THE CIP REPORT

CENTER FOR INFRASTRUCTURE PROTECTION
AND
HOMELAND SECURITY

JULY 2013
LEGAL INSIGHTS

VOLUME 12 NUMBER 1

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 *The CIP Report* highlights several legal and regulatory issues in the critical infrastructure field. With articles from academics as well as practicing counsel, this issue offers insightful analysis on a broad spectrum of legal topics.

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

First, Professor David Fidler examines legal rules governing cybersecurity in the international realm, as well as existing gaps. Then, George Baker, William Harris, and Thomas Popik evaluate the legal and policy considerations of protecting the U.S. electric grid from electromagnetic pulse threats. Next, Michael Kennedy of the Agricultural Retailer's Association explains the regulation of ammonia nitrate and anhydrous ammonia in light of the tragic explosion inWest, Texas. Finally, Professor Joseph MacDougald uses recent legislative efforts in Connecticut to advocate for task forces and microgrids as a means of hardening electrical infrastructure against severe weather.

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

As always, 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

Mind the Gap: Explaining Problems with International Law Where Cybersecurity and Critical Infrastructure Protection Meet

by David P. Fidler, James Louis Calamaras Professor of Law,
Indiana University Maurer School of Law

Critical infrastructure protection (CIP) policy emphasizes the importance of protecting such infrastructure from vulnerabilities associated with information and communication technologies (ICTs) and recognizing that networked ICTs (and the network architecture) constitute critical infrastructure. Similarly, cybersecurity policy identifies CIP as an objective. The CIP-focused and cybersecurity approaches have stressed the need for international cooperation, including the value of developing international legal rules. However, after over a decade of experience, a gap persists between the much-proclaimed need for more effective international law in this area and the international law that exists.

Three factors explain the gap's persistence. First, cooperation on CIP and its cyber features developed within existing diplomatic mechanisms without requiring new international law. Second, patterns in cybersecurity policy affect what states seek to achieve and how they use international law. Third, international politics on cybersecurity increasingly reflect geo-political competition—a context that has never proved conducive to international law. These factors create obstacles for developing international law on the cyber aspects of CIP, meaning that the existing gap might go from persistent to permanent.

International Cooperation on Critical Cyber Infrastructure

Efforts to bolster CIP, including its cyber aspects, include international cooperation. National CIP strategies identify such cooperation as critical; bilateral relations often involve CIP elements; regional organizations, such as the European Union and Organization of American States, facilitate collaboration on CIP; security organizations, such as NATO and the Shanghai Cooperation Organization, work on CIP; and multilateral institutions, such as the UN, stress the importance of cooperation to achieve better CIP. With some exceptions, this cooperation has proceeded without the need for, or the production of, new international legal rules or

(Continued on Page 3)

* Image courtesy of scottchan/FreeDigitalPhotos.net.

(Continued from Page 2)

instruments specific to the protection of critical cyber infrastructure.

Generally, this cooperation focuses on building domestic capacities to identify and respond to cyber threats, sharing information on threats and effective cybersecurity practices, providing assistance when requested, and devoting regular diplomatic attention to this challenge. Existing diplomatic or treaty-based mechanisms have proved flexible enough to allow cybersecurity and its CIP elements to become part of the agenda. Although most cooperative efforts have not generated new international law specific to the protection of critical cyber infrastructure, they echo international law on transboundary pollution and industrial accidents, which includes responsibilities to prevent and mitigate threats, consult and share information, provide assistance, and engage in periodic diplomacy to improve cooperation.

Specific international rules and mechanisms that have emerged are limited in scope or substance. For example, the EU requires members to identify "European critical infrastructure" in the energy and transport sectors, provide information about such designations, and mandate that operators have security plans.[1] Members of the Shanghai Cooperation Organization agreed to cooperate on "[e]nsuring information security of critical structures of the Parties."[2] A draft African Union treaty requires parties to adopt a national cybersecurity policy that includes protecting "essential information infrastructure."[3]

To date, state practice reveals a preference for using existing mechanisms for cooperation on CIP and its cyber components rather than establishing new legal regimes. Proposals to create-cyber specific international law, such as an obligation to provide assistance to victims of cyber attacks or prohibitions against attacks on the Internet's root servers, have not gained diplomatic traction. Whether this preference remains dominant will depend, in part, on how cybersecurity policy changes and what impact those changes have on prospects for using international law.

Patterns in Cybersecurity Policy and Their International Legal Implications

Although cybersecurity policy is complex, three patterns have emerged. First, policymakers have used a "cyber threat" approach in which they classify an incident into existing categories—crime, terrorism, espionage, and armed conflict—and then apply the policies and legal rules associated with each category. International law exists for each category, but states have so far only developed specific international law for cyber crime (e.g., Council of Europe Convention on Cybercrime). For terrorism, espionage, and armed conflict, pre-cyber international law is applied to cyber incidents (e.g., the law of armed conflict).

However, experts debate the efficacy of this approach, with critics observing that international law on crime, terrorism, espionage, and armed conflict cannot handle cyber threats adequately. Although it is the most prominent cyber crime instrument, the Convention on Cybercrime's effectiveness has been challenged, especially because of its limited number of state parties (39 as of June 2013). Further, international law does not seriously constrain espionage, which creates a permissive context that adversely affects CIP. Despite recent efforts to clarify how the law of armed conflict applies to cyber warfare,[4] its utility for CIP during armed conflict remains unclear.

The second pattern in cybersecurity policy is the "cyber defense" approach, which focuses on defending against cyber threats regardless of their type or origin.

(Continued on Page 4)

---

[1] Council Directive 2008/114/EC 345/75-345/76, Dec. 8, 2008, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:EN:PDF.

[2] Agreement on Cooperation in the Field of International Information Security, 2008, Art. 3.

[3] Draft African Union Convention on the Establishment of a Credible Legal Framework for Cyber Security in Africa, Jan. 1, 2011. Art. III-1-4, http://www.itu.int/ITU-D/projects/ITU_EC_ACP/hipssa/events/2011/WDOcs/CA_5/Draft%20Convention%20on%20Cyberlegislation%20in%20Africa%20Draft0.pdf.

[4] International Group of Experts, *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge: Cambridge University Press, 2013), http://issuu.com/nato_ccd_coe/docs/tallinnmanual?e=5903855/1802381.

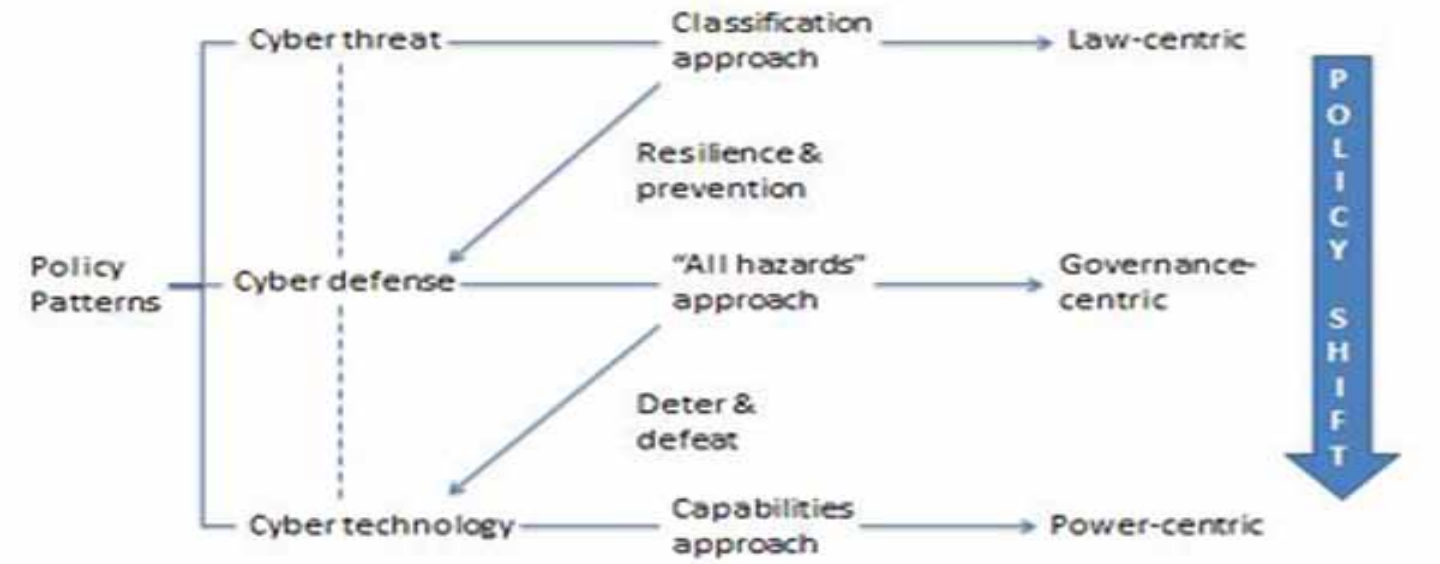
(Continued from Page 3)

This approach adopts an "all hazards" strategy that does not require slotting cyber intrusions into existing policy and legal categories. The motivation behind emphasizing cyber defense relates to concerns that the cyber-threat approach is too reactive, faces technical and legal attribution problems, and fails to achieve prevention, deterrence, or resilience.

Stressing cyber defense produces different legal issues, including the impact of "active defenses" on the principles of sovereignty and non-intervention, the effect of heightened electronic surveillance and information sharing on civil liberties, the problem of regulating critical infrastructure operated by the private sector, and ideological disagreements about Internet governance. While the cyber-threat approach applies existing law (*lex lata*) to cyber incidents, the cyber-defense approach more directly raises questions about what law should be (*lex ferenda*), which stimulate larger considerations about governance on which consensus does not exist (e.g., how should cybersecurity and privacy be balanced?; should Internet governance be more intergovernmental or multi-stakeholder in nature?; and should it emphasize sovereignty or "Internet freedom"?). The lack of consensus limits what states can achieve through international law when cyber defense is the focus.

The third pattern involves emphasis on developing "full spectrum" cyber capabilities—the technological ability to defend against, deter, and—if needed—defeat cyber threats. This "cyber technology" approach holds that focusing on defensive measures is inadequate because, in cyberspace, the offense always has the advantage. Cybersecurity requires technological capabilities that permit not only robust defense but also offensive operations. This pattern is prominent in U.S. policy, as evidenced by actual and contemplated offensive cyber attacks against states and terrorist websites, development of "full spectrum" cyber capabilities by the military and intelligence community, and establishment of "rules of engagement" for offensive operations. Experts believe many countries, ranging from China to Iran, are scaling up their intelligence

(Continued on Page 5)



(Continued from Page 4)

and military cyber capabilities. However, this pattern creates problems for collective action. For example, though keen on cyber defense, NATO members, to date, have resisted discussing the Alliance developing offensive cyber capabilities or engaging in offensive cyber operations.

The cyber-technology approach connects more with material power than application of *lex lata* or development of *lex ferenda*. Technological prowess, rather than law, determines how well critical cyber infrastructure is protected from cyber attack. The cyber-technology approach moves policy closer to managing cybersecurity through balance-of-power politics, including making credible the threat to use cyber capabilities to deter serious attacks on critical infrastructure. In other contexts, international law has not fared well when balance-of-power politics characterized the dynamics of international relations.

Geo-Politics, Cybersecurity, and Critical Infrastructure Protection

In addition to these patterns, cybersecurity policy has shifted in emphasis. Although each pattern remains part of cybersecurity, the patterns overlap in ways that reveal a restless search for more effective strategies. In the CIP context, policymakers have not been content to rely on international legal instruments on cyber crime but have moved to bolster cyber defenses against the range of cyber threats that exist against critical infrastructure. Experts perceive that more powerful countries, including China, Russia, and the United States, are not basing strategies on defensive measures alone but are developing "full spectrum" capabilities to defend against, deter, and defeat serious cyber attacks.

This shift flows from not only the evolution of thinking about cyber threats but also the rise of cybersecurity as a strategic problem in competition among the great powers, especially between the United States and China. Recent events illustrated how raw cybersecurity issues have become in Sino-American relations, with the United States accusing China of cyber theft of U.S. companies' trade secrets, and China accusing the United States of cyber attacks against Chinese targets (accusations assisted by Edward Snowdon's revelations about secret U.S. cyber activities). Although both countries have discussed these problems at a summit and created a working group to address cyber issues, the prospects for new international agreements from this process are, in the current climate of deep mistrust, not good.

Geo-political tensions do not preclude great powers from cooperating, as illustrated by new U.S.-Russia cybersecurity initiatives announced in June 2013, which include confidence-building measures (e.g., information sharing) and a "cyber hot line." However, whether these kinds of initiatives will change the trajectory of cybersecurity in great power politics is doubtful. Confidence-building measures might permit countries to cooperate better on, for example, cyber crime, but such measures do not address strategic tensions related to the threats cyber espionage and military cyber capabilities present to critical infrastructure. And tensions continue to mount, as illustrated by CIP concerns about the security of global ICT supply chains and the licit and illicit markets for "zero day" software exploits. The distrust among the great powers on these strategic and emerging issues represents an obstacle to development of more cyber-specific rules of international law that might benefit CIP.

The gap between calls for additional international law on cybersecurity and critical cyber infrastructure, but existing international law will persist despite cooperation on CIP and its cyber aspects having taken root around the world. Although existing rules and mechanisms facilitate cooperation, policy shifts in cybersecurity are creating a more difficult environment for international law with respect to applying these rules and developing more cyber-specific norms. Given this reality, progress in international cooperation on CIP will depend less on new international law than on maximizing the potential like-minded states can wring from existing regimes, diplomatic venues, and technological capabilities. ❖

Protecting the Electric Power Grid from Electromagnetic Pulse Threats: Legal and Policy Considerations

by George H. Baker, William R. Harris, and Thomas S. Popik

Since the release of the 2004 and 2008 reports of the congressionally authorized Commission to Assess the Threat to the United States from Electromagnetic Pulse Attack ("EMP Commission"), there has been a growing societal realization that civilian infrastructure is vulnerable to electromagnetic pulse (EMP) threats. And among the Department of Homeland Security (DHS) list of critical infrastructure sectors, the electric power grid is both the most vulnerable, because EMP couples most efficiently to long power lines, and the most critical, because the grid is the keystone infrastructure upon which all other infrastructures depend. Simply put, grid failure is an existential threat to the survival of the United States as a nation and to the American population.

EMP threats can be broadly categorized into man-made threats—such as nuclear EMP or intentional electromagnetic interference (IEMI)—and naturally occurring solar storm effects, commonly called "geomagnetic disturbance" or GMD. Nuclear EMP is caused by detonation of a warhead in the upper atmosphere, while IEMI can be induced by non-nuclear weapons such as the recently-tested CHAMP drone developed by the U.S. Air Force. GMDs are caused by masses of charged particles released by the sun.

EMP has the potential to cause widespread and long-term collapse of the electric power grid. Both solar storms and nuclear EMP induce currents in long transmission lines, producing surges of thousands of amperes that are known to damage large bulk-power system transformers. The United States is no longer a major manufacturer of large power transformers and under normal conditions it would take 1-2 years to remanufacture and ship replacements from overseas plants. Nuclear EMP also causes a short, very high-voltage pulse that damages sensitive electronic components used in computers and telecommunications equipment. With increasing use of electronic SCADA devices (Supervisory Control And Data Acquisition) and the internet communications by electric utilities within a "smart grid", electric grid control has become highly vulnerable to nuclear EMP. A coordinated IEMI attack on key grid substations also has the potential to cause widespread and long-term grid collapse.

Since the 1950's the electric grid in the United States has evolved into three major interconnections—Eastern, Western, and Texas. While food, drugs, transportation, financial services, and numerous other industries had a federal regulatory regime imposed in the early part of the 20th century, it may come as a surprise that electric utilities successfully avoided federal regulation for grid reliability until just a few years ago. In 2003, a major blackout in the Eastern Interconnection caused reexamination of the voluntary system for grid reliability standards and resulted in enactment of the Federal Energy Power Act of 2005.[1] This Act gave additional federal authority to the Federal Energy Regulatory Commission (FERC), a body previously responsible for rates and tariff-setting for the energy sector. But through action of the North American Electric Reliability Corporation, the self-regulatory organization known as NERC, the electric utility industry must propose reliability standards before FERC can adopt

(Continued on Page 7)

[1] *See* Federal Power Act, 16 U.S.C. §824a-2 (2006). This Act provides for designation of an Electric Reliability Organization, presently NERC, that proposes reliability standards which FERC may approve or order NERC to reconsider and resubmit for FERC approval before the standards take effect.

(Continued from Page 6)

them. To date, NERC has not proposed reliability standards to mitigate hazards of electromagnetic pulses, whether naturally occurring or man-made.

A moderate solar storm in March 1989 resulted in a Province-wide blackout for Quebec, Canada and more than six million electric customers; this event amply demonstrated that EMP from geomagnetic disturbance can cause both cascading grid collapse and permanent damage to high voltage transformers. In the subsequent 24 years, NERC issued multiple reports on solar storm threats and convened a Geomagnetic Disturbance Task Force, but avoided initiating a formal reliability standard. Finally, in May 2013, the FERC Commissioners voted 5-0 to order NERC to impose a GMD reliability standard, an unprecedented use of FERC's "sua sponte," or self-initiating, authority.

Nuclear power plants generate approximately 18-19% of baseload power for the U.S. electric grid, but are regulated by a separate federal agency, the Nuclear Regulatory Commission (NRC). Importantly, nuclear power plants cannot operate while the local grid is in outage, nor generate their own long-term power for cooling of reactor cores and spent fuel pools. During short-term Loss of Outside Power (LOOP) conditions, nuclear plants are dependent on diesel generators, which typically have a seven-day supply of fuel on site. Nuclear plants are vulnerable to EMP effects, both directly on reactor control electronics, and indirectly through loss of commercial grid power.

In February 2011 the Foundation for Resilient Societies, a non-profit group that researches critical infrastructure protection, filed a petition with the NRC to require nuclear power plant operators to install backup power for spent fuel pool cooling in the aftermath of severe solar storms resulting in long-term grid outage. Despite opposition from the Nuclear Energy Institute, the trade association for nuclear plant operators, in December 2012 the NRC acted to further consider Petition for Rulemaking PRM-50-96, the first favorable ruling on a public stakeholder petition out of 116 petitions filed since the year 2000. Yet this ongoing rulemaking would protect nuclear plants against solar storms but not against foreign threats—including the threat of nuclear EMP attack. In order for the NRC to protect against man-made EMP threats, the Commission would need to restrict, as it has done before, the so-called "Enemy of the State" rule that the Commission adopted in 1967.[2] By requiring protection against high-altitude EMP hazards, the Commission could significantly reduce costs to protect control rooms and critical equipment for all newly-licensed facilities, and require backfitting for existing nuclear power plants.

Two legislative initiatives to protect against EMP, the GRID Act and the SHIELD Act, have been introduced in the U.S. Congress. The GRID Act was unanimously passed by the U.S. House of Representatives in 2010, but was never acted upon by the Senate. At the time of this writing, the SHIELD Act is currently pending in the House.[3] While legislative initiatives for EMP protection have gained widespread public support, the reality of the legislative process is that bills can be effectively blocked by just one or two members of key committees—recently, the House Committee on Energy and Commerce Committee, and the Senate Energy and Natural Resource Committee. In written testimony before Congress, NERC has opposed legislation to protect against the geomagnetic storm aspect of EMP, citing the need to balance GMD risks against mitigation costs. However, according to a report produced by Oak Ridge National Laboratory for FERC and other federal agencies, average yearly

(Continued on Page 8)

[2] *See* 10 C.F.R. § 50.13: "Attacks and destructive acts by enemies of the United States; and defense activities" providing "An applicant for a license to construct and operate a production or utilization facility, or for an amendment to such license, is not required to provide for design features or other measures for the specific purpose of protection against the effects of (a) attacks and destructive acts, including sabotage, directed against the facility by an enemy of the United States, whether a foreign government or other person, or (b) use or deployment of weapons incident to U.S. defense activities." 32 FR 13445, Sept. 26, 1967. This doctrine was affirmed in *Siegel v. AEC*, 400 F.2d 778,783-784 (1968).

[3] *See* H.R. 2417 introduced on June 18, 2013. This proposed legislation would strengthen FERC's authority to impose reliability standards to protect against both geomagnetic storms and man-made EMP, adding a new Section, 215A, to the Federal Power Act.

(Continued from Page 7)

cost of installing equipment to mitigate severe solar storms is estimated at less than 20 cents per year for the average residential customer.[4]

Frustrated with blocked EMP protection legislation in the U.S. Congress, some state legislators have acted. For example, Representative Andrea Boland and other Maine legislators succeeded in passing legislation that requires the Maine Public Utility Commission to study and report back to the legislature on EMP protection that could be implemented for an ongoing $1.4 billion transmission line upgrade in that state.[5]

Action under existing legal authority of the Executive Branch is also an option for EMP protection. While FERC and NERC now have a reliability standard for solar storm EMP protection in development, the timeline for installation of protective hardware will be in the year 2015 at the earliest. Meanwhile, during the peak and active backside of the 11-year solar cycle, the United States could be unprotected against severe solar storms. However, the President has existing legal authority to de-energize substantial portions of the three U.S. regional grid interconnections, including all nuclear, gas-fired, and oil-fired generation facilities upon confirmed warning of a severe solar storm.[6] De-energizing transformers with long replacement times could reduce grid recovery time and save millions of lives.

The insurance industry has initiated changes in underwriting practices to reduce inadvertent coverage for equipment and business interruption losses during and after severe solar storms. The first step towards revised underwriting practices has been to reassess risks of catastrophic losses, both by region and by electric utility. A recent Lloyds of London study[7] determined that an extreme geomagnetic storm is virtually inevitable. The study cited increased human and financial risks due to grid aging and our increasing dependence on electricity. Weighted by population, Lloyds determined that the highest risk area of the United States is the Atlantic corridor between Washington D.C. and New York City. Other high-risk regions are New England; upper Midwest states such as Michigan and Wisconsin; the Pacific Northwest; and portions of the Gulf Coast. As the insurance industry sets differential rates that depend upon decisions to provide or forego hardware protection for vulnerable grid equipment, financial benefits of protecting critical grid equipment may better align with federal reliability standards. However, because insurance covers fortuitous risks and not "acts of war" the burden of initiating protection against man-made EMP risks will remain with governmental decision-makers.

In conclusion, legal options for EMP protection of the electric grid include: regulatory action by FERC and the NRC; federal and state legislation; emergency action under existing Executive Branch authority; and contractual agreements by private parties such as insurance carriers and their insureds. Already, active participation by public stakeholder groups has encouraged EMP protection. The principal impediment to EMP protection is not cost, but citizen and legislative awareness. As usual, legal mandates and public policies need to catch up with scientific developments. ❖

---

[4] *See* Oak Ridge National Laboratory, *Electromagnetic Pulse: Effects on the U.S. Power Grid*, January 2010, *available at* http://www.ornl.gov/sci/ees/etsd/pes/pubs/ferc_Executive_Summary.pdf (last accessed July 11, 2013).

[5] L.D. 131, enacted by the Maine legislature in June 2013, empowers the Maine Public Utilities Commission to periodically assess protection of Maine transmission and distribution companies against both solar and man-made EMP hazards.

[6] *See* 3 U.S.C. §301.

[7] Lloyd's of London; "Solar Storm Risk to the North American Electric Grid," Maynard, Smith, and Gonzales, AER.

* Image courtesy of franky242/FreeDigitalPhotos.net.

The West Fertilizer Accident: A Road Map of Ammonia Nitrate and Anhydrous Ammonia Regulations for Agricultural Retailers*

by Michael Kennedy, Public Policy Counsel, Agricultural Retailer's Association

On April 17, a massive explosion at the West Fertilizer Plant in the town of West, Texas, killed at least 15 people and injured more than 160 people. The impact of the blast was equivalent to a 2.1 earthquake and felt for miles, but for the agricultural (ag) retail industry the repercussions will resonate for years. Although there is no indication that the blast was anything other than an industrial accident, authorities are treating the scene as if it was a criminal act. Many media reports try to claim that a lack of regulation of ammonia nitrate (AN) and anhydrous ammonia (NH_3) was the problem, but until the Chemical Safety Board establishes the root cause, it is too dangerous to speculate.[1]

AN and NH_3 are heavily regulated by various federal and state agencies across multiple areas of expertise: terrorism (DHS), workplace safety (Occupational Safety and Health Administration- OSHA), air quality (Environmental Protection Agency- EPA), highway safety (Department of Transportation- DOT). And, this does not take into account voluntary consensus standards for products adopted by retailers created by the National Fire Protection Association (NFPA) and American National Standards Institute (ANSI).

The Agricultural Retailer's Association (ARA) works closely with federal and state agencies to further educate and provide services to support its members in their quest to maintain regulatory compliance, a profitable business, and help feed the world. The following sections of this article provide a road map of Ammonia Nitrate (AN) and Anhydrous Ammonia (NH_3) regulations that ag retailers need to comply with.

OSHA: Workplace Safety

OSHA ensures that all chemical hazards produced or imported are classified, and that information concerning classified hazards is transmitted to employers and employees along with first responders. OSHA regulates the storage of AN and NH_3 and requires emergency response plans, emergency response training, and compliance with all OSHA hazardous communication standards.

Ag retailers are required to provide material safety data sheets (MSDSs or SDSs) and emergency response plans to first responders so they know how to handle the hazard. As many retailers know, SDSs are an important component of product stewardship and occupational safety and health. They provide workers and emergency personnel with procedures for handling or working with that substance in a safe manner (NH_3 and AN included). Information such as physical data (melting point, boiling point, flash point, etc.), toxicity, health effects, first aid, reactivity, storage, disposal, protective equipment, and spill-handling procedures are condensed into a one- to two-page fact sheet.

DHS: Terrorism Prevention

DHS regulates Chemical Security Anti-Terrorism Statutes (CFATS) that present high levels of security risk. AN and NH_3 fertilizers are considered chemicals of interest under CFATS for different threats. Under CFATS, any facility storing more than 400 lbs of AN (or 2,000 lbs of agricultural grade AN, which

(Continued on Page 10)

* This article was adapted from an article originally published in the AG Professional Magazine, found here.

[1] At the time of this publication little information is available to determine the root cause of the explosion. West Fertilizer is not a member of the Agricultural Retailer's Association.

(Continued from Page 9)

normally has less than 0.2 percent combustible organics) is considered a theft threat and therefore must submit a "top screen survey application" to DHS. NH_3 is a toxic chemical release threat, and as such has a screening threshold quantity (STQ) of 10,000 lbs.

A top screen is used to determine whether the facility presents a high-level security risk. If so, the facility is required to submit a security vulnerability assessment (SVA) to DHS. The department reviews the SVA and advises the facility as to its status as a covered facility. DHS has established four tiers of security risk—Tier 1 for the highest risk facilities and Tier 4 for the lowest risk facilities. A facility that is tiered in one of the four tiers must submit a site security plan. If DHS determines a facility is not a threat, no tier will be assigned and DHS will advise the facility that no further action is required. To our knowledge, not one ag retailer has been inspected, but such lower risk facilities are scheduled for inspection starting this year.

DHS regulates the sale and transfer of AN by each facility that handles this product in order to prevent its misappropriation or use in an act of terrorism. However, the rule has been held up in the rule making process since 2008 with an expectation of a final rule released by the end of 2013.

DOT: Hazardous Material Transportation

DOT regulates the transportation of hazardous materials, including AN, which is administered by the Pipeline and Hazardous Material Safety Administration (PHMSA). The DOT regulations govern the transportation of hazardous materials by highway, rail, vessel, and air. The regulations address hazardous materials classification, packaging, hazard communication, emergency response information, and training.

AN is classified as a 5.1 oxidizer, and in quantities of 1,000 lbs or more must be placarded and meet certain container specifications. Companies that transport AN must train employees, register with DOT, and comply with all other applicable PHMSA requirements for hazardous materials. DOT also considers AN to pose a security risk; therefore all placarded loads must have a security plan, and motor carrier drivers must have a commercial driver's license with a hazardous materials endorsement.

EPA: Air Quality Standards

EPA regulates air emissions from stationary and mobile sources. Among other things, this law authorizes EPA to establish National Ambient Air Quality Standards to protect public health and welfare and to regulate emissions of hazardous air pollutants.

Under Section 112(r) of the Clean Air Act, ag retailers with more than 10,000 lbs of NH_3 must develop a risk management plan that documents and describes a facility's hazard assessment and response plan. The assessment must document the worst case scenario for a chemical accident and the consequences of that scenario, and implement accident prevention and emergency response programs.

Consensus Standards: ANSI and NFPA

The NFPA has developed a code for AN storage. By itself, AN is not combustible. However, AN is an oxidizer, and it can accelerate the burning of fuels when it is involved in a fire. Code 490 applies to the storage of AN, which includes storage in containers, storage in bulk, contaminants, and fire protection. According to the ANSI Standard for Storage and Handling of NH_3, the conditions favorable for ignition are seldom encountered during normal operations due to the high ignition temperature required. However, NFPA 490 recommends that should a fire break out where AN is stored, emergency responders apply large volumes of water as quickly as possible.

Partnerships that Matter

ARA belongs to the Chemical Sector Coordinating Council (CSCC), one of 16 critical infrastructure committees established to facilitate effective coordination between the private sector and federal, state, local, territorial and tribal governments. Just recently, ARA also forged a partnership with the FBI and has been working with them on security education and outreach efforts. FBI representatives have made presentations at ARA meetings

(Continued on Page 11)

(Continued from Page 10)

and exhibited at the 2012 ARA Conference.

Several years ago, ARA joined The Fertilizer Institute (TFI) in putting together the "Know Your Customer" Campaign. This campaign was initiated to prevent the misuse of nitrate-based fertilizer and provides retailers with suggested guidelines to follow regarding the sale of these products.

Additionally, tools like the Asmark Security Vulnerability Assessment (SVA) help ag retailers identify and evaluate potential security threats, risks, and vulnerabilities. ARA has been working with Asmark, TFI, and CropLife America on this program since 2003, well before the DHS CFATS program was established. ARA also participates in the Fertilizer Institute Security Task Force which works with the Joint IED Defeat Organization (JIEDDO), a leader in Department of Defense efforts to detect, counter, and neutralize improvised explosive devices.

A Path Forward

ARA members take pride in offering products and services to their farmer customers that help provide food, feed, fuel, and fiber to the world. While we should not speculate about the root cause of the West Fertilizer accident, ag retailers continue to comply with AN and NH_3 regulations in striving towards the most efficient, safe, and best practices to accomplish their goals. ARA continues to carefully monitor safety and security issues and works with government agencies and allied organizations to apply any lessons learned so a tragic incident like the facility explosion in Texas will never happen again. ❖

Two Legal Responses to Storm-Threatened Critical Infrastructure: Task Forces and Microgrids

by Joseph Allan MacDougald*

"Superstorm Sandy did change the conversation around infrastructure, particularly in the Northeast."
- Robert Puentes, The Brookings Institution[1]

Extreme weather events now seem so frequent they have lost their shock value.[2] China experienced one of its coldest winters in nearly 30 years. Severe heat waves and fires raged across Australia in January,[3] and then across the United States in June.[4] Tornadoes of record intensity plague the Midwest.[5] Extreme weather is discussed on the campaign trail and in commencement speeches.[6] Taken as individual events, elected officials typically "vow to rebuild" without reassessing the changing storm realities.[7]

Yet the Northeastern United States, particularly Connecticut, is beginning to move the policy debate from episodic repair to systematic infrastructure hardening. One possible reason for this shift might be that Northeastern policy makers are handling stronger and more frequent storms. A 2012 study by Environment America shows that extreme precipitation events have an 85% increase in frequency in the Northeast and a 26% increase in intensity across several decades.[8] Experience bears out the report, when considering the storm timeline:

- *Hurricane Irene*, August 2011 – More than seven million people lost power from the Carolinas to Maine,[9] with parts of Connecticut and New York left without power for a week.

(Continued on Page 17)

---

[1] Alex Goldmark, *Amtrak asks for subsidies in wake of Hurricane Sandy* Marketplace, American Public Media, December 13, 2012, http://www.marketplace.org/topics/life/transportation-nation/amtrak-asks-subsidies-wake-hurricane-sandy (last visited July 14, 2013).

[2] "India is also experiencing record cold, and forecasts in Israel call for 2 inches of snow, a rare occurrence. The Weather Underground reports that the northern Indian state of Uttar Pradesh, where New Delhi is located, has seen record cold temperatures. Temperatures in New Delhi fell to …the coldest daily maximum in 44 years." Sunny Yang, *China is experiencing its coldest winter in decades,* USA TODAY, Jan. 8, 2013, http://www.usatoday.com/story/news/world/2013/01/08/china-cold/1817271/ (last visited July 14, 2013).

[3] "Four months of record-breaking temperatures stretching back to September 2012 have produced what the government says are 'catastrophic' fire conditions along the eastern and southeastern coasts of the country, where the majority of Australians live." Matt Siegel, *Record Heat Fuels Widespread Fires in Australia,* New York Times, Jan. 9, 2013, http://www.nytimes.com/2013/01/10/world/asia/record-heat-fuels-widespread-fires-in-australia.html (last visited July 14, 2013).

[4] "While no single wildfire can be pinned solely on climate change, researchers say there are signs that fires are becoming bigger and more common in an increasingly hot and bone-dry West." Alicia Change & Seth Borenstein, *Climate Change And Wildfires: Bigger, Fiercer Blazes Expected In West,* Huffington Post, July 5, 2013, http://www.huffingtonpost.com/2013/07/05/climate-change-wildfires_n_3550397.html (last visited July 14, 2013).

[5] Matthew DeLuca, *El Reno tornado, at 2.6 miles across, was widest on record*, NBC News, June 4, 2013, http://usnews.nbcnews.com/_news/2013/06/04/18751584-el-reno-tornado-at-26-miles-across-was-widest-on-record?lite (last visited July 14, 2013).

[6] This is an interesting trend for weather events to now make the signposts. The 2013 season saw weather-mentioning commencement speeches from President Obama, Former President Bill Clinton, and Senator Elizabeth Warren.

[7] Interesting proof of this sentiment can be found by a ready Google search of "vows to rebuild" in quotes followed by the name of the particular weather event one has in mind. Example: *"vows to rebuild" flooding* finds the vow to reconstruct flood torn areas from President Obama, Vladimir Putin, Philippine President Benigno Aquino, and Indonesian President Susilo Bambang Yudhoyono. Yet add the word "infrastructure" and the search becomes less pointed and refers dominantly to the health care system.

[8] Travis Madsen and Nathan Willcox, *When It Rains, It Pours. Global Warming and the Increase in Extreme Precipitation from 1948 to 2011,* Environment America Research & Policy Center (Summer 2012) 17, 20, *available at* http://www.environmentamerica.org/sites/environment/files/reports/When%20It%20Rains,%20It%20Pours%20vUS.pdf.

[9] Chris Kahn, *Hurricane Irene Power Outages: Electricity Blackouts Affect 4 Million Homes and Businesses,* The Huffington Post, August 28, 2011, http://www.huffingtonpost.com/2011/08/28/hurricane-irene-power-outages_n_939441.html (last visited July 14, 2013).

(Continued from Page 16)

- *Winter Storm Alfred,* October 2011 –Two months after Hurricane Irene, power was again unavailable for a week or more. The storm came unusually early while the leaves were still on the trees. The leaves trapped the heavy wet snow, decimating trees and powerlines alike.

- *Superstorm Sandy*, October 2012 – This massive, deadly storm devastated coastal New Jersey and parts of New York. The storm created huge flooding in the Long Island Sound.

- *Winter Storm Nemo*, February 2013 – The giant snow totals from this storm hampered the Northeast for weeks and brought comparisons to some of the largest snow storms in history.

Facing frequent power outages, legislatures borrowed the language of national security, turning the conversation toward "hardening" Northeastern electrical infrastructure.[10] Among the regional states, Connecticut in particular had the most frequent electrical disruption across the largest population percentage—yielding a push toward legally enabling creative grid hardening strategies. In assessing this region's critical infrastructure, two early issues have emerged. First, what legislative group leads the policy discussion; and second, what changes in the law are necessary to harden the electrical infrastructure? This article will draw extensively from examples in Connecticut, given the state's recent microgrid legislation.

Infrastructure Working Groups

The storms revealed that Connecticut and New York had rail, electrical, emergency, and hospital infrastructure in flood-prone areas.[11] But infrastructure re-evaluation poses some unusual challenges. Large scale problems require common, broad solutions. Yet local control over infrastructure and the expertise from the utility companies require more stakeholders to be part of the solution. For example, Connecticut long ago abandoned its counties. Unlike New York, which has enacted county-based infrastructure responses, Connecticut has 169 separate municipalities and a constitutional command for a strong home rule form of government. Hence, it is virtually impossible to address infrastructure at the necessary level without the towns.[12]

A trend among these states has been to utilize legislative action to enable working groups or task forces outside of the regular legislative processes. This approach has the benefit of assembling the most motivated constituent parties, but is outside of the traditional legislative committees.

In Connecticut, Governor Malloy launched the "Two-Storm" panel, whose focus included electrical infrastructure needs. This panel recommended a program of legal and policy reform to encourage microgrids in Connecticut. Similarly, the Connecticut legislature created the Shoreline Preservation Task Force, a bipartisan group consisting primarily of legislators from storm-affected coastal towns charged with identifying areas for state action and formulating legislative recommendations, including these for critical infrastructure protection:

- Preparing a shoreline map identifying high hazard areas that are vulnerable to extreme weather conditions and rising sea levels, and compiling a statewide coastal infrastructure inventory to assess the risks to these facilities in high hazard areas and identify potential adaptation strategies;

(Continued on Page 18)

---

[10] For instance, Governor Cuomo's Rebuild NY initiative with a section entitled "Harden our infrastructure," http://www.governor.ny.gov/2013/rebuild-ny. Or Governor Dannel Malloy seeking federal funds "for infrastructure hardening, following the extensive damage incurred most recently from Storm Sandy," http://www.governor.ct.gov/malloy/cwp/view.asp?A=4010&Q=514784. It should be noted that some legal scholars voice concerns over the growing interconnection between natural disaster and national security planning. See Lisa Sun and RonNell Jones, *Disaggregating Disasters*, 60 UCLA L. Rev. 884 (2013).

[11] Neena Satija *Waiting for the next storm, Part 3: A rail corridor exposed,* CT Mirror, May 15, 2013, http://www.ctmirror.org/story/waiting-next-storm-part-3-rail-corridor-exposed (last visited July 14, 2013). *See also* Beth Garbitelli, *Weighing Options and Infrastructure at Hospitals in Flood Zones*. MetroFocus, Dec. 19, 2012, http://www.thirteen.org/metrofocus/2012/12/weighing-options-and-infrastructure-at-hospitals-in-flood-zones/ (last visited July 14, 2013).

[12] Conn. Gen. Stat. § 8-2 et seq., outlining a municipality based framework for land use decisions.

(Continued from Page 17)

- Cartographic documentation of historical shoreline changes, including measurements of erosion, transport, and accretion rates;

- Adopting legislation mandating that sea level rise be addressed in the design for construction or upgrade of sewage treatment plants or supporting infrastructure financed by the state's Clean Water Fund;

- Requiring the Department of Transportation to develop a plan for addressing the impacts of climate change on transportation infrastructure.[13]

Similar state level responses can be found in New York and New Jersey. Governor Cuomo created the New York Works Task Force that conducted a year-long infrastructure study leading to the creation of a $174 billion plan to modernize the state's infrastructure.[14] Likewise in New Jersey, the state's Domestic State Preparedness Act created a Domestic Security Preparedness Task Force with a similar Infrastructure Advisory Task Force.[15]

Counties and municipalities have followed suit. For example, New York's Suffolk County passed legislation to form a working group comprised of legislators and utility representatives to "look at all capital projects in Suffolk County from the perspective of hardening the system, and make a determination as to which County, utility and local government projects could be coordinated to save time and reduce costs."[16]

Microgrids and Submetering—Electrical Grid Hardening in Connecticut

Following through on the panel's recommendations, the Connecticut legislature passed laws encouraging microgrids to protect Connecticut's electrical infrastructure. Microgrids are "sub-grids" located on the electrical system that allows the users to remove themselves from the grid and receive independently generated power. This is called "islanding"—wherein the microgrid becomes a self-contained unit away from the main grid. When coupled with a power-generating source, regardless of the energy production, the microgrid can serve power to those connected to it; when the main grid goes down, the microgrid stays up.[17]

Municipalities have expressed interest in microgrids to service critical town centers comprising gas stations, pharmacies, groceries, and areas for seniors. Once implemented, microgrids will also affect local zoning and land use as municipalities will choose which uses are allowed into the microgrid area. Further, the siting of renewable energy, such as solar or wind power, could receive a bias if connected to a microgrid which powers critical uses. However, the immediate obstacles to microgrid development in Connecticut were legal.

Recommendations from the Two-Storm Panel included a path to enable microgrids in Connecticut, and in 2012 and 2013, the state enacted several laws designed to encourage microgrid development. For instance, Public Act 12-148, An Act Enhancing Emergency Preparedness and Response, required the Connecticut Department of Energy & Environmental Protection to establish a grant and loan program sufficient to create 65 megawatts of submetered power in Connecticut with the specific intention that the homes or businesses served by the microgrid be able to function in island mode.[18] Municipalities approached the Department with proposals for funding grids in areas

(Continued on Page 19)

---

[13] Kevin E. McCarthy *Report of the Shoreline Preservation Task Force*, OLR Research Report, January 14, 2013, http://www.housedems.ct.gov/Shore/pubs/Task_Force_Report_Final.pdf (last visited July 14, 2013).

[14] *New York infrastructure task force to meet in Albany*, Businessweek, Oct. 9, 2012, http://www.businessweek.com/ap/2012-10-09/ny-infrastructure-task-force-set-to-meet-in-albany (last visited July 14, 2013). *Governor Cuomo Announces State's First Ever 10-Year Capital Spending Plan*, Governor Andrew M. Cuomo, June 6, 2013, http://www.governor.ny.gov/press/06062013-10-Year-Capital-Spending-Plan (last visited July 14, 2013).

[15] Ch. 246, N.J. Gen. Stat. C. App.A. 9-64, *available at* http://www.njleg.state.nj.us/2000/Bills/pl01/246_.pdf (last visited July 14, 2013).

[16] County Legislator Wayn R. Horlsey, "Legislature Unanimously Approves Horsley Bill to Improve Infrastructure" (press release, Apr. 29, 2013) http://legis.suffolkcountyny.gov/press/do14/2013/do14pr_042913_infrastructure.pdf (last visited July 14, 2013).

[17] Sara Bronin, *Curbing Energy Sprawl with Microgrids*, 43 Conn. Law Rev., 547 (2010), providing a detailed discussion on the legal and practical intricacies and benefits of microgrids.

[18] While this is a funded program, it is a pilot program with 65 megawatts approximating only 50,000 homes.

(Continued from Page 18)

of high need.

Significantly, Connecticut recently removed a substantial legal barrier to development of private microgrid systems by reforming the state's policies on submetering.[19] Submetering is the process through which a private developer provides power from an independent source of energy, such as a wind turbine or fuel cell, and defrays the cost by charging the tenants directly for the power provided. Connecticut's newly approved energy strategy allows for submetering in multi-unit buildings, increasing incentive for private developers to engage in the process, whereas before, without the ability to charge for this privately installed backup or supplemental power, developers would rationally be reluctant to make the investment.[20]

Until recently, Connecticut's legal regime compelled the developer/power provider to comply with all of the requirements of a fully functioning public utility with the end result that it was prohibitively expensive and administratively complex. The ultimate bill, correcting this problem, modified Connecticut General Statute 16-19ff to allow for submetering to any facility provided that the power source comes either from Class I renewable power or is otherwise in furtherance of the goals of the energy policy.[21] These goals include reliability and grid hardening.

Conclusion

The Northeast has a policy base capable of leading the way toward electrical infrastructure hardening, an important goal given that this arena is bearing the brunt of our changing climate. The task of infrastructure evaluation requires a multi-stakeholder approach across different legal regimes, which is why special action or laws have been employed to create task forces to bring energy and policy stakeholders and legislators together. This process led directly to legal reform enabling microgrid development in Connecticut. Microgrids and submetering are two key components to grid hardening, and through legislative changes that offer pilot programs and pave the way for private development of electrical infrastructure, states can utilize these methods to harden their own critical electrical infrastructure. ❖

** Professor in Residence, Executive Director of the Center for Energy & Environmental Law, University of Connecticut School of Law. With thanks to my Center's research assistant, Kathy Coss (J.D. cand. 2014).*

---

[19] Bryan Cohen, Conn. *AG Announces Order to Secure Refund for Utility Customers*, Legal Newsline, June 10, 2013, http://legalnewsline.com/news/242146-conn-ag-announces-order-to-secure-refunds-for-utility-customers (last visited July 14, 2013).

[20] *See* Sara Bronin, *Building-Related Renewable Energy and the Case of 360 State Street*, 65 Vanderbilt Law Rev. 1875 (2012) for a thoughtful case study and policy discussion of submetering and its broader legal implications.

[21] Conn. Gen. Stat. § 16-1(a)(26) defines a Class I renewable energy source as: "(A) energy derived from solar power, wind power, a fuel cell, methane gas from landfills, ocean thermal power, wave or tidal power, low emission advanced renewable energy conversion technologies, a run-of-the-river hydropower facility provided such facility has a generating capacity of not more than five megawatts, does not cause an appreciable change in the river flow, and began operation after July 1, 2003, or a sustainable biomass facility with an average emission rate of equal to or less than .075 pounds of nitrogen oxides per million BTU of heat input for the previous calendar quarter, except that energy derived from a sustainable biomass facility with a capacity of less than five hundred kilowatts that began construction before July 1, 2003, may be considered a Class I renewable energy source, or (B) any electrical generation, including distributed generation, generated from a Class I renewable energy source."

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 here:
http://listserv.gmu.edu/cgi-bin/wa?SUBED1=cipp-report-l&A=1