (2011), http://www.merikotka.fi/uk/STOCA.php. Representatives of 19 companies in different critical industries (energy production, food supply & food exports, chemical production, pharmaceuticals & healthcare supplies, forestry, metal production, electronics and freight forwarding) were interviewed for the study.

Ports *(Cont. from 4)*

Continental Europe, where goods are either reloaded to/from inter-continental vessels, or from where the goods continue their journey by other transport modes to their final destination. When public ports in Finland were closed because of the strike of the stevedores, the feeder vessels delivering the containerized goods to and from the overseas ports stopped running as there was no cargo to transport. Shipments in bulk form were only possible via private, industry-owned ports. However, this private port option was available for some companies only, so those companies had to wait until the strike was over to be able to transport their goods. During the strike, Finnish companies could either try to transport their goods in a truck by road via Sweden, or use liner ferries running between Finland and Sweden, Finland and Estonia, and Finland and Germany or use Swedish and Estonian ports for their shipments. To load the goods into ferries, the road haulage companies had to use their own drivers to drive truck and trailer combinations into the ferries.

When the ports were closed, Finnish companies did all they could to secure their procurement and the delivery of their products. Most companies were able to supply at least their key customers with the most essential goods and materials. The companies used a combination of several strategies in order to do this.[5] Preventive measures the interviewees used during the strike include:

- Raising inventory levels at their own and customers' sites before the strike began;

- Changing the delivery schedule, e.g. making orders of incoming supplies earlier and/or postponing orders to customers if possible;

- Changing the transport mode and route if possible;

- Having spare capacity (e.g. in production or storage), using several transport companies;

- Supplying the customer from another site (outside Finland) among the corporation's network producing the same or suitable products and transferring customer orders between the plants. However, many companies have specialized production plants producing only certain products with no compensatory production elsewhere; and

- Buying finished or semi-products from a competitor to fulfil delivery contracts to customers in case the company's own production had to be stopped, e.g. due to shortage of raw materials caused by the transport disruption.

However, depending on the industry, ways to cope with maritime transport disruptions can be quite limited. Many companies in the Finnish export industries transport goods with very specialized characters, such as chemicals or large and heavy equipment. Therefore, maritime transport cannot be replaced by any other transport mode. In addition, companies have adopted lean strategies, having goods in stock ties capital so all the companies regardless of industry try to keep their stocks at a minimum. Reliability of the deliveries is thus the main concern for all companies. For these reasons, possibilities to prepare against the transport disruption caused by the strike varied between industries. Industries that suffered the most during the port strike in Finland were the county's main export sectors, including forestry, chemicals, production of metals and machinery, and also food. Products requiring temperature controlled transport, including pharmaceuticals and food, do not bear interruptions at all in the transport chain and are thus very vulnerable. Companies in the process industries, such as chemical, forestry, and steel industries, transport large amounts (several thousand tonnes) of both raw materials and finished products. In addition, these industries have constantly running processes which are dependent on continuous, daily delivery of raw materials and continuous transports carrying finished products. For those companies, both the lack of availability of raw materials and/or difficulties delivering the finished product can cause production reduction or even stoppage immediately, resulting in considerable economic loss. Some companies found that none of their mitigation strategies worked when

(Continued on Page 12)

[5] For a more detailed analysis see: J. Yliskylä-Peuralahti, M. Spies, and U. Tapaninen, "Transport Vulnerabilities and Critical Industries: Experiences from a Finnish Stevedore Strike," *International Journal of Risk Assessment and Management*, 15: 2/3, (2011), 222-240.

Critical Transportation Infrastructure: A Multi-Faceted Discipline

by Irvin Varkonyi,
Adjunct Professor, George Mason University, School of Public Policy

Transportation has evolved as a multi-faceted discipline based on its role as the economic engine of the Nation (and the globe) and more recently, how its vulnerability to disruptions inflict adverse consequences to the Nation and the world. The annual conference of the Transportation Research Board (TRB), held in Washington in January 2012, offered several perspectives on transportation infrastructure protection including disaster logistics, transportation cybersecurity, emergency response planning, and global standards in supply chain security. A significant dilemma faced by transportation infrastructure is managing the dual challenges of optimizing operational performance while minimizing operational vulnerabilities.

Logistics Issues during Large-Scale Emergencies

One panel discussed supply chain and logistics issues during large scale emergencies. We know that as an emergency unfolds, it impacts the normal state of transportation, disrupting travel and cargo movement. This occurs simultaneously with the urgent need to provide relief materials to disaster victims. Thus, strengthening transportation systems to become more resilient will benefit the normal state by minimizing the impact of a disruption and benefits disaster management networks by mitigating the impact of a disaster. There is a burgeoning research community which focuses on Humanitarian Logistics, along with its differences with Commercial Logistics. Dr. Jose Holguin-Veras, and his team from Rensselaer Polytechnic Institute, proposed the thesis that an emergency can become a disaster and a disaster can become a catastrophe based on the level of capabilities in transportation systems.

Humanitarian Logistics can be defined as "a branch of logistics which specializes in organizing the delivery and warehousing of supplies during natural disasters or complex emergencies to the affected area and people."[1] Holguin-Veras identified Humanitarian Logistics Structures that deal with emergencies. "Three structures emerged in the research with vastly different network topologies: Agency Centric Efforts, Partially Integrated Efforts, and Collaborative Aid Networks."[2] The Agency Centric Model is utilized by traditional non-governmental organizations where single agencies effect distribution of relief goods directly to victims. They can be constrained by the inability of transportation infrastructure to allow them to reach victims.

The second model, Partially Integrated Efforts, may involve multiple agencies who work together with wholesale as well as retail distribution points. The third model, Collaborative Aid Networks, enhances collaboration among providers and expands distribution beyond traditional wholesale and distribution points. In Haiti, the infrastructure was so damaged that aid agencies did not have the means to distribute relief goods nor did victims have the means to reach distribution centers. One solution was to use the network of thousands of churches in Haiti, as well as the neighboring Dominican Republic, as distribution points. Individuals in non-affected churches reached distribution points and then used their church/parishioner networks to connect with victims.

On the same panel, a presentation was offered by the American Logistics Aid Network (ALAN.) This is a network composed of nearly 20 supply chain associations whose members volunteer to help

(Continued on Page 7)

1. Holguin-Veras, et al., "On the need to reformulate Humanitarian Logistics Modeling: Deprivation Costs, and Material Convergence," (2011).
2. Holguin-Veras. TRB presentation, "The Lessons of Haiti and Japan Disasters for Humanitarian Logistics." (January 2012).

Transportation *(Cont. from 6)*

disaster victims. These associations, including the Council of Supply Chain Management Professionals, American Production and Inventory Control Society, Association for Operations Management, and others who are experts in delivery in the normal state, compose ALAN membership. Through ALAN, best practices are applied, based on experience and collaboration, to utilize transportation infrastructure in understanding the impact of damaged networks. ALAN provides a primary point of contact for the U.S. logistics industry's donation activity and information. Everyone wants to be generous to help disaster victims but the state of logistics during and following a disaster requires expertise to maximize the amount of relief reaching victims as rapidly as possible with minimum loss of relief goods.

This author also spoke on this panel, illustrating the capabilities of global supply chains. These capabilities may also exacerbate vulnerabilities, which jeopardize supply chains. In the case of the earthquake in Japan, and subsequent tsunami (see *The CIP Report, July 2011*), several electronic goods supply chains, including Apple's Ipad, were adversely affected because key suppliers were taken down during the disaster. The impact of the disaster was magnified because significant, and in some cases, most of the components were made by a single supplier in a disaster prone region. The catastrophe exposed the vulnerability of these systems.

The Role of Academia in the Nation's Critical Transportation Infrastructure

Academia was also a focus of the TRB Committee on Critical Transportation Infrastructure Protection. The session, *Harnessing Academic Expertise to Address the Nation's Critical Transportation Security Challenges*, brought together several of the Nation's Centers of Transportation Security Excellence, including Rutgers University, University of Connecticut, Stevens Institute of Technology, and George Mason University (GMU). Shahin Saloom represented GMU's Center for Infrastructure Protection and Homeland Security (CIP/HS) and spoke on the new series of course syllabi designed by CIP/HS on the topic of critical infrastructure protection.

Rutgers demonstrated its research efforts for development of educational/training videos for transportation employees and research on the development of specific models and decision support systems for the U.S. Coast Guard and Amtrak. Stevens' focus was on research projects for maritime transportation and port security while the University of Connecticut focused on the university's role in the use of transition technology, using case studies/scenarios to illustrate the range of transportation activity and issues. This author also participated on the panel and focused on the delivery of transportation security education to undergraduate and graduate students. Multiple delivery models are available in addition to traditional face to face learning in brick and mortar institutions. Virtual universities with all classes online as well as hybrid education, which combine face to face learning with online learning, have become extremely popular.

Transportation Cybersecurity

Transportation cybersecurity was a main focus of a panel which asked the questions: how secure are your car, plane, and other transportation systems? Increasingly, technology is an enabler for transportation systems. Great improvements were noted which have taken place in transportation efficiency because of technology. Yet simultaneously, we see increased vulnerability has also been experienced. Are planes more efficient and safer with fly by wire technology driven flight systems? Consider the crash of the Air France A-380 on a flight between Brazil and France. The plane dove almost vertically into the South Atlantic as systems malfunctioned but the pilots were not able to react with sufficient skills or capabilities, in part due to training or lack of training, in dealing with the situation they encountered. Reliance on systems to fly and correct malfunctions left the human factor in uncertain limbo. Vulnerabilities of transport systems to technology hacking and malfunction is real. El-Al Israel airlines was recently shut down for several hours while hackers crashed its passenger reservation system. This is thought to have been part of the conflict between Israel and some

(Continued on Page 14)

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.

Manufacturing *(Cont. from 3)*

The innumerable links in the supply chain coupled with the growing dependence on information technologies offer ample opportunity for terrorist infiltration and cyber espionage. There is particular concern over the amount of counterfeit goods flooding U.S. markets from China, a significant portion of which are electrical components indispensable to our defense ability. Not only do these inferior products create massive profit losses and consumer safety concerns, but they can easily wreak havoc within our military systems.[5] When more of the production process is conducted within U.S. borders, these risks are greatly diminished, simply due to greater operational control and the reduction in cross-border transfers.

Finally, the manufacturing industry itself is on the verge of a revolutionary change that many believe is on par with the invention of the assembly line. Though still in the early stages, engineers have begun harnessing computational power to "print" three-dimensional objects. Basically, thin layers of material comprised of powdered metals and resins are printed layer by layer according to complex two-dimensional base patterns, which are then added to a third dimension to complete a specified product.[6]

Widespread Internet access and integrated systems are also enabling cost-effective small-scale orders.[7] Such advancements are "moving manufacturing closer to the point of purchase,"[8] and the United States is in prime position to take the lead in developing and implementing these technologies.

As emphasized in the President's recently released *National Strategy for Global Supply Chain Security*,[9] all of these issues highlight the need for every level of government to partner with private industry in the effort to minimize risks and encourage innovation. This includes providing incentives tied to inshore manufacturing such as tax breaks, workforce training, and R&D funding. Fortunately, the primary draw of foreign markets, cheap labor, is becoming less influential in the overall production process. While labor costs have remained fairly stagnant in the United States, they are increasing by as much as 15-20 percent each year in developing nations such as China.[10] Coupled with a much higher U.S. productivity rate, this trend is quickly narrowing the gap between foreign and domestic labor costs, especially in small towns and rural areas. Moreover, the many costs associated with transportation and energy are rising steadily across the globe, further contributing to the appeal of in-shore manufacturing. As these foreign economies continue to grow, overseas manufacturers are shifting focus to supply local markets.

Obviously, U.S. overseas manufacturing is not coming to an end. Nor should it. The numerous advantages of a progressively more connected and open global society are real. But, Americans cannot afford to be blinded by short-term benefits at the expense of our long-term economic and physical security. A comprehensive examination of global market behavior and emerging technological capability reveals that a robust industrial base is essential to our national defense as well as our economic prosperity. ❖

5. Mike Collins. "How China is Stealing our Secrets," Manufacturing.Net, (January 12, 2012), accessed Feb. 12, 2012, http://www.manufacturing.net/articles/2012/01/how-china-is-stealing-our-secrets.
6. Mark P. Mills and Julio M. Ottino. "The Coming Tech-led Boom," *The Wall Street Journal*, (January 30, 2010), accessed Feb 12, 2012, http://online.wsj.com/article/SB10001424052970203471004577140413041646048.html.
7. David Bourne. "Trends and the Future of American Manufacturing," in *Manufacturing a Better Future for America*, ed. Richard McCormack. (Alliance for American Manufacturing, 2009), Kindle edition.
8. Ibid.
9. Available at http://www.whitehouse.gov/sites/default/files/national_strategy_for_global_supply_chain_security.pdf.
10. Harold L. Sirkin, Michael Zinser, and Douglas Hohner, *Made in America, Again: Why Manufacturing Will Return to the U.S.* (The Boston Consulting Group, August 2011), http://www.bcg.com/documents/file84471.pdf.

Ports *(Cont. from 5)*

ports were closed. The forestry industry was one of the sectors which had to stop factories as a result of the strike. According to forestry companies, over 60 percent of the paper production in Finland was stopped because of the strike, causing 2.5 to 3 million Euro losses per day to the companies. Timber production was not stopped as largely as in the pulp and paper production, but the industry suffered losses of export revenues.[6] If the strike had continued longer, suppliers of the forestry production (e.g., companies producing chemicals for pulp production) would have been forced to diminish or shut down their production.

Implications for the Security of Supply

The Finnish stevedore strike in spring 2010 made visible the Finnish society's dependency on maritime transports very concretely because many critical supplies, including energy, pharmaceuticals, and raw materials needed in export industries, are imported to the country. Furthermore, for many of the companies in the critical industries, maritime transport is the only transport mode they can use. Compared with many other threats transport chains are facing, such as accidents, natural disasters, or terrorism, a strike is different as there usually is a warning given beforehand, allowing the companies to make preparations. This was the case with the Finnish strike: a strike warning was given two weeks before. After that, the parties tried to negotiate to solve their conflict. The companies could use this time for making preparations towards the upcoming stoppage in transports. How well these chosen preparatory measures actually worked in practise was then put to a test during the strike. While the majority of the companies could continue their operations and fulfill customer orders during the 16 days the strike lasted with the special arrangements they had made beforehand, some companies in the process industry were forced to shut down production only a few days after the strike had started. This shows how dependent many industries are on continuous transports. Had there not been a warning about the strike, or had the strike lasted for a longer period, e.g. a month, or involved land transport, several companies in other industries (besides process industry) would have faced serious trouble and would have been forced to shut down production within a few days.

For all companies regardless of industry, the strike closing the ports in Finland was a concrete learning experience for the importance of being prepared for unexpected events: the strike made them re-think their preparedness towards transport disruptions in general. Even though in Europe strikes are a fairly common reason for causing a stoppage in transports,[7] the companies we interviewed said a strike closing all the ports at the same time was actually a very rare event and for that reason, many of our informants admitted their companies were rather ill-prepared for such events. Many companies thus realized they need to adapt their long-term countermeasures against such events and transport risks in general. Our results also show that preparing for transport disruptions can be quite difficult, as there are many matters that are not in their own hands. Both companies and governments should be aware of vulnerabilities like this and work together to build resilience capacities so that they would be able to respond and recover quickly when something unexpected happens.

Acknowledgements

The paper is based on the research project "Study of Cargo Flows in the Gulf of Finland in Emergency Situations" (STOCA), financed by the Central Baltic INTERREG IV A programme 2007-2013 of the European Union Regional Development Fund, Regional Council of Southwest Finland, Estonian Maritime Academy and National Emergency Supply Agency. The STOCA project focused on improved sustainable accessibility and transport of cargoes in the Baltic Sea region, with emphasis in particular on economical and environmentally sustainable cargo transportation in emergency situations. The paper reflects the views of the authors. ❖

6. Helsingin Sanomat, International Edition, "Harbour Strike Shuts Down Most of the Forestry Industry Output," (February 13, 2010), http://www.hs.fi/english/article/Harbour+strike+shuts+down+most+of+Finnish+forest+industry+output/1135254453770; and Finnish Forest Industries, Press Release, "Mills Starting up Gradually, Impacts of Stevedore Strike Will be Felt for Quite Some Time, (March 19, 2010), http://www.forestindustries.fi/juurinyt2/Tiedotteet/Pages/Millsstartingupgradually.aspx.

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. ❖

Transportation *(Cont. from 7)*

of its Middle East neighbors.

Conclusion

The Nation's critical transportation infrastructure is viewed far differently than it has been in the past. We find that emergencies can become far worse if transportation is not prepared to meet the unique and uncertain demands of disruptions. Academia has a role in transportation infrastructure protection by conducting research on transportation changes' impact on infrastructure. We must consider efficient operations equally to vulnerability mitigation of these operations. We note that transportation cybersecurity poses increased opportunity and risk. ❖

Overview *(Cont. from 2)*

each functional area would then be assessed again to determine if there are any suppliers who have enough of a market share that their incapacitation would create similar consequences. Once the critical organizations have been identified a risk analysis will be conducted which uses the variables of "consequence, vulnerability, and threat information "to arrive at a baseline of risk information."[5]

The members of the Critical Manufacturing Sector have made great strides in the few years since it has been established and its successes is largely owed to the close coordination between private and public sectors through the Government Coordinating Council and the Sector Coordinating Council. As the Sector matures, close attention will be paid to encompassing more of the owners and operators that are part of the Sector and applying DHS R&D to solving the issues of the day. ❖

5. Ibid.

The Center for Infrastructure Protection and Homeland Security (CIP/HS) works in conjunction with James Madison Univerity and seeks to fully integrate the disciplines of law, policy, and technology for enhancing the security of cyber-networks, physical systems, and economic processes supporting the Nation's critical infrastructure. The Center is funded by a grant from the National Institute of Standards and Technology (NIST).

If you would like to be added to the distribution list for *The CIP Report*, please click on this link:
http://listserv.gmu.edu/cgi-bin/wa?SUBED1=cipp-report-l&A=1