THE CIP REPORT

CENTER FOR INFRASTRUCTURE PROTECTION AND HOMELAND SECURITY

JUNE 2013
ENERGY

VOLUME 11 NUMBER 12

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

Follow us on Twitter here
Like us on Facebook here

This month's issue of *The CIP Report* focuses on the Energy Sector. Consisting of electricity, petroleum, and natural gas, Presidential Policy Directive-21 identifies the Energy Sector as particularly crucial because of its "enabling function" across all other sectors. Our authors highlight some of the unique threats to this sector, as well as several initiatives to enhance its security.

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

First, Dr. Jeffrey Tang provides a breakdown of energy usage in the United States, along with its implications for the future. Seth Grae, President of Lightbridge Corporation, then discusses the Virginia Nuclear Energy Consortium as a conduit for Virginia to become the Nation's nuclear power hub. We then reproduce former Director of Central Intelligence R. James Woolsey's recent Congressional testimony on the threat of electromagnetic pulse. Canadian Security Advisor Craig Thompson next analyzes the threat to transformer stations, and Brigham McCown of United Transportation Advisors examines the need to protect pipelines from cyber attack. GridPoint's Mark Straton then explains how data driven energy management reduces costs and encourages business continuity. Finally, CIP/HS Associate Director Dr. Mark Troutman outlines the Center's recent partnerships in energy research and education.

We would like to take this opportunity to thank this month's contributors. 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

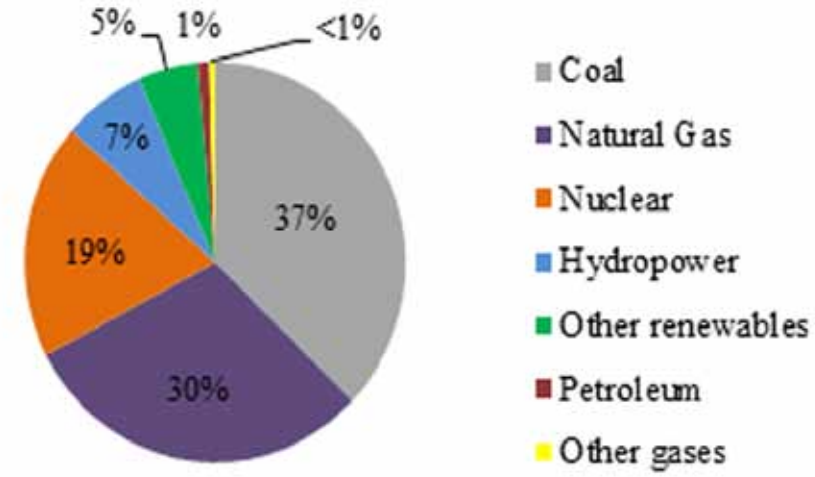
Oil and Gas Boom and the Future of Energy in the United States

by Jeffrey Tang, Ph.D., Associate Professor, Department of Integrated Science and Technology, James Madison University

Energy has been and continues to be a major vulnerability for the United States. The rise in hydrofracking presents an unmitigated boon in the short- and medium-term, but may threaten the development of nuclear power and renewable energy that we believe is essential to our long-term energy future.

The United States is heavily dependent on imported oil for its transportation, importing more than 3 billion barrels of oil every year since 1997.[1] More than 90% of all non-human transportation in the United States is powered by petroleum-based fuels.[2] The non-fuel energy picture is far rosier in terms of domestic supply and energy independence. The United States is blessed with copious reserves of coal, amounting to just over one-fourth of all the coal worldwide.[3] Though coal-fired plants still provide more of our electricity than any other source, the past decade has seen the portfolio of sources for U.S. electricity generation broaden considerably. In 2012,

Figure 1. Share of Total U.S. Electricty Generated, 2012 (%)



coal fell to just 37% (compared with over 50% in 2003) whereas natural gas rose to 30% of total electricity generation, with nuclear (19%), hydropower (7%), and other renewables (5%) providing most of the rest (see Figure 1).[4]

Outside of fossil fuels, nuclear power continues to be our leading energy source, accounting for nearly two-thirds of the emission-free energy produced in the United States.[5] Years of rising oil prices and concerns about greenhouse gas emissions led to a global nuclear-energy renaissance prior to the Fukushima disaster in 2011. Afterwards, concerns arose on the safety and security of nuclear energy production, in addition to

(Continued on Page 3)

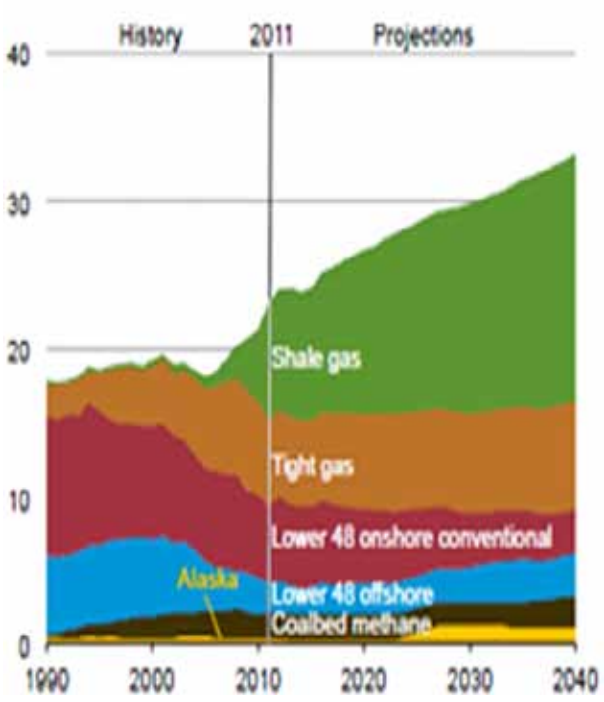
[1] U.S. Energy Information Administration. "Petroleum & Other Liquids," http://www.eia.gov/dnav/pet/hist/leafhandler.ashx?n=pet&s=mcrimus1&f=a (accessed May 27, 2013).
[2] In April 2013, 93% of energy in the U.S. transportation sector was petroleum-based. Institute for Energy Research. "Petroleum (Oil)." http://www.instituteforenergyresearch.org/energy-overview/petroleum-oil/ (accessed May 27, 2013).
[3] U.S. Department of Energy. "Coal: our most abundant fuel." http://www.fossil.energy.gov/education/energylessons/coal/gen_coal.html (accessed May 27, 2013).
[4] U.S. Energy Information Administration. "What is U.S. electricity generation by energy source?" http://www.eia.gov/tools/faqs/faq.cfm?id=427&t=3 (accessed May 27, 2013). The 2003 figure from: Texas State Comptroller. "Energy Reports: Coal." http://www.window.state.tx.us/specialrpt/energy/nonrenewable/coal.php (accessed May 27, 2013).
[5] Nuclear Energy Institute. "Quick Facts: Nuclear Energy in America." Resources & Stats. http://www.nei.org/resourcesandstats/Documentlibrary/Reliable-and-Affordable-Energy/factsheet/nuclear-energy-quick-facts (accessed May 8, 2013).

(Continued from Page 2)
the challenging economic calculus driven by high construction costs and reliance on federally supported loans.[6] The current U.S. portfolio of nuclear power includes 104 nuclear reactors in 31 states, with five reactors currently under construction and an additional 14 licenses pending review.[7] Since 1990, technological advancements have led to an increase in efficiency equal to bringing 27 new reactors online. Despite these new projects, predicting the role of nuclear power in America's energy future is purely speculative until the Nuclear Regulatory Commission comments on the 14 licenses currently under review.

Spurred in part by high prices in the early 2000s, new sources of oil have extended the expected future supply of crude oil substantially. Unconventional oil sources like tar sands, heavy oil, and oil shale have made huge resources in the United States and Canada potentially economically viable—though energy-intensive to extract and refine—and accounting for more than half of the growth in new oil production worldwide.[8] Deep-water drilling has also expanded dramatically: even after the Deepwater Horizon spill, offshore (mostly deep-water) production accounts for nearly one-quarter of U.S. domestic oil production.[9] Enhanced oil recovery techniques including CO_2 injection have extended the potential life of many oil wells in the United States and elsewhere, currently accounting for 6% of domestic oil production. In all, oil production has enjoyed a renaissance, keeping global prices hovering around $100/barrel since 2011.[10] Much of this has been due to increased production in the Americas and other non-traditional regions, subtly changing the political geography of petroleum.

Similarly, the much-debated expansion of hydrofracking —a process in which water, sand, and chemicals are injected under high pressure into shale formations, which causes the natural gas to flow out of the shale for capture and use—has dramatically expanded U.S. natural gas production.[11] Proved reserves in the United States have risen to 318 trillion cubic feet, and have been increasing every year this century.[12] More importantly, most observers expect this trend to continue, greatly expanding natural gas production (see Figure 2).[13]

Figure 2: Natural Gas Production by Source, 1990-2040 (trillion cubic feet)



(Continued on Page 4)

[6] Mufson, Steven. 2012. "NRC Approves Construction on New Nuclear Power Reactors in Georgia," *Washington Post*, February 9. http://articles.washingtonpost.com/2012-02-09/business/35444551_1_nrc-chairman-gregory-jaczko-reactors-nuclear-power (accessed May 8, 2013).

[7] Holt, Mark. 2013. *Nuclear Energy: Overview of Congressional Issues*. Congressional Research Service, April 29.

[8] Young, Angelo. 2013 "IEA Says 'Supply Shock' From North American Shale And Tar Sands Is Transforming Global Energy Scene." *International Business Times*. May 27. http://www.ibtimes.com/iea-says-supply-shock-north-american-shale-tar-sands-transforming-global-energy-scene-1257095# (accessed May 27, 2013).

[9] U.S. Department of Energy. 2011. "Improving Domestic Energy Security and Lowering CO2Emissions with 'Next Generation'CO2-Enhanced Oil Recovery (CO2-EOR)." June 20. http://www.netl.doe.gov/energy-analyses/pubs/storing%20co2%20w%20eor_final.pdf (accessed May 27, 2013).

[10] U.S. Energy Information Administration. "Short-term Energy Outlook: Real Prices Viewer." http://www.eia.gov/forecasts/steo/realprices/ (accessed May 27, 2013).

[11] Ground Work Protection Council and ALL Consulting. 2009. "Modern Shale Gas Development in the United States: A Primer." http://energy.gov/sites/prod/files/2013/03/f0/ShaleGasPrimer_Online_4-2009.pdf (accessed May 27, 2013).

[12] U.S. Energy Information Administration. "Natural Gas Explained: How Much Gas Is Left." http://www.eia.gov/energyexplained/index.cfm?page=natural_gas_reserves (accessed May 27, 2013).

[13] Source of image: U.S. Energy Information Administration. 2013. *Annual Energy Outlook 2013 with Projections to 2040*. http://www.eia.gov/forecasts/aeo/pdf/0383%282013%29.pdf (accessed May 27, 2013).

(Continued from Page 3)

Because natural gas can be used for heating, cooking, electricity generation, and even powering vehicles (when compressed), a surge in natural gas supply might transform the U.S. energy landscape, though uncertainties regarding the magnitude of economically viable untapped reserves persist.[14] Debates over environmental concerns have raged in localities across the Nation where extraction through hydrofracking has been proposed or implemented, yet there is little indication that these concerns will halt or even substantially slow its expansion.[15]

The changes in the U.S. energy picture in recent years have thus been dramatic, though perhaps not transformative. The increased supply of oil has stabilized prices, though actual price decreases have not materialized because of growing demand worldwide. Indeed, there is no reason to believe that global demand for oil will decrease in the coming decade despite increases in vehicle fuel efficiency in the United States and elsewhere. In the United States, biofuels—most notably corn-based ethanol—have been a constant, if contentious, renewable energy source for transportation. Improvements in corn ethanol production techniques have improved the net energy balance, but its potential remains limited. Cellulosic ethanol is potentially transformative, offering the possibility of a much better energy balance, economic bottom line (eventually), and an escape from the food-fuel debates. Up to now, however, this promise remains largely unrealized.[16] Diesel is more problematic, with biodiesel production amounting to a tiny fraction of ethanol production, and algae-based diesel technology only a distant hope.

Electricity generation has changed substantially, with the most rapid growth coming from renewables (by percentage) and natural gas (by total generation). This is not purely coincidental, as the appeal of natural gas generators include substantially less start-up efficiency losses than coal-fired plants. Nevertheless, after coal, renewables have been the hardest hit by the boom in electricity generation from natural gas, as historically low commodity prices for gas make it nearly impossible for most renewables to compete in terms of generation cost per kw/h. In states without Renewable Portfolio Standards or similar policy tools in place, renewable energy systems face an uphill battle. Given that many of the most dynamic companies in this field lack extensive capitalization, short-term threats to revenue streams might set the industry back by a decade or more. Of the renewables, hydropower is the leading electricity generator, but there is little opportunity for substantial growth in this area unless micro-scale hydropower becomes more viable. Biomass, particularly woody biomass, is a popular source of heat in homes and its use as a renewable complement to coal in electricity generation has taken off, with many co-fired plants being built or retrofitted in recent years. Wind power has lower generation costs and more installed capacity than solar photovoltaics (PV),[17] though the collapse in prices in the PV market in 2011-12 may provide a real opportunity for more rapid growth. Despite its excellent potential in certain geographic regions, geothermal energy generation is growing very slowly in the United States and abroad.[18]

In the longer term, numerous issues and uncertainties pose concerns for U.S. security and prosperity. Given the dominance of fossil fuels as energy sources both in the United States and more globally, questions

(Continued on Page 5)

---

[14] Lee, A. et al. National Renewable Energy Laboratory. "Synergy Between Natural Gas and Renewable Energy in the Electric Power and Transportation Sectors." http://www.nrel.gov/docs/fy13osti/56324.pdf (accessed May 29, 2013).

[15] For example, see: Nolon, J. & Polidoro, V. 2012. "Hydrofracking: Disturbances Both Geological and Political: Who Decides?" *The Urban Lawyer* 44 (2012): 507-532. http://www.planning.org/audioconference/frackingre/pdf/UrbanLawyerFracking.pdf.

[16] U.S. Energy Information Administration. "Today in Energy: Cellulosic biofuels begin to flow but in lower volumes than foreseen by statutory targets." 2013 (Feb. 26) http://www.eia.gov/todayinenergy/detail.cfm?id=10131 (accessed May 29, 2013).

[17] U.S. Energy Information Administration. "Short-term Energy Outlook Renewables and CO2 emissions." http://www.eia.gov/forecasts/steo/report/renew_co2.cfm (accessed May 29, 2013).

[18] Musolino, E. "Global Hydropower and Geothermal Growth Slow." Environmental News Network 2013 (Feb.15). http://www.enn.com/energy/article/45602 (accessed May 29, 2013).

(Continued from Page 4)

about the size of viable reserves of both oil and natural gas loom large. If technological developments continue to expand the scope of such reserves, continuing increases in demand might be largely offset by new production. The political geography of non-conventional oil and shale gas potentially offers a much more stable and conflict-free supply chain than in traditional markets. Many are skeptical, however. It is not clear whether the promised vast reserves really are viable, and even if they are, if we will expend more energy and more money on extraction and refinement than are yielded in a final product. Additionally, non-conventional oil and shale gas both pose serious environmental risks that have caused considerable political controversy in the United States and abroad.

Another major uncertainty in energy markets is the price of carbon. In the United States, carbon emissions are still essentially costless, which removes a major disadvantage of fossil fuels from pricing considerations. Should a viable and legally enforced price on carbon emissions emerge, the economics of the industry might shift, potentially dramatically. While natural gas has much lower CO2 emissions than coal, nuclear and renewables have no greenhouse gas emissions at all associated with energy generation. Nuclear power can provide a large amount of baseline power with low operating costs, but comes with its own environmental and safety concerns. Fukushima was the latest mishap reminding us of the low-probability, high-risk dangers associated with nuclear power plant operation. Spent nuclear fuel—of which there is currently 68,000 metric tons stored on-site at 72 nuclear power plant facilities across the Nation—is another major environmental and security concern that is dealt with by a public-private partnership between the federal government and nuclear power plant operators.[19] Although Yucca Mountain in Nevada was chosen as the site for a permanent repository, in 2010 those plans were suspended because of construction delays, public protests by Nevadans, and other political and technical concerns.

In the long-term, renewable energy sources will be necessary for continued prosperity and security. The challenge lies in knowing how urgent the need to shift to renewables is. Europe has adopted very aggressive policy measures including feed-in tariffs to promote renewable energy, and with substantial success.[20] The United States lags far behind in this respect, and the recent oil and natural gas boom simply makes developing a strong domestic industry in renewable energy more difficult. Whether the considerable short-term benefits of the oil and gas boom outweigh the longer-term risk of delaying progress on renewables remains to be seen. ❖

[19] U.S. Department of Energy. 2013 (3). Strategy for the Management and Disposal of Used Nuclear Fuel and High-Level Radioactive Waste, January 11.

[20] For example, Portugal derived 70% of its energy from renewable sources during a 3-month period recently. Koronowski, R. (2013) "Is 70 Percent Renewable Power Possible? Portugal Just Did It For 3Months." http://thinkprogress.org/climate/2013/04/14/1858811/is-70-renewable-power-possible-portugal-just-did-it-for-3-months/?mobile=nc (accessed May 29, 2013).

Virginia—The Center for Nuclear Energy?

by Seth Grae, President and CEO, Lightbridge Corporation

When you think of Virginia, what comes to mind? The birthplace of our Nation, military, Government? Perhaps, but the Virginia Nuclear Energy Consortium (VNEC) is a twenty first century concept designed to change this and make Virginia a national and global leader in nuclear energy. Can it succeed? Can a state form an entity that makes companies and other entities in it collectively a leader in a global industry? The way Virginia is approaching VNEC, it has a good shot at succeeding.

The nuclear power industry does not have a center the way the theater industry has New York or the tech industry has Silicon Valley. Virginia aims to claim this. Other locations, including Chicago, have tried to establish a theater district to rival Broadway, but have not succeeded. Chicago has several theaters with plays and shows running in them, but few tourists visit Chicago for its theater scene, while thousands arrive in New York each day for that very reason. In Chicago there are touring productions and revivals of plays and shows that originated elsewhere, mostly in New York. A theater district is so much more than just theaters and shows.

The Success of Broadway

Strolling through New York's Broadway area, we see costume shops, rehearsal spaces, and all the "supply chains" that go into a vibrant theater district. The seed corn of off-Broadway, university theater departments, history, and strong New York City support—such as TKTS, where same-day half-price tickets are sold for shows to many of those thousands of tourists who arrive each day—add support. This cohesion, along with the rich industry history seals New York City as the home for Broadway.

What can Virginia learn from the success of Broadway in New York? In a word—synergy. Success requires a coherent and resilient supply chain from design through delivery to waste disposal of energy. Often it is a major advantage to have these technology and supply chain elements located in close proximity to enhance innovation and coordination. A ready source of demand located near the supply chain is useful as a spur of technological development.

One advantage for Virginia is its proximity to Washington, D.C. with its government agencies that the nuclear sector is involved with, including the U.S. Department of Energy, Nuclear Regulatory Commission, as well as Congress. VNEC deliberately aims to bring together into one community the intellectual supply chains of nuclear, similar to Broadway. Under new legislation, VNEC will come into existence on July 1, 2013. VNEC creates an Authority that will in turn establish a Consortium. The Consortium will be an interdisciplinary body, with a newly established VNEC Authority Board, drawing members from government, industry, and the private sector.

These members may each appoint a designee to represent their institution on the VNEC Authority Board, allowing experts to be leaders in this effort. The Governor will appoint the remaining board members, who represent the Commonwealth's energy industry, and research and education communities.

The intent of the Consortium is to serve as an interdisciplinary study, research, and information resource for Virginia on nuclear energy issues. This intentionally diverse representation is designed to set Virginia up for success. The legislation gives authority to establish an action structure to drive research, innovation, and professional education to create a safe, reliable, and resilient energy source for the Commonwealth and its surrounding areas.

First Mover Advantage

Virginia has a first-mover advantage. VNEC is unique. Virginia will be the only state to

(Continued on Page 7)

(Continued from Page 6)

formally bring together institutions of higher education, for-profit and not-for-profit entities, and research institutions to help them succeed in the nuclear power sector. Not only is the effort diverse like the theater district in New York, but the institutions are already established as experts, and are well known.

Virginia already houses many of these experts, and prior efforts show that the foundation has been laid in this endeavor. The World Nuclear Association estimates that approximately $1.5 trillion will be spent worldwide in construction of new reactors between now and 2030. Portions of that supply chain of goods and services can be provided by entities that are already here, or can be attracted to Virginia.

Virginia and the country can benefit from having a U.S.-based nuclear energy center. Will this effort be like the theater district in New York or in Chicago? That remains to be seen, but the structure is more similar to Broadway.

Adopting the Silicon Valley Culture

Another successful center that others have widely tried to emulate but none have succeeded is Silicon Valley. Silicon Valley has an ethos that attracts creative people and gives them an infrastructure where they can change the world. In addition, there is Stanford University, other research centers, successful technology companies, and venture capital firms. Silicon Valley also has a culture that does not regard failure as a negative, but rather as a learning experience without creating a stigma. Start-up companies strive to create value and protect their intellectual property. Once they create value, business people either arrange to join or even acquire the company to create profits for investors. This leaves the creative people who started the companies free to continue creating or adding value in the same company or by moving on. Virginia can attract and produce talented people who can move around through the life cycle of nuclear technologies and entities.

Nuclear power is technology-centered. The success of Silicon Valley lies in its creativity culture, which Virginia will need to foster. Can VNEC help Virginia become a nuclear "Silicon Valley"? In Virginia, there is a continued interest from academic institutions, research organizations, and private sector companies who are enthusiastic about establishing this culture and have a truly unique array of nuclear-related assets. Among the board members of the VNEC Consortium, there will be many that are analogous to the players in Silicon Valley. VNEC is designed to help kick-start a Silicon Valley-like nuclear center in Virginia.

Driving Towards Success

Virginia should take the lessons from both Broadway and Silicon Valley to leverage its success. The potential Virginia has to provide a unique benefit and culture to our citizens and the Nation is tremendous. Virginia is not waiting for the next big thing to happen before jumping on board. Instead, the Commonwealth is preparing a team to create the Center for nuclear energy. Just as synergy is necessary to drive technological development, thoughtful design will be necessary along the path from energy source through delivery and disposal to ensure that next generation nuclear power is safe, reliable, and resilient. In this regard, VNEC also provides the opportunity to enhance design and investment of security and resilience measures outlined in recent policy directives.

A coordinated structure that ensures vibrant innovation and designs critical infrastructure security and resilience will be a source of enduring value. VNEC is such a structure and signals a bright future for the prospects of next generation nuclear power and energy resilience within the Nation's overall energy portfolio. ❖

Testimony Before the House Committee on Energy and Commerce May 21, 2013

by R. James Woolsey

This hearing is about cyber threats and solutions. But I am going to talk about a dimension of the cyber threat that is not usually considered a cyber threat in Western doctrine, but is in the playbooks for an Information Warfare Operation of Russia, China, North Korea, and Iran. These potential adversaries in their military doctrines include as a dimension of cyber warfare a wide spectrum of operations beyond computer viruses, including sabotage and kinetic attacks, up to and including nuclear electromagnetic pulse (EMP) attack.

It is vitally important that we understand that a nuclear EMP attack is part of cyber and information warfare operations as conceived by our potential adversaries. Our cyber doctrine must be designed to deter and defeat the cyber doctrines of our potential adversaries by anticipating how they plan to attack us—but our doctrine currently does not.

Our cyber and information warfare doctrines are dangerously blind to the likelihood that a potential adversary making an all-out information warfare campaign designed to cripple U.S. critical infrastructures would include an EMP attack.

The assessment that nuclear EMP attack is included in the cyber and information warfare doctrine of potential adversaries, and the effects of an EMP attack described here, are based on the work of the Congressional EMP Commission that analyzed this threat for nearly a decade (2001-2008). The Congressional Strategic Posture Commission and several other major U.S. Government studies independently arrived at similar conclusions, and represent collectively a scientific and strategic consensus that nuclear EMP attack upon the United States is an existential threat.

What is EMP? A nuclear weapon detonated at high-altitude, above 30 kilometers, will generate an electromagnetic pulse that can be likened to a super-energetic radio wave, more powerful than lightning that can destroy and disrupt electronics across a broad geographic area, from the line of sight from the high-altitude detonation to the horizon.

For example, a nuclear weapon detonated at an altitude of 30 kilometers would project an EMP field with a radius on the ground of about 600 kilometers, that could cover all the New England States, New York and Pennsylvania, damaging electronics across this entire region, including electronics on aircraft flying across the region at the time of the EMP attack. The EMP attack would blackout at least the regional electric grid, and probably the entire Eastern Grid that generates 70% of U.S. electricity, for a protracted period of weeks, months, possibly years. The blackout and EMP damage beyond the electric grid in other systems would collapse all the other critical infrastructures—communications, transportation, banking and finance, food and water—that sustain modern civilization and the lives of millions.

Such an EMP attack, a nuclear detonation over the U.S. East Coast at an altitude of 30 kilometers, could be achieved by lofting the warhead with a meteorological balloon.

A more ambitious EMP attack could use a freighter to launch a medium-range missile from the Gulf of Mexico, to detonate a nuclear warhead over the geographic center of the United States at an altitude of 400 kilometers. The EMP field would extend to a radius of 2,200 kilometers on the ground, covering all of the contiguous 48 United States, causing a nationwide

(Continued on Page 9)

(Continued from Page 8)

blackout and collapse of the critical infrastructures everywhere. All of this would result from the high-altitude detonation of a single nuclear warhead.

The Congressional EMP Commission warned that Iran appears to have practiced exactly this scenario. Iran has demonstrated the capability to launch a ballistic missile from a vessel at sea. Iran has also several times practiced and demonstrated the capability to detonate a warhead on its medium-range Shahab III ballistic missile at the high-altitudes necessary for an EMP attack on the entire United States. The Shahab III is a mobile missile, a characteristic that makes it more suitable for launching from the hold of a freighter. Launching an EMP attack from a ship off the U.S. coast could enable the aggressor to remain anonymous and unidentified, and so escape U.S. retaliation.

The Congressional EMP Commission warned that Iran in military doctrinal writings explicitly describes making a nuclear EMP attack to eliminate the United States as an actor on the world stage as part of an Information Warfare Operation. For example, various Iranian doctrinal writings on information and cyber warfare make the following assertions:

- "Nuclear weapons...can be used to determine the outcome of a war... without inflicting serious human damage [by neutralizing] strategic and information networks."

- "Terrorist information warfare [includes]...using the technology of directed energy weapons (DEW) or electromagnetic pulse (EMP)."

- "...today when you disable a country's military high command through disruption of communications you will, in effect, disrupt all the affairs of that country....If the world's industrial countries fail to devise effective ways to defend themselves against dangerous electronic assaults, then they will disintegrate within a few years."

China's premier military textbook on information warfare, written by China's foremost expert on cyber and information warfare doctrine, makes unmistakably clear that China's version of an all-out Information Warfare Operation includes both computer viruses and nuclear EMP attack. According to People's Liberation Army textbook *World War, the Third World War—Total Information Warfare*, written by Shen Weiguang, "Therefore, China should focus on measures to counter computer viruses, nuclear electromagnetic pulse...and quickly achieve breakthroughs in those technologies...":

With their massive destructiveness, long-range nuclear weapons have combined with highly sophisticated information technology and information warfare under nuclear deterrence....Information war and traditional war have one thing in common, namely that the country which possesses the critical weapons such as atomic bombs will have "first strike" and "second strike retaliation" capabilities....As soon as its computer networks come under attack and are destroyed, the country will slip into a state of paralysis and the lives of its people will ground to a halt. Therefore, China should focus on measures to counter computer viruses, nuclear electromagnetic pulse...and quickly achieve breakthroughs in those technologies in order to equip China without delay with equivalent deterrence that will enable it to stand up to the military powers in the information age and neutralize and check the deterrence of Western powers, including the United States.

North Korea appears to be attempting to implement the information warfare doctrine described above by developing a long range missile capable of making a catastrophic nuclear EMP attack on the United States. In December 2012, North Korea demonstrated the capability to launch a satellite on a polar orbit circling the Earth at an altitude of 500 kilometers. An altitude of 500 kilometers would be ideal for making an EMP attack that places the field over the entire contiguous 48 United States, using an inaccurate satellite warhead for delivery, likely to miss its horizontal aimpoint over the geographic center of the United States by tens of kilometers. North Korea's satellite did not pass over the United States—but a slight adjustment in its trajectory would have flown it over or near the U.S. bull's eye for a high-altitude EMP burst.

Miroslav Gyurosi in *The Soviet Fractional Orbital Bombardment System* describes Moscow's development of the FOBS:

(Continued on Page 10)

(Continued from Page 9)

The Fractional Orbital Bombardment System (FOBS) as it was known in the West, was a Soviet innovation intended to exploit the limitations of U.S. BMEW radar coverage. The idea behind FOBS was that a large thermonuclear warhead would be inserted into a steeply inclined low altitude polar orbit, such that it would approach CONUS from any direction, but primarily from the southern hemisphere, and following a programmed braking maneuver, re-enter from a direction which was not covered by BMEW radars.

"The first warning the U.S. would have of such a strike in progress would be the EMP...," writes Gyurosi.

The trajectory of North Korea's satellite launch of December 12, 2012 looked very much like a Fractional Orbital Bombardment System for EMP attack. The missile launched southward, away from the United States, sent the satellite over the south polar region, approaching the United States from the south, at the optimum altitude for EMP attack—although the test trajectory deliberately avoided flying over the United States.

North Korea appears to have borrowed from Russia more than the FOBS. In 2004, a delegation of Russian generals met with the Congressional EMP Commission to warn that design information for a Super-EMP nuclear warhead had leaked from Russia to North Korea, and that North Korea might be able to develop such a weapon "in a few years." A few years later, in 2006, North Korea conducted its first nuclear test, of a device having a very low yield, about 3 kilotons. All three North Korean nuclear tests have had similarly low yields. A Super-EMP warhead would have a low-yield, like the North Korean device, because it is not designed to create a big explosion, but to produce gamma rays, that generate the EMP effect.

According to several press reports, South Korean military intelligence concluded independently of the EMP Commission that Russian scientists are in North Korea helping develop a Super-EMP nuclear warhead. In 2012, a military commentator for the People's Republic of China stated that North Korea has Super-EMP nuclear warheads.

One design of a Super-EMP warhead would be a modified neutron bomb, more accurately an Enhanced Radiation Warhead (ERW) because it produces not only large amounts of neutrons but large amounts of gamma rays that cause the EMP effect. One U.S. ERW warhead (the W-82) deployed in NATO during the Cold War weighed less than 50 kilograms. North Korea's so-called Space Launch Vehicle, which orbited a satellite weighing 100 kilograms, could deliver such a warhead against the U.S. mainland—or against any nation on Earth.

Iran may already have a FOBS capability, as it has successfully launched several satellites on polar orbits, assisted by North Korean missile technology and North Korean technicians. Iranian scientists were present at all three North Korean nuclear tests, according to press reports.

What is to be done about the cyber and EMP threats?

Technically, it is important to understand that surge arrestors and other hardware designed to protect against EMP can also protect against the worst-case cyber scenarios that, for example, envision computer viruses collapsing the national power grid. For example, surge arrestors that protect Extra High Voltage transformers from EMP can also protect transformers from damaging electrical surges caused by a computer virus that manipulates the grid Supervisory Control And Data Acquisition Systems (SCADAS).

Administratively, a coherent and effective answer will not likely arise from uncoordinated decisions made independently by the thousands of individual industries at risk. Because cyber preparedness should encompass EMP preparedness—and since EMP is an existential threat—it is imperative that Government play a supervisory and coordinating role to achieve protection against these threats swiftly. ❖

Critical Infrastructure Protection and Transformer Stations: An Overlooked Cog in our Energy Infrastructure

by Craig Thompson, Carleton University, Ottawa, Canada*

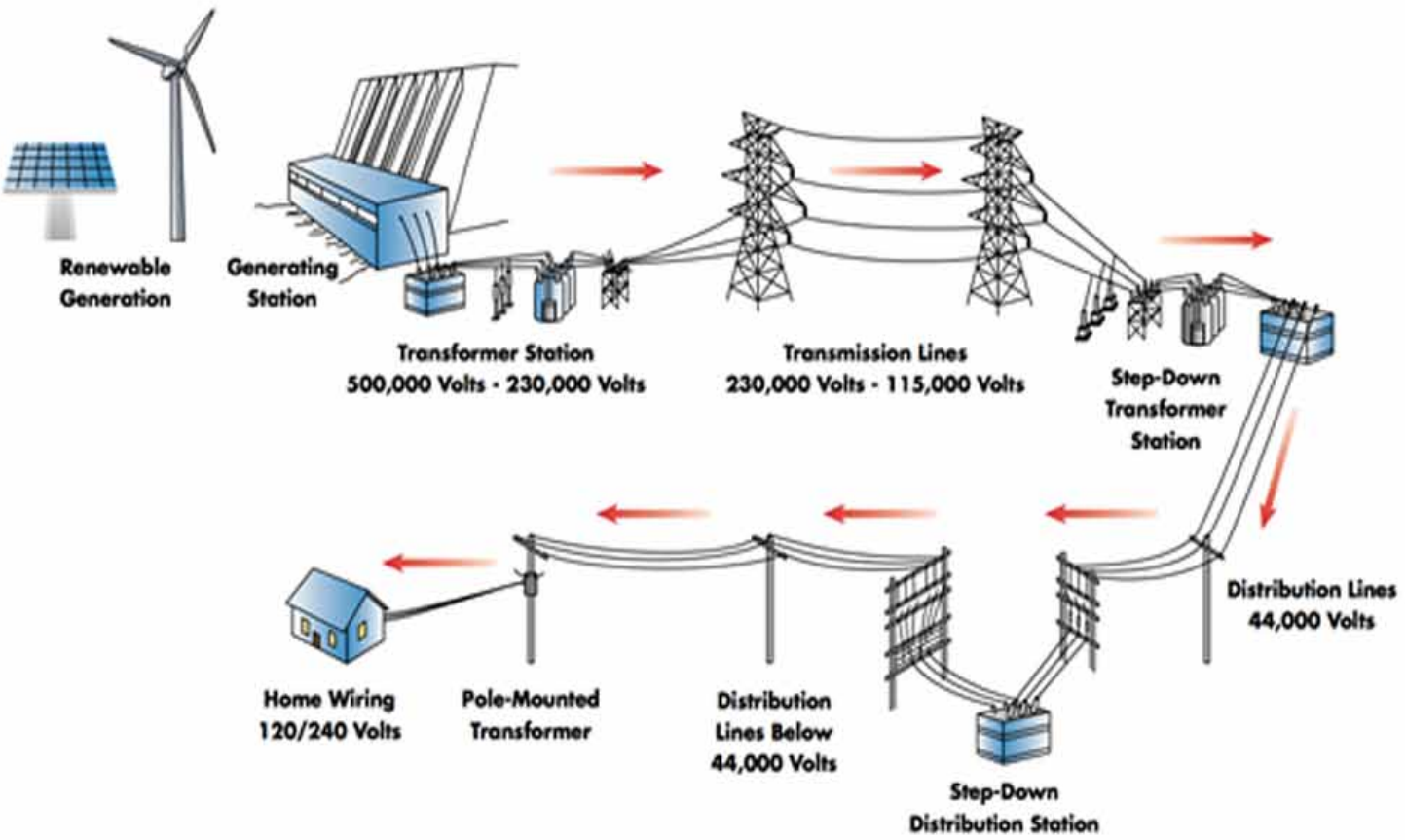
Transformer stations in North America pose a vulnerable and often overlooked target in the energy critical infrastructure supply system. Using the Cherrywood Transformer Station in Ontario, Canada as a primary example, the requirements and some methods available to cripple the station will be analyzed, as well as the effects that a similar station failure would have on the associated power grid.

Transformer Stations and North America's Energy Critical Infrastructure

Illustrated in Figure 1 below, transformer stations are only a part of the entirety of the electricity supply chain. Initiated at the generating station, energy is then transferred via transmission lines into a transformer station. From here, the energy is sent via transmission lines to the rest of the energy supply chain, and eventually, to each citizen's home.

(Continued on Page 12)

Figure 1: The Electricity Supply Chain[1]



[1] Hydro One. *Welcome to our Public Information Centre*. Clarington: Hydro One, 2012.

(Continued from Page 11)

Figure 2: Cherrywood Power Supply[2]

Depicted in Figure 2 above, is the power supply running to the Cherrywood Transformer Station. Nearly the entirety of all power carried from the Pickering, Ontario, and Darlington, Ontario Nuclear Generating Stations, as well as that being sent from the rest of Eastern Canada, flows through Cherrywood station. After power flows through the Cherrywood Transformer Station, it is sent to step-down stations such as those in Whitby, Oshawa, and Pickering.[3]

As seen above, Cherrywood station not only is an inherent critical node in North America's energy supply system, but it is so critical that since there are no other redundant transformer systems on this particular section of the power grid, it approaches a single point of failure (SPOF). Cherrywood station supplies nearly 70% of the entire Toronto and Vaughn electrical power load, and nearly 90% of the power load to Markham, Richmond Hill, and Durham region.[4] Combined, this represents over 6.3 million citizens depending nearly entirely on the Cherrywood Transformer Station.[5] This number does not include those people outside the surrounding area of the Greater Toronto Area (GTA) who depend on power from Cherrywood station, and who would also be affected by a failure.

Cherrywood Station Vulnerabilities

Seen in Figure 3, the Cherrywood facility is protected by an alarmed fence, ringed with barbed and razor wire. Oddly, there appears to be no on-site security staff or cameras throughout the exterior or visible interior of the facility. The only notable security system is the exterior fence, and while signs state that it is alarmed, it is unknown if there is any actual response capability by police, or how long that response would take. Regardless of how secure the fence is, or even if it is alarmed, the two secondary gates located within the facility are only secured by a single padlock, and have no alarm cable so as to alert any first responders if the gate is opened. This seems to indicate that an individual armed with only

(Continued on Page 13)

[2] Ontario Power Authority. *Description of Need and Rationale for "Oshawa Area" TS by 2015*. Toronto: Ontario Power Authority, 2012.
[3] Ibid.
[4] Hydro One. *Hydro One's Transmission System Adequacy in Ontario*. Toronto: Hydro One, 2005.
[5] Office of Economic Policy. *Population Growth in Ontario's CMAs and the GTA*. Ottawa: Ontario Ministry of Finance, 2009.

(Continued from Page 12)

a pair of bolt-cutters could gain access to the facility without raising any alarms.

Figure 3: Cherrywood Main Gate

Vulnerabilities of Transformer Unit Based Attacks

Due to the high voltage of electricity at transformer stations, fire is one of the most dangerous threats to the continuity of the facility.[6] Since electricity is both an ignition source and fuel for fire, and since the elements are already in place to destabilize the facilities' energy output, all one would need to do is overcome the insulation and fire retardant measures currently installed on transformer units to ignite the facility.[7] There are many reports of transformer station fires in North America, some of which cause intermittent power failures to the region, while others do not. In the region directly related to Cherrywood station there has been one small fire event in 2005 at Cherrywood itself, and several large fires at the Richview transformer station in Etobicoke. Should these fires however be set intentionally at multiple locations within the Cherrywood facility, one could cripple the entire location instead of only a single transformer.

Figure 4: One of the Cherrywood Secondary Gates

Consequences

A successful strike against Cherrywood that causes the failure of the transformer station would likely create at minimum an immediate loss of power to the entire GTA. The length of the power outage in most parts of Toronto, York, and Durham

(Continued on Page 14)

[6] Kjolle, G.H., and I.B. Utne. *Critical Infrastructures and Risk Analysis of Electricity Supply*. SINTEF Energy Research, Trondheim: Sintef Energy Research, 2010.
[7] Ibid.

(Continued from Page 13)

Region would be expected to be commensurate with the length of time that it takes to repair Cherrywood station. This is because there are no other networks available to transfer the mass of power needed to maintain the electrical grid in the area. Fatalities resulting from the loss of power are difficult to calculate, since many result from situational factors such as the local temperature during the outage, length and area affected by the outage, as well as competence of local emergency services.

A successful attack on Cherrywood or other transformer stations may even trigger the 'Cascade Effect'.[8] The 'Cascade Effect' suggests that if a node is removed from the power grid, then the load placed on that node is redistributed to the neighboring nodes on the system connected to the failed node.[9] Therefore, if the load of the failed node (or in this case, nodes) is too high for the neighboring nodes, then these nodes too will fail and further exacerbate the disaster. Eventually, this 'Cascade Effect' ripples throughout the entire power grid, resulting in widespread loss of power over a massive region.

The 'Cascade Effect' was the cause of the 2003 blackout across the power grid of the Canada/ United States Eastern Seaboard. The blackout spawned from an accidental event resulting in a massive power outage throughout most of Ontario, New York State, Ohio, Pennsylvania, New Jersey, Vermont, Michigan, Connecticut, and Massachusetts, affecting roughly 50 million people.[10] The blackout is reported to have touched all 10 Canadian critical infrastructure sectors and most if not all 16 American critical infrastructure sectors, resulting in widespread panic and an increase in crime throughout the affected regions.[11]

Recommendations

The low protection and susceptibility to fire and explosives make North America's energy Transformer stations a weakness in the United States and Canadian energy infrastructure which can be monopolized by violent radicals with either single person strikes or coordinated attacks, effectively crippling the local and extended power grid. The protection of transformer stations, and in particular Cherrywood station, needs to be increased to help ensure the continuity of energy to the local population. Firstly, and most importantly, there needs to be redundancy within the energy transmission network. Hydro One is currently proposing a Clarington Transformer station project, which addresses the upcoming need for an increased energy supply to the GTA.[12] This new facility offers a secondary path for transmission of the electrical load should the Cherrywood station be compromised (See Figure 5, Page 15).

The benefit of this station for the region cannot be understated, as not only does it help meet the advancing energy supply requirements for the region, but it also removes Cherrywood station as a SPOF and implements redundancy within the energy transmission system. While the region would still feel the effect of losing the station, the risk of the 'Cascade Effect' would be largely mitigated, and limited energy supply could be maintained to the affected population.

Secondly, increased physical protection and surveillance of the transformer station facilities should be considered due to the vulnerabilities of leaving such a critical target with little supervision. This could include electronically alarmed perimeter fences and gates, as well as motion sensor and camera systems.

Finally, a stock of spare transformers (new transformers take up to two years to build and obtain) should be maintained to quickly replace failed transformer units and return power to the affected area. These steps, if implemented appropriately,

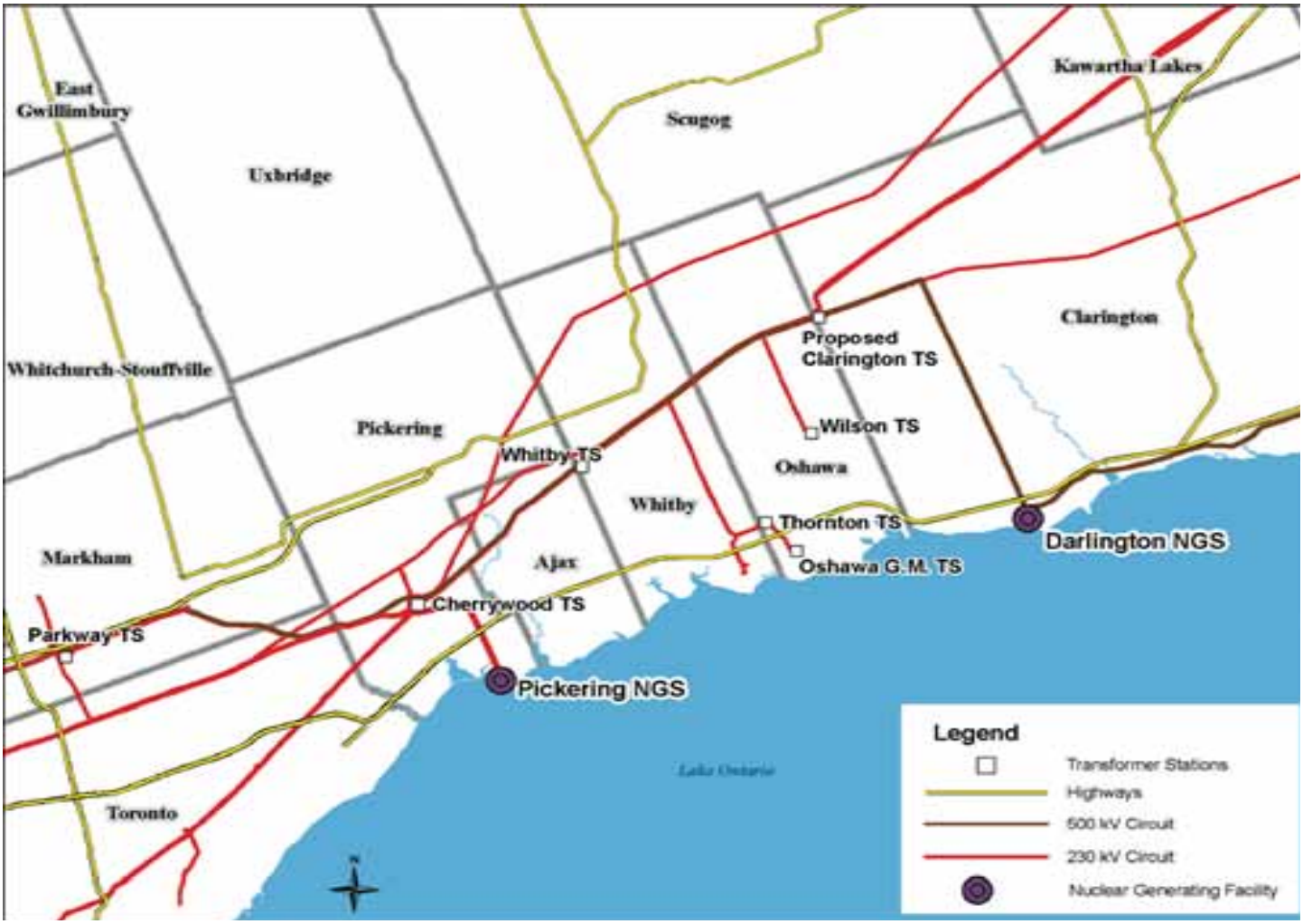
(Continued on Page 15)

---

[8] Wang, Jian-Wei. "Cascade-Based Attack Vulnerability on the US Power Grid." *Institute of System Engineering* 47, no. 10 (December 2009): 1332-1336.
[9] Ibid.
[10] Public Safety Canada. *Ontario-U.S. Power Outage-Impacts on Critical Infrastructure*. Ottawa: Public Safety Canada, 2006.
[11] Ibid.
[12] Hydro One. *Welcome to our Public Information Centre*. Clarington: Hydro One, 2012.

(Continued from Page 14)

Figure 5: Energy Distribution throughout Southern Ontario after the Inclusion of the Clarington Transformer station[13]



will help to mitigate this vast risk to North America's energy supply. ❖

** Craig Thompson is a graduate student with the Masters of Infrastructure Protection and International Security Program at Carleton University in Ottawa. He previously worked as a Reconnaissance Soldier with the Canadian Forces and currently works as a Research Affiliate with Public Safety Canada, and as a Security Advisor with Transport Canada.*

---

[13] Ibid.

Protecting U.S. Pipelines from Cyber-Attacks

by Brigham A. McCown, Principal and Managing Director, United Transportation Advisors*
and Stephanie C. Hallgren, J.D. Candidate, Texas A&M University Law School

Introduction

The Internet has undoubtedly become the most useful communications and knowledge referral network ever conceived. Its massive expansion in the 1990s consequently resulted in the emergence of corresponding risk. Public and private sector entities have spent, and will continue to spend, significant resources aimed at controlling access to the very data the Internet was designed to share as economic crimes and acts of espionage and sabotage have proliferated.

The Internet is not just a ready repository of information; it is a conduit, through which telecommunications, corporate data, and government business is conducted. This business naturally includes information, but the Internet is also used to send and receive signals needed to run systems, facilities, factories, and even critical national infrastructure.

Background

For the past two decades, the regularity and severity of cyber-attacks have exponentially increased, rendering many systems vulnerable.[1]

The U.S. Government has been a frequent target for cyber-attacks due to its highly classified information. In 2008 alone, the Pentagon reported approximately 360 million endeavors to breach its security, including an ostensibly successful invasion and duplication of the $300 billion Joint Strike Fighter project.[2] These premeditated events are the direct product of foreign powers.

One particular form of cyber-attack has evolved into an instrument of war, the denial-of-service (DoS) attack.[3] This form of attack paralyzes websites, financial networks, and other processing systems by deluging them with data from external processors, rendering the system susceptible to harm.[4] North Korea, Iran, Russia, and most notably, China have boasted of the capabilities of their "cyber-warriors,"[5] counting them as an arsenal of their militaries.[6] Evidence indicates the United States and/or Israel are certainly both proponents of cyber tactics, with many attributing one or both of these nations to the successful deployment of the Stuxnet worm against an Iranian nuclear facility.[7]

Why Pipelines are National Critical Infrastructures

Critical infrastructure protection takes many forms, transcending industries throughout the United States. The U.S. pipeline infrastructure system is the primary network for energy transportation, and thus of great significance to protect.[8]

Pipelines are generally classified into two distinct types, liquid and gas based upon the state of the material being transported. Liquid lines transport crude oil, refined products such as gasoline and diesel fuels, jet fuel, kerosene, and many other products in liquid form. As the name suggests, gas pipelines transport fuels in a gaseous state, most notably, natural gas. Based upon this distinction and beginning upstream, pipelines are then broken down into production, gathering, transmission, and distribution pipelines.

(Continued on Page 17)

[1] Randy James, "A Brief History of Cybercrime," *Time* (June 01, 2009), http://ti.me/17uYyLF.
[2] Ibid.
[3] Ibid.
[4] Ibid.
[5] Julian Ryall, "Cyber-Attacks & Warfare," *Intellectual Takeout* (Sep. 20, 2011), http://bit.ly/14Gg0X7.
[6] Ibid.
[7] Ibid.
[8] Transportation Systems Sector, Homeland Security, http://1.usa.gov/13LKZ5k.

(Continued from Page 16)

The energy transportation network in the United States consists of more than 2.6 million miles of pipelines, enough to circle the earth one hundred times.[9] This vast energy highway provides the distribution of 65% of all energy consumed by the country each year.[10] Therefore it is easy to see that pipelines have transported the lion's share of energy products necessary to feed electric generation facilities, power factories and businesses, heat homes, and fuel the country's vast transportation network.

No longer are these sophisticated energy highways monitored and run by workers in pickup trucks, hand turning valves at urban and remote stations. Today's pipelines are dependent upon technology. Sensors and automated gates, switches, and valves are remotely monitored and controlled from specialized control rooms maybe hundreds, or even thousands of miles away. From these control rooms, specially trained individuals monitor every aspect of a pipeline in much the same way a large nuclear power plant is run. Supervisory Control and Data Acquisition (SCADA) controls enable the controller to electronically collect data and monitor all activity, as well as distribute commands to the pipeline facility from a third party location.[11]

Security

According to reports, in February 2011 McAfee, a computer security firm, exposed a cyber-attack labeled "Night Dragon" which attempted to obtain sensitive data and financial documents from oil and gas companies.[12] From December 2011 through June 2012, an anonymous group coordinated a cyber-attack on the control system of U.S. pipelines prompting the Department of Homeland Security (DHS) to issue alerts.[13] It is believed cybersecurity researchers traced the digital signatures from the attacks to an espionage group potentially allied with the Chinese military.[14] According to DHS, the hackers used a technique called "spear-phishing" by sending targeted e-mails to individuals and camouflaging the sender as an acquaintance. When opened, attachments or leaks in the e-mails release malware into the victim's computer.[15]

In 2013, cyber-attacks that may have been backed by the Iranian government launched a series of surveillance missions against the control systems of some U.S. energy companies.[16] Current and former

(Continued on Page 18)

---

[9] Annual Report Mileage for Gas Transmission and Gathering, Gas Distribution and Hazardous Liquid, PHMSA (Apr. 30, 2013) http://1.usa.gov/11KlpKy.
[10] General Pipeline, PHMSA, http://1.usa.gov/13XAlJ3.
[11] Operations & Maintenance Enforcement Guidance Part 195 Subpart F, PHMSA, http://1.usa.gov/1150HGu.
[12] Jason Ryan, "DHS: Hackers Mounting Organized Cyber Attack on U.S. Gas Pipelines," *ABC News* (May 8, 2012) http://abcn.ws/14Ggw7F.
[13] Ibid.
[14] Joao Peixe, "US Gas Pipelines at Risk after Chinese Military Cyber Attack," *OilPrice* (Feb. 28, 2013) www.oilprice.com/Latest-Energy-News/World-News.
[15] Jason Ryan, *supra*, note 12.
[16] Fahmida Y. Rashid, "Iranian Cyber-Attackers Target US Energy Companies," *SecurityWatch* (May 25, 2013), http://bit.ly/14lZbE9.
*Image courtesy of Vichaya Kiatying-Angsulee/FreeDigitalPhotos.net.

(Continued from Page 17)

officials confirm the intruders successfully collected information on the inner workings of the system.[17]

The escalating occurrence of cyber-attacks highlights the vulnerability of the United States. Tom Cross, director of security research at Lancope, reiterated the vulnerability of pipelines due to their strong reliance upon the Internet. Many systems are further compromised with long repair times after a security breach.

Similar to recent events in Iran, pipeline infrastructure is vulnerable to intrusion. Although these systems are generally housed in a dedicated line, it is still possible to gain entry. If such were to occur, a pipeline could be shutdown, or worse, run in such a way to intentionally cause damage. That said, counter methods have been deployed to eliminate and minimize any such attempts. Nonetheless, the risks are real.

Protection & Mitigation

Congress is currently debating the safety of industrial control systems from cyber-attacks. The federal government is seeking authority to require sectors of the transportation system to increase security measures to mitigate risks.[18] Additionally, President Obama signed a directive in mid-October effectively enabling the military to act more aggressively to thwart cyber-attacks.[19] According to several U.S. officials who have seen the classified document, the directive established broad, yet strict standards guiding the operations of federal agencies during cyber-threats.[20]

On June 7, 2013 President Obama traveled to China to meet with President Xi Jinping to discuss the emergence of cyber-attacks on American industrial secrets.[21] Obama's council has suggested if milder measures continue to fail, companies may be granted the right to retaliate with counterstrikes of their own.[22] At the same time, military leaders have equated these types of events as tantamount to a military attack on the United States.

Moving Forward

Today, computer scientists are devising guardians called 'symbiotes' to help protect critical infrastructure by allowing the processor to run regardless of the underlying operating systems.[23] As stated by Mr. Cross, "It is extremely important that [these systems are monitored] with systems that can identify anomalous activity that might be associated with an attack because of the relatively homogeneous nature of network activity."[24]

While many reactionary steps have been taken post cyber-attack, they are notably lacking in proactive efforts. The resiliency of U.S. control systems should be adapted to combat cyber-attacks with greater absorption capacities to mitigate failures with alternatives to recover the system.

Conclusion

The occurrence of cyber attacks will only increase over time, as our society becomes more digitally reliant. It is vitally important we protect our infrastructure programs from cyber-attacks, by supporting new developments in technology to minimize the risk from such attacks. ❖

** United Transportation Advisors (UTA) provides a single point of access for entities seeking executive guidance, professional and technical support, and consulting services covering significant transportation and energy issues.*

---

[17] Fahmida Y. Rashid, "Iranian Cyber-Attackers Target US Energy Companies," *SecurityWatch* (May 25, 2013), http://bit.ly/14lZbE9.
[18] Mark Clayton, "Alters say major cyber attack aimed at gas pipeline industry," *NBC News* (May 6, 2012), http://nbcnews.to/11xDShP.
[19] Ellen Nakashima, "Obama signs secret directive to help thwart cyber attacks," *Washington Post*, http://bit.ly/14lZAGH .
[20] Ibid.
[21] David E. Sanger, "As Chinese Leader's Visit Nears, U.S. Is Urged to Allow Counterattacks on Hackers," *New York Times* (May 21, 2013), http://nyti.ms/11mrNIj.
[22] Ibid.
[23] Industrial Control Systems Cyber Emergency Response Team, *ICS-Cert Monitor*, http://1.usa.gov/11plFQn.
[24] Iranian Hackers Launching Cyber-Attacks on U.S. Energy Firms: Report, *eWeek* (May 27, 2013), www.eweek.com/security.

Data-Driven Energy Management Delivers Enterprise Savings and Business Continuity

by Mark Straton, Senior Vice President of Marketing, GridPoint*

The perpetual growth of energy costs over the last few decades has undoubtedly spurred the adoption of intelligent energy solutions, energy efficiency, and sustainability for enterprises across the country. With commercial and industrial energy use accounting for 53% of all non-transportation energy spending in the United States, energy management systems (EMS) and their associated cost savings and sustainability opportunities are increasingly vital to enterprise cost control and competitive strategies. The emergence of relatively inexpensive computing, data storage, and cloud deployment options have already transformed many industries, and are now poised to do the same for enterprise energy management.

We have seen this in our automobiles with the use of sophisticated instrumentation to constantly monitor and adjust key systems to optimize fuel economy, maximize performance, and provide critical information to the driver. The same approaches can now be applied to create smart buildings which will now be able to utilize data-driven energy management solutions on a cost-effective basis—providing predictable and unprecedented energy, operational, and capital expenditure savings.

Driving Factors for Enterprise Energy Management Adoption

There are many forces shaping today's energy market. The first two are economic and political drivers. Analysts estimate that there will be a 1.9% real annual price increase (before inflation), and 46% real increase over the next 20 years. These are staggering numbers that encourage many enterprises to take another look at their energy and sustainability practices, so that they may minimize energy consumption and carbon emissions, as well as meet increasing government regulations.

The third main driver is technology. With the emergence of the Software as a Service (SaaS) model, enterprises are able to implement sophisticated systems across large geographies and execute daily business functions with minimal expense and complexity. Next, the proliferation of smart, low cost, and wireless energy endpoints enables real-time data collection and control to be broadly deployed across enterprises. Finally, enterprises can take the real-time data from these smart endpoints and push their efficiency measures even further with advanced data aggregation and deep analytics to drive optimization in real-time and over the long-term.

Addressing Today's Energy Efficiency and Sustainability Opportunities

Energy, facility, and sustainability managers are confronted with a myriad of energy efficiency and sustainability tools that are designed to reduce consumption and costs, but today's tools are not integrated, and lack real-time data and the artificial intelligence needed to minimize energy consumption on an ongoing basis. To effectively utilize and maximize the breadth of energy solutions available, the market needs a single integrated software platform and application suite that supports all efficiency and sustainability measures, from energy consumption to renewable generation management, including solar energy, fuel cells, wind, and more.

To do so, the platform must provide a single, integrated suite of hardware, software, and services that features real-time and historical data in an easy-to-use tool set that minimizes deployment and support resources, or more easily stated, a data-driven EMS. With this capability, enterprises are able to aggregate and simplify consumption, production, and demand management data to centrally and effectively manage a large portfolio

(Continued on Page 20)

(Continued from Page 19)

of sites. This level of data allows enterprises to maximize energy savings and efficiency through actionable alarms and intelligence, as well as plan for future projects armed with detailed financial analysis, project performance comparisons, and predictive intelligence.

Data-Driven Energy Management for Immediate and Lasting Savings

For most enterprises, the foundation of success to date has been a building control program consisting of hardware and perhaps limited software to allow for basic setpoint and control monitoring. These systems follow simple schedules to turn heating/air conditioning and lighting on/off with predetermined schedules to save cost. However, such traditional approaches leave competitive opportunities and money on the table. For example, they do not measure component level energy consumption or take into account critical environmental factors like human comfort, multiple zone temperatures, humidity, CO2, occupancy, and outside temperature.

The savings an enterprise can achieve all comes down to an intelligent, automated control solution that collects real-time usage data that can be combined with information from outside sources like rating, demand response programs, and historical data for predictive analytics. A data-driven EMS is designed to be a self-learning feedback system where each new piece of information constantly fuels a circle of feedback resulting in the certainty of planned results, continual refinement and optimization, and further understanding of effective best practices for facilities.

By monitoring the real-time energy consumption of components such as lighting, HVAC (heating, ventilation and air conditioning), and refrigeration, energy managers begin to understand how their facilities are using energy and are thus able to make data-based decisions resulting in optimal energy consumption, utility bill validation, and do so in real-time versus after the fact management by utility bill. Built on the data store from an increasing number of existing and new sensors, submeters, meters, and controls, this advanced building instrumentation allows intelligent algorithms

(Continued on Page 21)

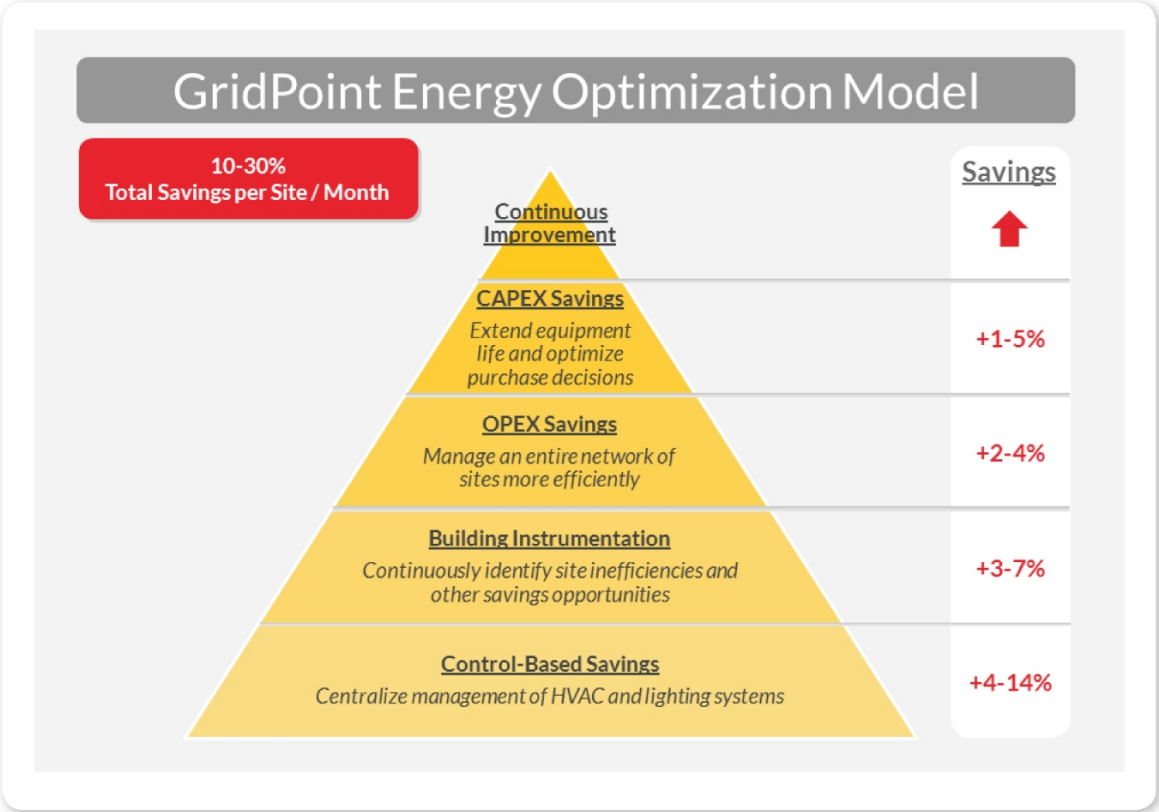


Figure 1. The GridPoint Energy Optimization Model
GridPoint's comprehensive energy management system delivers up to 30% total saving per site / month

(Continued from Page 20)

to constantly self-tune and improve results, saving enterprises as much as 30%. The savings potential drastically increases when energy efficiency and sustainability solutions are combined. In addition, because these capabilities are tied to an analytics software platform, actual historical energy consumption and production usage patterns can be used to compare current performance, as well as to forecast future needs (Figure 1).

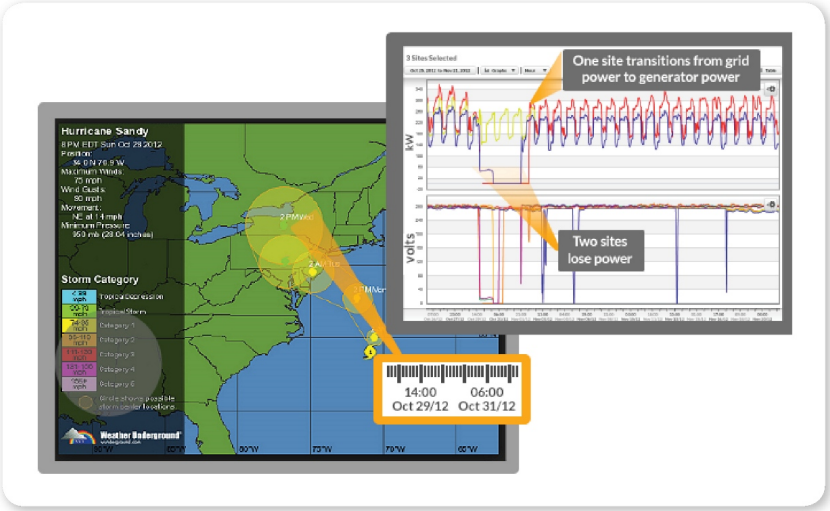


Figure 2. GridPoint Energy Manager software details site operability as Hurricane Sandy passes through the region

Maximize Learning for More Effective Facility Operation and Design

Most buildings are engineered for maximum load or a worst-case scenario. For some systems, this is totally appropriate, but for others, it is expensive and only seemingly necessary due to insufficient insight. A data-driven EMS provides the benefit of analyzing results over time; comparing reliability and cost-effectiveness of one type of equipment versus another (e.g., different HVAC units used in similar environments) and identifying unnecessary overcapacity in design (e.g., four HVAC units designed in, where three would have been sufficient).

Bringing such data to the design and planning phase of facility management can have a tremendous impact on the use of capital. While not normally thought to be the purview of EMS systems, a data-driven EMS can offer tremendous insight into capital decisions and save money over time.

In addition, when data is collected on an enterprise-wide basis, results and practices between similar facilities can be compared to provide insight into new best practices, which saves money without compromising customer and employee comfort or environmental needs. This kind of forensic analysis inevitably reveals new sources of previously hidden and fully actionable savings opportunities.

Real-Time Data Plays a Critical Role in Disaster Recovery

The ability to capture and store real-time data not only allows enterprises to achieve energy management and sustainability goals, but can also play a vital role in maintaining business continuity in the event of a natural disaster. By utilizing a data-driven energy management and cloud-based analytics software suite, enterprises are able to quickly assess site power and equipment performance through a variety of sophisticated reports and dashboards. The remote monitoring, management, and granular visibility of site operations, including equipment and environmental conditions, enables an enterprise's disaster recovery and facility management teams to focus their attention on re-opening stores and optimizing on-the-ground operations (Figure 2).

In 2012, the East Coast was devastated by Hurricane Sandy, one of the most catastrophic storms in U.S. history, causing more than $50 billion in damage. With communities under extreme distress, one major retailer used its integrated energy management suite to remotely view site and equipment performance data in near real-time, prioritize needs based on power supply, potential inventory loss, and equipment failure, and drive faster site and equipment recovery time.

With the valuable real-time data provided by the data-driven energy management systems in hand, the retailer was able to proactively plan for the anticipated storm, and then remotely monitor and manage their recovery after the storm had passed. This approach ensured perishable

(Continued on Page 22)

(Continued from Page 21)

inventories were salvaged and stores returned to full operating mode as quickly as possible to support local recovery efforts. Perhaps most importantly, the retailer could assist the communities that were most severely impacted by the storm and access the emergency supplies, medicine, and food items that are so vital in a disaster situation.

Maximize Energy Savings, Operational Efficiencies, and Sustainability Results with Intelligent Energy Management

The opportunity now exists for enterprises to achieve unprecedented results in energy savings, operational efficiencies, and business continuity, as well as environmental and sustainability goals with a data-driven approach to energy management based on advanced data collection and analysis tools.

These savings are made available through a combination of collection and storage of highly granular energy data, specialized submetering and control hardware designed to economically gather endpoint data, a software-based management, and analytics system delivered via the cloud. ❖

**GridPoint is an established leader in smart energy solutions, providing Fortune 1000 enterprises, government agencies, and utilities with the tools to implement and maintain sustainable energy management practices that improve operational efficiency and maximize energy savings. Founded in 2003, GridPoint is headquartered in Arlington, Virginia, with offices in Austin, Texas, Roanoke, Virginia, and Seattle, Washington. GridPoint has deployed more than 11,000 sites across the U.S., Canada, and U.K., which include 4 of the top 10 U.S. retailers and 3 of the top 10 U.S. casual dining restaurants in addition to government entities and leading North American utilities.*

GMU CIP/HS Research Partnerships in Energy Research and Education

by Mark D. Troutman, Ph.D., Associate Director, CIP/HS

The Center for Infrastructure Protection and Homeland Security (CIP/HS) seeks to investigate solutions in policy, law, and technology to increase the security and resilience of the Nation's critical infrastructure and that of our international partners. In our continuing inquiry and education programs, CIP/HS leverages research, education, and outreach efforts through partnerships with business, academic, and government organizations. We have created two new partnerships that extend and deepen our research in the Energy Sector and its related interdependencies with other critical infrastructure sectors. These partnerships will also extend our engagement in the international space. This short overview will outline these partnerships and fit them into overall CIP/HS efforts.

George Mason University (GMU) is a founding partner of the Virginia Nuclear Education Consortium (VNEC), designed to investigate research and applications in energy and related infrastructure sectors. VNEC focuses on next generation nuclear power and is presented in some depth elsewhere in this issue. The initiative seeks energy system resilience from supply through generation, to delivery and disposal. Virginia's position as a net power importer and its unique combination of industry, research/education, and technology assets in close proximity offers a unique combination to spur development.

Technological advances that lower cost, increase reliability and safety, and solve problems of waste disposal in an environmentally sustainable manner promise significant advances but are in themselves insufficient. The broad power generation industry and nuclear industry in particular require a professional workforce that understands the special requirements of this critical infrastructure sector in all its dimensions. Further, this workforce must understand the linkages and dependencies that exist with other infrastructure sectors. VNEC is a great vehicle to commission multidisciplinary professionals who understand the specific demands of their sector as well as the interdependencies of other infrastructure challenges.

In September 2012, GMU finalized a partnership with the Energy Security Research Center (ESRC) of Ajou University located in Suwon, South Korea. Like GMU, Ajou is a young university, founded in 1973. ESRC is likewise a recent development, created to address South Korea's challenges in the area of Energy Sector security and resilience. Also in common with GMU, Ajou shares proximity with its nation's capital, and access to major international transportation sources across all nodes.

This new partnership offers the opportunity for important bilateral and international impact. Korea is the world's 12th largest economy and among the largest and most diversified economies of Asia. Trade comprises over two thirds of South Korea's economy and is a major source of its economic growth, making reliable sources of energy of primary importance. Korea imports virtually all of its fossil fuel energy requirements, and secure energy sources and resilient transportation that connect energy sources to generation and distribution are major concerns.[1]

South Korea and the United States share common security interests in northeast Asia and on the international stage. Bound by a mutual defense treaty since 1953, both countries clarify and extend their security dialogue through twice yearly ministerial level meetings. In 2011, the countries broadened their economic partnership through ratification of a Free Trade Agreement. Academic partnerships and research ventures have

(Continued on Page 24)

[1] World Nuclear Association, Country Profiles: South Korea, available at http://www.world-nuclear.org/info/Country-Profiles/Countries-O-S/South-Korea/#.UbX2ttjm5qA.

(Continued from Page 23)

flourished through the same period. South Korea has a strong commitment to education and research as a source of growth. The GMU—Ajou partnership and CIP/HS—ESRC tie are natural outgrowths of this trend and offer bright opportunities.

This international partnership offers many opportunities to explore the broad topic of energy security, resilience, and sector interdependence. Both the United States and South Korea provide for their national energy needs through a varied mix of fossil fuel, renewable, and nuclear based sources. Both nations face challenges of security, transportation, and sector interdependency issues from source through generation and distribution of energy. Both nations face unique climate and geography challenges. South Korea faces the added challenge of providing energy sector security and resilience with a belligerent nation adjacent to its north. The proximity of our two universities to government decision makers, robust research, and international partners offers an opportunity to pool solutions and increase our respective Energy Sector security and resilience.

Cybersecurity of source, generation, and distribution systems is a further Energy Sector concern. CIP/HS partnerships with the Volgenau School have produced insights into cybersecurity and its applications to infrastructure sectors. South Korea is an international leader in the electronics and information systems fields, and Ajou University features a robust computer science research and education capability. Cybersecurity and its applications to industrial control systems, transportation networks, power generation systems, and distribution networks represent a fertile area for research to produce practical solutions that enhance energy sector security and resilience. Cybersecurity education, particularly the professional education of system professionals who lead the development and implementation of cross sector solutions, is a particular need and natural outgrowth of the strengths found in our two universities and their research centers.

Both the United States and South Korea produce a significant share of their generated power from nuclear sources.[2] Between 20 – 30% of each country's overall generated power derives from nuclear sources. The countries share a long history of collaboration in the development of safe nuclear power and a commitment to non-proliferation of nuclear materials embodied within the 1-2-3 Accords. South Korea has made a major commitment to the development of nuclear power as a means of reducing its near dependence on fossil fuel imports. Therefore, development of a professional workforce to meet the needs of the nuclear Energy Sector is a high priority. In addition, South Korea has identified nuclear power as a viable export industry. Within the past few years, South Korea secured its first major export opportunity with a contract for four reactors in the United Arab Emirates. Thus, research into education and systems necessary to enable safe nuclear power export in accord with non-proliferation norms is a fertile area for inquiry.

GMU and South Korea have an established history in the area of nuclear power professional education. GMU and the Korea Electric Power Company (KEPCO) established the Korea International Nuclear Graduate School (KINGS), which took in its first class of international students in 2012. GMU and KINGS share research and education responsibilities for this one of a kind graduate school. In combination with the VNEC initiative, CIP/HS and ESRC have the opportunity to leverage existing and future opportunities in the areas of next generation nuclear power, professional education, and export opportunities.

Energy production and distribution is a highly regulated industry for a variety of reasons. The industry exhibits characteristics of a natural monopoly which presents a base case for regulation to protect consumers. Environmental and safety issues abound in this sector and require standards to prevent unwanted external effects. Finally, the dependence of other sectors and essential functions on the provision for reliable electric power renders the energy generation and distribution system among the

(Continued on Page 25)

[2] World Nuclear Association, Country Profiles, available at http://www.world-nuclear.org/info/Country-Profiles/.

(Continued from Page 24)

most highly regulated of sectors to insure its resilience. CIP/HS' partnerships with GMU's School of Management and School of Public Policy provide a unique opportunity to develop concepts of smart regulation that provide essential safeguards with a minimum impact on efficiency. ESRC provides a similar opportunity to test these concepts in a challenging environment and export context. The area of regulatory science represents a final area for robust collaboration between our two research centers.

The VNEC and ESRC partnerships represent opportunities to apply the rich body of work that CIP/HS has generated in its first ten years of existence. In addition, these relationships offer the opportunity to identify new challenges and innovations to enhance energy security and resilience. We will report these innovations in the future and look for a dynamic road ahead. ❖

8th Annual Homeland Security Law Institute

When
June 19 - 21, 2013

Where
Capital Hilton Hotel
1001 16th St NW
Washington, DC 20036-5794
United States of America

Sponsored by the ABA Section of Administrative Law and Regulatory Practice

To Register Click Here

To View the Program Click Here

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