THE CIP REPORT

CENTER FOR INFRASTRUCTURE PROTECTION VOLUME 10 NUMBER 5
AND HOMELAND SECURITY

NOVEMBER 2011
RISK MANAGEMENT

EDITORIAL STAFF

EDITORS
Devon Hardy
Olivia Pacheco

STAFF WRITERS
M. Hasan Aijaz
Shahin Saloom

JMU COORDINATORS
Ken Newbold
John Noftsinger

PUBLISHER
Liz Hale-Salice

Contact: dhardy1@gmu.edu
703.993.8591

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

This month's issue of *The CIP Report* focuses on risk management. In particular, we highlight the link between infrastructure protection and risk management.

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

First, the U.S. Department of Homeland Security (DHS) discusses the Critical Infrastructure Risk Management Enhancement Initiative (CIRMEI), a new effort launched by DHS to strengthen infrastructure protection and resilience across all sectors and regions. The risks, costs, and benefits of counter-terrorism protective measures for infrastructure is then assessed by the Director of the Centre for Infrastructure Performance and Reliability at The University of Newcastle, Australia and Professor and Woody Hayes Chair of National Security Studies at Ohio State University. Next, the L.Q. Professor of Engineering and Applied Science at the University of Virginia examines the vulnerabilities and resilience of infrastructure systems. A Senior Expert on Risk Management at the European Network and Information Security Agency (ENISA) then provides an overview of the link between national risk management preparedness and critical information infrastructure protection. The President of the Security Analysis and Risk Management Association (SARMA) explains the benefits of a risk-based approach to managing the Federal Emergency Management Association's (FEMA) preparedness grants. An Associate Professor in the Department of Civil and Environmental Engineering at the University of Delaware then provides insights into the new concept of Resilience Engineering. The future of infrastructure protection is then considered by a doctoral student in the Department of Computer and Telecommunications Systems at the University of Florence and a representave from the European Commission's Joint Research Centre, Institute for the Protection and Security of the Citizen, Security Technology Assessment Unit. Finally, an Associate Professor of Law at the University of Colorado Law School reviews the history of the Terrorism Risk Insurance Act of 2002.

This month's *Legal Insights* analyzes the role of the Legal Risk Manager in protecting critical infrastructure.

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

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

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

The Critical Infrastructure Risk Management Enhancement Initiative: Creating a New Framework to Measurably Enhance Critical Infrastructure Protection and Resilience

by Todd M. Keil, Assistant Secretary for Infrastructure Protection, National Protection and Programs Directorate, U.S. Department of Homeland Security

Over the past decade, the U.S. Department of Homeland Security (DHS) has made great strides in strengthening the protection and resilience of our Nation's critical infrastructure. However, evolving threats, diverse sectors and regions, and limited resources require us to streamline, prioritize, and evaluate the steps we take. That is why we have launched a strategic effort called the Critical Infrastructure Risk Management Enhancement Initiative (CIRMEI), which will strengthen critical infrastructure protection and resilience across all sectors and regions.

Upon my appointment as the Assistant Secretary of Infrastructure Protection in December 2009, a considerable amount of time was spent reviewing documents that either set the basis for, or reported on, the National Infrastructure Protection Plan (NIPP) partnership's risk management efforts — including the NIPP,[1] the National Risk Profile (NRP),[2] and the National Critical Infrastructure Protection Annual Report (commonly referred to as the National Annual Report or NAR).[3] Several things were immediately apparent. First, the documents were not linked to each other in a way that allowed one document to influence another or the resource allocation process. Second, they reported on progress without having a systematic method by which to measure that progress. Finally, the timing of the release of the documents was such that they were not able to directly inform budgetary and programmatic planning.

Because of these observations, in October 2010, the establishment of the CIRMEI was announced. Its goal is to ensure that NIPP critical infrastructure protection and resilience activities achieve outcomes that are developed based upon the most pressing risks and our effectiveness in managing those risks.

This goal will be accomplished in three steps. First, we need to understand the risks confronting the critical infrastructure protection and resilience community each year. Second, we will use metrics to assess our progress toward the achievement of specific outcomes related to the management of risk to critical infrastructure. The outcomes and metrics were developed in collaboration with our sector and State, local, tribal, and territorial (SLTT) partners to ensure that the expertise of the critical infrastructure community as a whole is incorporated into the CIRMEI. Finally, through the budget formulation process, we will address opportunities to improve critical infrastructure and resilience which are identified throughout the initiative. Together, these steps establish a feedback loop that will allow us to adjust our efforts and resources to where they are most needed.

Understanding the Risks to Critical Infrastructure through the National Risk Profile

In the past, the NRP has identified the risks facing critical infrastructure and highlighted areas where the risk landscape has changed or the government's understanding of specific risks has changed. As part of the CIRMEI, the 2011 NRP will also describe how national risks affect specific sectors and regions by incorporating the information provided by our sector and SLTT partners. In addition, we have modified the

(Continued on Page 25)

1. The National Infrastructure Protection Plan provides the unifying structure for the integration of a wide range of efforts for the enhanced protection and resilience of the Nation's critical infrastructure into a single national program.
2. The National Risk Profile is produced annually by NPPD/IP and identifies the risks facing critical infrastructure across all sectors and regions.
3. The National Annual Report is produced by NPPD/IP and assesses the risk management activities of the NIPP partnership.

Assessing the Risks, Costs, and Benefits of Counter-Terrorism Protective Measures for Infrastructure

by Mark G. Stewart and John Mueller*

Evaluating protection measures and policies in a responsible manner does not simply involve ranking targets by their vulnerabilities, by the consequences of an attack on them, or by the likelihood they will be attacked. Rather, it requires a composite cost-benefit assessment in which the costs of protection are systematically blended with the consequences of an attack on a target, with the likelihood the target will be attacked, and the degree to which protection reduces the consequences and/or the likelihood of an attack, keeping in mind issues like the potential for displacement or risk transfer.

The *benefit of a security measure* is a function of three elements:

> Benefit = (probability of a successful attack) × (losses sustained in the successful attack) × (reduction in risk)

The *probability of a successful attack* is the likelihood a successful terrorist attack will take place if the security measure were not in place. The *losses sustained in the successful attack* include the fatalities and other damage — both direct and indirect — that will accrue as a result of a successful terrorist attack. The *reduction in risk* is the degree to which the security measures foil, deter, disrupt, or protect against a terrorist attack. This *benefit*, a multiplicative composite of three considerations, is then compared with the costs of providing the risk-reducing security required to attain the benefit.

The same equation can be used in a break-even analysis to calculate how many attacks would have to take place to justify the expenditure:

> Probability of a successful attack = security cost/ [(losses sustained in the successful attack) × (reduction in risk)][1]

Many reports and studies have highlighted the vulnerability of critical infrastructure to terrorism, and the list of potential targets is extensive, typically including buildings, bridges, airports, dams, pipelines, ports, and nuclear facilities. This article focuses on bridges and applies break-even cost-benefit analysis to determine the minimum probability of a successful attack, absent the security measures, that is required for the benefit of the security measures to equal their cost.

There are 600,000 highway bridges in the United States. Moreover, bridges are — or seem to be — especially vulnerable. It happens, however, that a bridge is very difficult to damage severely because its concrete and steel construction makes it something of a hardened structure from the outset. Buildings are far more vulnerable, and many casualties can be caused if their thin and brittle masonry and glass facades are shattered. The Global Terrorism Database shows that of the 14 bridges attacked by insurgents in the war zones of Iraq and Afghanistan between 1998 and 2007, the total number of fatalities was relatively few at 59, and no more that 10 perished in any single attack (See Figure 1 on Page 4).

Since highway bridges have a large variety of spans, widths, geometry, and other characteristics, it is difficult to generalize about damage costs. However, the replacement and demolition costs for two damaged U.S. interstate highway bridges were $4 million and $11.75 million, and for bridges in Los Angeles from $6.2 million to more than $60 million. Applying this experience, we set replacement costs for a typical interstate highway bridge at $20 million. In addition to the economic cost of traffic diversion, there are other social and economic costs to a community. These are

(Continued on Page 4)

1. Mark G. Stewart, "Risk-Informed Decision Support for Assessing the Costs and Benefits of Counter-Terrorism Protective Measures for Infrastructure," *International Journal of Critical Infrastructure Protection*, 2010, 3(1): 29–40.

Counter-Terrorism *(Cont. from 3)*

harder to quantify but may be in the order of tens to hundreds of millions of dollars because loss of one bridge will generally cause considerable inconvenience and disruption. We will assume this causes a loss of $100 million, and we assume that the expected number of fatalities is 20, at a cost of $130 million based on value of statistical life considerations.[2] The total losses for a damaged bridge, including both the loss of life and economic considerations, thus come approximately to $250 million. This, then, would be the *losses sustained in a successful attack* element in the break-even equation above.

We will conservatively assume that substantial mitigation of blast effects can be achieved at a cost of 20 percent of a bridge's replacement value. If the bridge replacement value is $20 million, the cost of strengthening it is then $4 million. Annualized over a remaining service life of roughly 10 years, this comes to a present value cost of approximately $500,000 per year. This, then, would be the *security cost* element in the break-even equation above.

As for the *reduction in risk* element in that equation, we will generously assume that protective measures reduce the risk by 95 percent. This is substantial and biased in favor of showing that security measures are cost-effective.

Table 1: The probability of an otherwise successful terrorist attack, in percentage per year, required for protective security expenditures to be cost-effective, assuming the expenditures reduce the risk of an attack by 95 percent. Note: A probability greater than 100 percent denotes more than one attack per year.

Cost of security measures (per year)	Losses from a Successful Terrorist Attack						
	$10 million	$100 million	$250 million	$1 billion	$2 billion	$10 billion	$100 billion
$1,000	0.01	0.001	0.0004	0.0001	0.00005	0.00001	0.000001
$100,000	1.0	0.1	0.04	0.011	0.005	0.001	0.0001
$250,000	2.6	0.3	0.11	0.026	0.013	0.003	0.0003
$500,000	5.3	0.6	0.21	0.053	0.026	0.005	0.0005
$1 million	10.5	1.1	0.42	0.105	0.053	0.011	0.0011
$5 million	52.6	5.3	2.10	0.526	0.263	0.053	0.0053
$10 million	105.3	10.5	4.20	1.050	0.526	0.105	0.0110
$100 million	1052.6	105.3	42.10	10.526	5.263	1.053	0.1060
$500 million	5263.2	526.3	210.50	52.650	26.316	5.263	0.5263

Table 1 arrays the annual attack probabilities required at a minimum for security expenditures on protecting a bridge to be cost-effective, assuming the expenditures reduce risk by an impressive 95 percent. This break-even analysis shows that protective measures that cost $500,000 per year and that successfully protect against an attack that would otherwise inflict $250 million in damage would be cost-effective only if the probability of a successful terrorist attack without them exceeds 0.21 percent or one in 480 per bridge per year.[3]

If there were one attack on a highway bridge every year in the United States, the attack probability would be only 1 in 600,000 per bridge per year because there are

(Continued on Page 5)

Figure 1: Vehicle Borne Improvised Explosive Device (VBIED) Damage to Bridge in Iraq (2009).

[2] Value of statistical life is taken to be $6.5 per life saved (in 2010 dollars) as suggested by Lisa A. Robinson, James K. Hammitt, Joseph E. Aldy, Alan Krupnick, and Jennifer Baxter, "Valuing the Risk of Death from Terrorist Attacks," *Journal of Homeland Security and Emergency Management*, 7(1), (2010).

[3] If we assume risk is reduced only by 50 percent (not 95 percent), the minimum attack probability per year required for bridge protective measures to be considered cost-effective increases to 0.4 percent per bridge.

Counter-Terrorism *(Cont. from 4)*

600,000 bridges in the country. This probability is obviously nowhere near the 1 in 480 likelihood of a successful attack required for bridge protective measures to be cost-effective.

If there is a specific threat such that the likelihood of attack massively increases, or if a bridge is deemed an iconic structure such that its perceived value is massively inflated, bridge protective measures may begin to become cost-effective. Thus, San Francisco's Golden Gate Bridge or New York's Brooklyn Bridge might be a more tempting target for terrorists than a more typical highway bridge.

Concerns about this led a blue ribbon panel on bridge and tunnel security to inform the Federal Highway Administration in 2003 that "preliminary studies indicate that there are approximately 1,000 [bridges] where substantial casualties, economic disruption, and other societal ramifications would result from isolated attacks," and that, summing reconstruction costs and socioeconomic losses, the "loss of a critical bridge or tunnel could exceed $10 billion."[4] This is certainly alarming, and an accompanying cost analysis of protective measures for four large U.S. bridges concludes that the cost to protect these bridges ranges from $20.6 million to more than $157.4 million. The protection costs include strengthening (retrofitting) piers, anchors, road deck, tension hangars, and approach highways. These are enormous protective costs. If the average cost of $95.6 million is annualized over a 25-year period, it comes to $5.5 million per year.

We can evaluate the panel's conclusion by referring again to Table 1 (see page 4). Applying the panel's dire expected losses of $10 billion with protective costs rounded down to $5 million per year, the attack probability would need to exceed 0.05 percent, or 1 in 2,000, per bridge per year. Taking the panel's estimate of 1,000 critical U.S. bridges, this would mean that terrorists would otherwise be able to successfully conduct a (truly) massive attack on one of these bridges at least once every two years for these protective costs to be cost-effective. The evidence to date suggests that such a high attack probability is not being observed.

Nearly half of American Federal homeland security expenditure is devoted to protecting critical infrastructure and key resources. Applying commonsense English about what critical infrastructure could be taken to mean, it should be an empty category. If any element in the infrastructure is truly "critical" to the operation of the country, steps should be taken immediately to provide redundancies or backup systems so that it is no longer so. Also, key resources are defined to be those that are "essential to the minimal operations of the economy or government." It is difficult to imagine what a terrorist group armed with anything less than a massive thermonuclear arsenal could do to hamper such "minimal operations." The terrorist attacks of 9/11 were by far the most damaging in history, yet, even though several major commercial buildings were demolished, both the economy and government continued to function at considerably above the minimal level.

Furthermore, it appears that vast sums of money are spent under the program to protect elements of the infrastructure whose incapacitation would scarcely be debilitating and would at most impose minor inconvenience and quite limited costs and would scarcely hamper the minimal operations of the economy or government.

There is no doubt that a terrorist attack on many infrastructure elements could cause considerable damage and significant loss of life. However, while targets such as buildings, bridges, highways, pipelines, mass transit, water supplies, and communications may be essential to the economy and well-being of a society, damage to one or even several of these, with few exceptions, will not be "critical" to the economy, or to the state.

In part, this is because infrastructure designers and operators place much effort on systems modeling to ensure that a failure of one node will not keep the network from operating, even if at reduced efficiency. This is done routinely. For example, it is necessary to close

(Continued on Page 31)

4. Blue Ribbon Panel on Bridge and Tunnel Security, *Recommendations for Bridge and Tunnel Security*, Federal Highway Administration, (September 2003).

On the Vulnerability and Resilience of Infrastructure Systems

by Yacov Y. Haimes, P.E., Ph.D.,
L. R. Quarles Professor of Systems and Information Engineering
Founding Director (1987), Center for Risk Management of Engineering Systems

Why do farmers irrigate their crops in non-rainy seasons? The answer is fundamental to understanding the definitions of vulnerability and resilience of, and the risk to, a system. To know when to irrigate and fertilize a farm to maximize crop yield, a farmer must assess the state of soil moisture and the level of the state of nutrients in the soil.

The literature is replete with misleading definitions of the vulnerability and resilience of a system. Thus, in our quest to provide theoretically based definitions, we must account for the fundamental characteristics of the system. In the parlance of systems engineering, this means that we must rely on the building blocks of mathematical models, focusing on the states of the system.[1]

Decisions are commonly made to achieve specific objectives (to secure specific outputs). From a systems engineering perspective, this implies that to achieve the desired outputs/outcomes by applying decisions/policies, one must control/change certain states of the system. Since this concept is fundamental to the theme of this article, it is appropriate to represent the decision-making process within the context of the states of the system. The behavior of the states of the system, as a function of time, decision, exogenous and random variables, and inputs, enables modelers to describe, under certain conditions, its future behavior for any given inputs (random or deterministic). For example, to determine the safety of drinking water from a reservoir (as a system), one must determine the states of the water in the reservoir: its acidity, turbidity, dissolved oxygen, bacteria, and other pathogens.

To determine the functionality and reliability of a bus, one must know the *states of* the bus's fuel, oil, tire pressure, and other mechanical and electrical components. To treat a patient, a physician first must know the temperature, blood pressure, and other states of the patient's physical health. To control the production of steel, one must have an understanding of the states of the steel at any instant — its temperature, viscosity, and other physical and chemical properties. In other words, all systems are characterized at any moment by their respective state variables. In reality, all state variables are under continuous natural positive or negative emergent forced changes. The term *emergent forced changes* connotes external or internal trends that constitute sources of risk to a system that may adversely affect or enhance specific states of that system and consequently affect the entire system. The decision as to whether a state variable of a system should be modeled as static (constant) or dynamic (time dependent) is one step in the modeler's determination to select only those state variables that represent the "essence" of the system. Note that models are built to answer specific questions, and they must be as simple as possible and as complex as required. For example, risk analysts commonly update the probability of the condition (level) of the state of the system with new information, using Bayes's theorem. For dynamic systems, where the states evolve over time, updating the conditions (levels) of the states of the system is essential. Examples include the states of all physical and cyber

(Continued on Page 7)

[1] Y.Y. Haimes, "On the Definition of Vulnerabilities in Measuring Risks to Infrastructures," *Risk Analysis*; 26(2), (2006), 293-296; Y.Y. Haimes, "On the Definition of Resilience in Systems," *Risk Analysis,* 29(4), (2009), 498-501; Y.Y. Haimes, "On the Complex Definition of Risk: A Systems-Based Approach," *Risk Analysis,* 29(12), (2009), 1647-1654; Y.Y. Haimes, "On the Complex Quantification of Risk: Systems-Based Perspectives on Terrorism," *Risk Analysis*, 31(8), (2011), 1175-1186; and Y.Y. Haimes, *Risk Modeling, Assessment, and Management*, Third Edition. New York: Wiley, (2009).

Infrastructure Systems *(Cont. from 6)*

infrastructures, the economy, technology, and public health.

The centrality of the states of a system requires a formal definition of the term s*tate variable: given a system's model, the states of a system constitute the smallest set of independent system variables such that the values of the members of the set at time t0 along with known inputs, decisions, random and exogenous variables completely determine the value of all system variables for all t > t0.* The selection of the appropriate state variables and their number to represent the essence of the multiple perspectives of the system is among the most challenging and important tasks of systems modelers.

Now we can properly define the vulnerability of a system: vulnerability is the manifestation of the inherent states of the system (e.g., physical, technical, organizational, cultural) that if exploited by an adversary, or affected by a harmful initiating event, can result in adverse consequences to that system. Note that the vulnerability of a system is a vector that is a function of the specific initiating event (or threat) and the time frame; this is a byproduct of the fact that the states of a system are also functions of the random initiating event and the time frame. For example, the human body is vulnerable to infectious diseases. Different organs are continuously bombarded by a variety of bacteria, viruses, and other pathogens. However, only a subset of the human body is vulnerable to the threats from a subset of the would-be attackers, and due to our immune system only a smaller subset of the body would experience adverse effects.

The resilience of a system is also a manifestation of the states of the system. It is a vector that is time and initiating-event (or threat) dependent. Resilience represents the ability of the system to withstand a major disruption within acceptable degradation parameters and to recover within an acceptable composite cost and time. The question "what is the vulnerability of the infrastructure of system X?" is unanswerable, because the answer to this question implicitly depends upon determining (knowing) whether the infrastructure of system X would suffer any damage from any specific threat (initiating event), which is an impossible premise. Similarly, the question "what is the resilience of the infrastructure of system Y?" is unanswerable, since the answer to this question implicitly depends upon determining (knowing) whether the infrastructure of system Y would recover following any specific initiating event (or threat) within an acceptable time and composite cost, disruption of operation, etc., which is an impossible premise. Thus, such questions can be answerable only when the initiating events (or threats or a set of scenarios), and their timing are specifically identified.

The vulnerability and resilience of a system are key concepts in risk analysis. The systems-based definitions of vulnerability and resilience improve our understanding of risk and help make them operational for modeling. Indeed, the vulnerability and resilience of a system are two sides of the same coin. Both are manifestations of the states of the system, whether the system is a physical infrastructure, a cyber infrastructure, or an organization. Both the vulnerability and resilience of a system are multidimensional vectors because the states of a system are vectors that are neither abstract or static, nor deterministic. Thus, neither the resilience nor the vulnerability of a system can simply be measured in a single unit metric. Its importance lies in the ultimate multidimensional outputs of the system (the consequences) for any specific inputs (threats).

The Vulnerability and Resilience of a System in the Context of Risk of Terrorism to Physical or Cyber Infrastructure Systems

There exists interdependence between a specific threat to a system by terrorist networks and the states of the targeted system, as manifested in the system's vulnerability and resilience. A specific threat, its probability, its timing, the states of the targeted system, and the probability of consequences can be interdependent. The three questions in the risk assessment process offered by Kaplan and Garrick,[2] "what can go wrong?" "what is the likelihood?" and "what

(Continued on Page 26)

2. S. Kaplan and B. Garrick, "On the Quantitative Definition of Risk," *Risk Analysis*, 1(1), (1981), 11-27.

National Risk Management Preparedness: The Key to Critical Information Infrastructure Protection

by Louis Marinos, Expert Risk Management,
Eurpoean Network and Information Security Agency (ENISA)
Crete, Greece

Taking protective measures is a genuine activity of any security strategy at any level of the society. Protective measures aim at reduction of exposure to risks and reduction of impact. Without proper risk assessment in place, the effectiveness of measures might be questioned. The monitoring and evolution of protective measures is a result of a proper risk management. Consequently, any protective action regarding critical information infrastructure (CII) needs to follow a risk analysis and needs to be managed with a well-defined risk management process. Given the degree of complexity, dependencies and coverage of CII, the role of national stakeholders in CII protection is a prevailing one. The establishment of a risk management process that applies for all involved entities seems to be of national importance and interest.

ENISA has established a working group to deliver proposals for the governance of National Risk Management (NRM). We introduced the notion of *National Risk Management Preparedness*, meaning the degree of a nation's maturity and effectiveness, in: establishing a policy framework; encouraging risk management within individual CII stakeholder organisations; supporting the implementation of risk management in those organisations; and monitoring and reviewing risk management and adapting national activities accordingly. We have identified the relationship between NRM and the management of information security risk in individual CII stakeholder organisations (i.e. stakeholder mapping).

With regards to *CII stakeholders*, we mean organisations such as governments, sectoral regulators, telecommunications, Internet service providers, and major outsourcers for government information systems. It should be noted that NRM is primarily the concern of national governments and national security institutions. However, all organisations, whether part of national government or of an individual sector, must attach equal importance to the implementation of risk management within their own organisation.

It is important to mention that the proposal for the governance of NRM, as described in this article, is not intended to be used as a blueprint for the creation of a fully functioning NRM programme. However, it is intended to enable governments and other stakeholders in a nation's CII to gain an overview of the elements that are required to build such a programme and to understand the relationships between these elements.

In addition to providing an overview of NRM governance, it is proposed that this article may be used in a number of practical ways by national governments. These include to:

- Identify strengths and weaknesses in the implementation of NRM in their country;
- Assist in the development of a framework for the governance of NRM;
- Help the government to assist CII stakeholder organisations in developing their own risk management processes; and
- Assess the country's NRM preparedness through the use of a defined testing process.

Overall Structure of NRM Governance

Having considered the congruency of information security risk management and NRM, we came to the conclusion that there are three essential components to the governance of information security risk management (in the context of European Union (EU) member states, but possible also outside the EU). These three elements may be described as follows:

1. The establishment of a policy framework to encourage the use of risk management within CII stakeholder organisations in both

(Continued on Page 9)

Preparedness *(Cont. from 8)*

public and private sectors within EU countries.

2. The investment by EU countries in measures to support individual CII stakeholder organisations in their implementation of appropriate risk management activities.

3. The ability of EU countries to monitor and review current NRM implementation levels and adapt national activities accordingly.

Each of these elements may be regarded as outlining the function of one of three processes considered essential to NRM. This document identifies these three processes as follows:

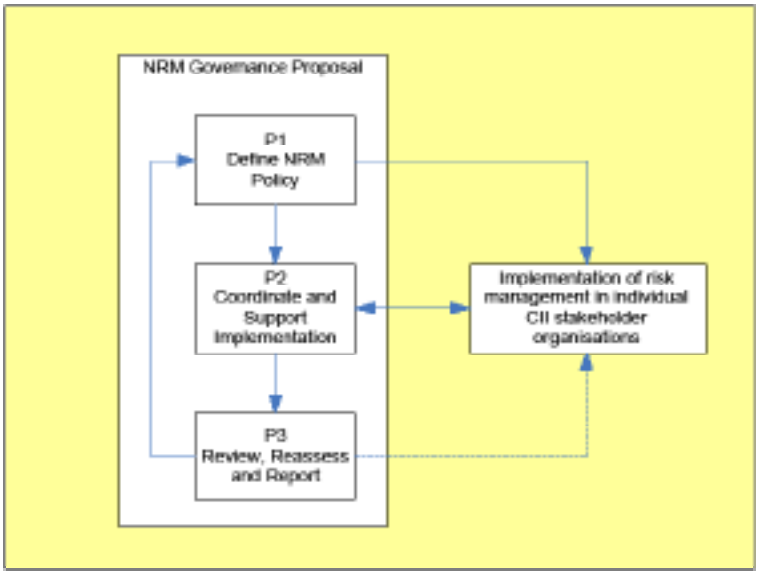
Process 1: The definition of NRM policy;

Process 2: The coordination and support implementation (of risk management in CII stakeholder organisations); and

Process 3: The review, reassessment, and report (on NRM).

The ability of a national government to implement these three NRM processes is taken to be the measure of the maturity of that country in terms of its NRM preparedness.

Figure 2: NRM Governance Proposal and Risk Management in Individual



It is evident that, alongside these three national processes (P1, P2, and P3), individual CII stakeholders must be able to implement effective risk management within their own organisations. Risk management methods for individual organisations encompass the ability to assess risks associated with specific targets (e.g., information systems, applications, or infrastructure components) and then act to manage and mitigate those risks. To do this, it is recommended that organisations use a clear iterative process such as the "Plan, Do, Check, Act" (PDCA) cycle,[1] see Figure 1.

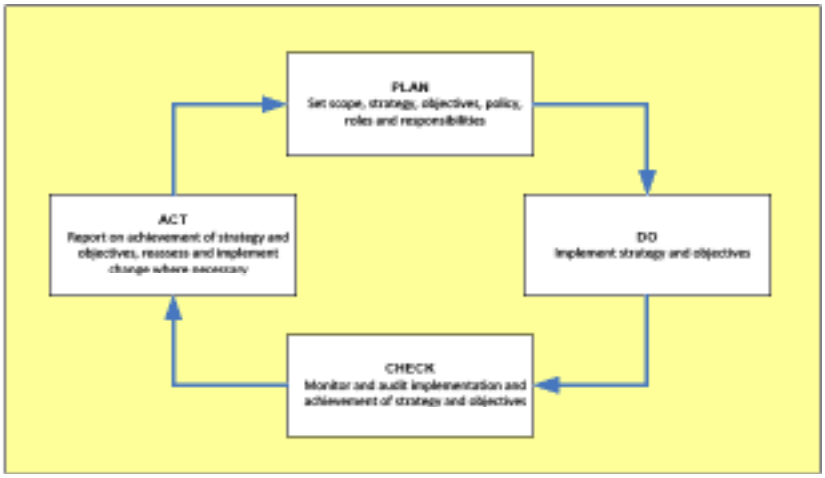


Figure 1: Plan, Do, Check, Act Cycle

The mutual exchange of information between NRM and risk management implementation in individual CII stakeholder organisations is fundamental to the overall management of risk in the national critical information infrastructure. It enables individual CII organisations to manage their risk better by assisting with coordination of risk response and ensuring consistency and effectiveness of risk management methodologies. Conversely, information received from the risk management implementation process in CII stakeholder organisations ensures that governments have up-to-date information about the management

(Continued on Page 10)

3. As described in ISO/IEC 27001: 2005.

Preparedness *(Cont. from 9)*

of threats, vulnerabilities, and impacts experienced, estimated, or perceived by the CII community. Thus governments can steer NRM activities in support of relevant nationwide protection, prevention, detection, and response capabilities.

Figure 2 (Page 9) shows the relationships and dependencies between the NRM processes (P1, P2, and P3) and risk management implementation in individual CII stakeholder organisations.

As Figure 2 indicates, the NRM policy definition process (P1) contributes to the implementation of risk management in individual organisations by delivering rules, guidelines, and stakeholder coordination information. The NRM process for coordinating and supporting implementation (P2) both contributes to the implementation of risk management in individual CII stakeholder organisations (for example, through information sharing) and receives contributions from it (such as information about identified threats, vulnerabilities, and impacts).

The review, reassessment, and reporting process (P3) does not contribute directly to risk implementation in individual CII stakeholder organisations. However, as Figure 2 indicates through the use of a dotted line, P3 does produce reports on the national governance of risk management that may be issued by individual CII stakeholders for informational purposes.

Overview of Proposed Processes

The delivery of NRM must take place within a clear governance proposal. It consists of all the processes and activities that go towards implementing, supporting, coordinating, testing, and maintaining NRM. Figure 3 is an expansion of the process chart shown in Figure 2; it shows not only the three processes (P1 to P3), but also the activities that form part of NRM. As can be seen, within the three processes we have identified 12 activities, shown in Figure 3 as A1 to A12. The box to the right in Figure 3 once again indicates the interdependency between NRM and risk management in individual CII stakeholder organisations.

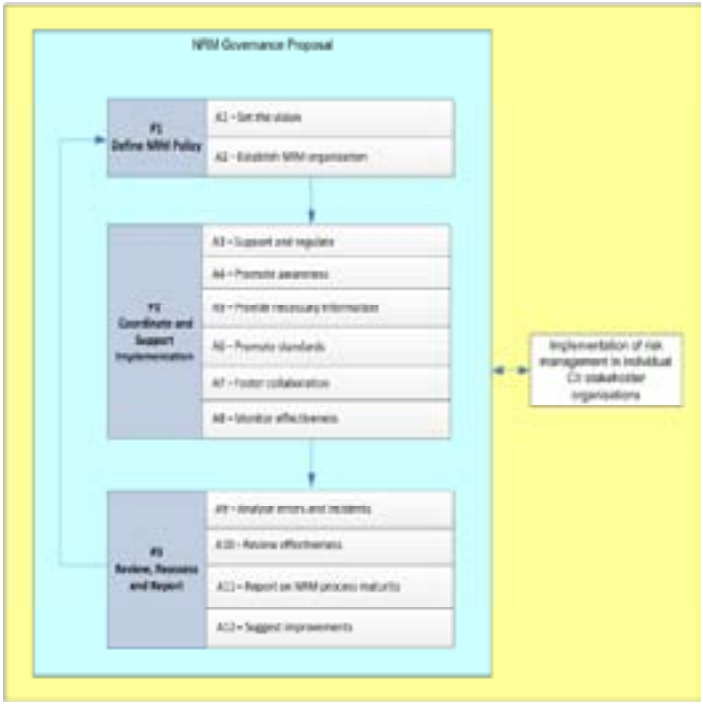


Figure 3: ENISA National Risk Management Activities

Each activity is described in relation to other processes and activities that are present not only within NRM, but also within risk management implementation in individual organisations as well as within other areas such as political, legal, and market activity. The description also includes information about the roles and responsibilities for carrying out each activity. As discussed above, NRM contributes to the implementation of risk management in CII stakeholder organisations. The outputs from each activity forming that contribution are listed as are the inputs to each NRM activity that are produced by risk management actions within CII stakeholder organisations.

The proposed governance structure also suggests that National Security Institutions (NSI) assess the strengths and weaknesses of their NRM by considering the maturity of their capability in each NRM activity. Five clear capability maturity measurement levels have been defined for each activity, based on the five-level model used by the Control Objectives in IT (COBIT) standard.[2] These definitions have

(Continued on Page 11)

2. COBIT 4.1. ISBN 1-933284-72-2. Copyright IT Governance Institute 2007. The model is derived from work by Carnegie Mellon University published in 1993, on behalf of the U.S. government, aimed at the assessment of software contractors.

Preparedness *(Cont. from 10)*

been incorporated into a questionnaire (available at http://www.enisa.europa.eu/act/rm/files/deliverables/WG%202010%20NRMP%20Questionnaire). In addition to assessing their own preparedness, the proposed governance structure shows how governments can determine the strengths and weaknesses of their interaction with CII stakeholder organisations by considering the maturity of their capability in such interactions in relation to each NRM activity. This again, is modelled on the five-level COBIT capability maturity measurements. A questionnaire for this purpose has also been developed.

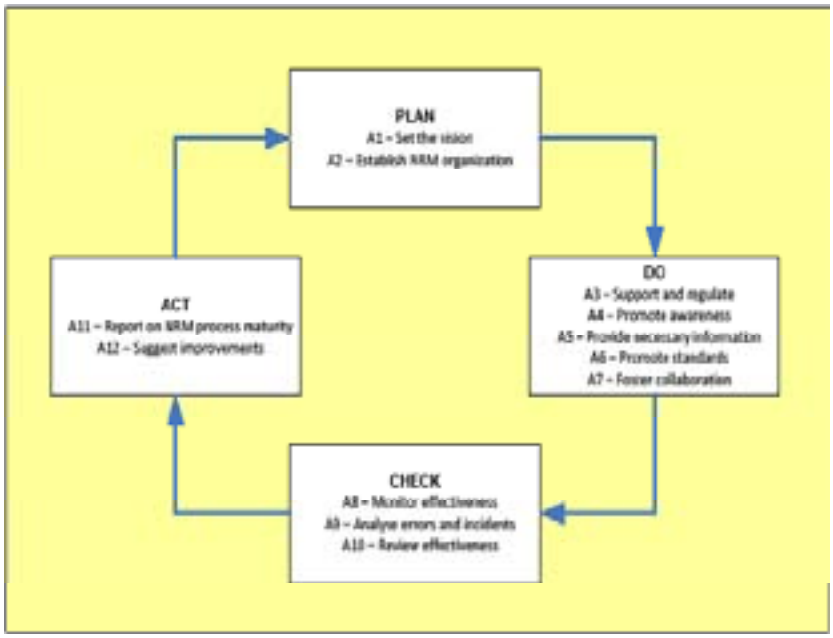
As part of our proposal for implementing governance of NRM, it is intended that NRM activities, like those of information security risk management, should follow an iterative PDCA cycle. Figure 4 illustrates how the 12 NRM activities fit into a PDCA cycle. Following this cycle should assist governments in implementing or developing their own approach for the governance of NRM.

The detailed description of all activities mentioned above can be found in the ENISA report on Risk Management Preparedness (http://www.enisa.europa.eu/act/rm/files/deliverables/WG%202010%20NRMP).

Content of ENISA Work and Open Issues

Apart from the NRM governance proposal, including the description of activities and their input/output

Figure 4: Plan, Do, Check, Act Cycle for NRM Governance Activities.



information, ENISA has developed a number of tools that may be used by various CII stakeholders. These are as follows:

- Questionnaires for use by governments, national security agencies, CII sectoral regulators, and CII stakeholder organisations to assess NRM capability maturity;

- A workflow for developing their governance of NRM; and

- A process for testing NRM preparedness.

The developed governance proposal formed the basis for understanding both how EU member states can develop a standardised way for the governance of their NRM and how they can test their NRM preparedness. However, some issues have not been fully dealt with and further effort may be carried out in a number of areas. Among these are the following:

1. Resolving issues concerning the confidentiality of NRM activities and the degree to which information relating to these activities can be shared with, and between, CII stakeholder organisations.

2. Developing processes for consolidating different NRM governance capability maturity levels in different sectors. For example, the implications for overall NRM preparedness where different sectors have very different levels of capability maturity in their implementation of risk management.

3. The possibility of generalising the proposed NRM governance to enable its use in risk management governance within individual organisations, particularly those with disparate physical or logical constituent groups.

(Continued on Page 27)

Why a Risk-Based Approach to Managing FEMA's Preparedness Grants is both Urgently Needed and Eminently Doable

by Kerry Thomas*

Since September 11, 2001, well in excess of $30 billion in Federal grant money has been provided to states, local communities, and the owners and operators of the Nation's critical infrastructure to enhance all-hazards preparedness. However, quantifying the impact of these grants remains an enormous challenge for the agency charged with administering them, the Federal Emergency Management Agency (FEMA). Over the years, this problem has been approached in a variety of ways, often resulting in new and increasingly complicated reporting requirements, but never allowing FEMA to answer the most fundamental question — how much safer are we as a result of these investments? The urgency of the current fiscal crisis, coupled with the recent release of Presidential Policy Directive (PPD) 8 on National Preparedness, makes this issue impossible to ignore any longer. The good news is that many of the tools needed to address the problem already exist.

Past Efforts to Measure Program Impact

In the early days, from 1998 – 2004, data collection efforts focused largely on the most fundamental issues, such as whether grantees could document that they had followed their approved budgets when making purchases. A parallel planning process was implemented in 1999 that resulted in the collection of baseline capability data at the State and local levels. Grantees were then asked to subjectively determine "needs" and develop State — and later Urban Area — Homeland Security Strategies that would be used to guide grant expenditures. This approach was modified further in 2004, when counting "widgets" was supplanted by efforts to measure program "effectiveness." This included additional reporting requirements, such as the Initial Strategy Implementation Plan (ISIP) and the Bi-annual Strategy Implementation Report (BSIR). Eventually, grantees were required to submit Investment Justifications (IJs) to be peer reviewed by panels of subject-matter experts. Most recently, DHS has sought to measure program impact through capability gain as a part of its Cost to Capabilities (C2C) initiative.

What is Missing?

Getting the most "bang for the buck" should be an important goal of the FEMA preparedness grant programs. However, it cannot be the first step in measuring their impact. In the absence of understanding the actual risks faced, simply optimizing across a portfolio of investments to maximize capability gain does little to guarantee the effectiveness of the expenditure. Establishing a risk baseline first would enable the identification of the actual capabilities required, allow for the measurement of risk reduction from the capabilities gained, and ultimately, support effective comparisons of the return on investment. Figure 1 illustrates this concept using the Government Accountability Office's (GAO) recognized and well established Risk Management Cycle.[1]

Figure 1

Why Act Now?

PPD-8 represents the first complete revision of our national policy on

(Continued on Page 13)

1. Government Accountability Office; *Protection of Chemical and Water Infrastructure: Federal Requirements, Actions of Selected Facilities, and Remaining Challenges*, GAO-05-327, (March 2005).

Grants *(Cont. from 12)*

preparedness since 2003, replacing Homeland Security Presidential Directive (HSPD)-8. The foundation of PPD-8 rests on the creation of a risk-informed National Preparedness Goal. According to PPD-8, the Goal:

…shall be informed by the risk of specific threats and vulnerabilities — taking into account regional variations — and include concrete, measurable and prioritized objectives that mitigate that risk. The national preparedness goal shall define the core capabilities necessary to prepare for the specific types of incidents that pose the greatest risk to the security of the Nation, and shall emphasize actions aimed at achieving an integrated, layered and all-of-Nation preparedness approach that optimizes the use of available resources.[2]

The implementation plan for PPD-8 goes on to explain that the Goal will:

…include a standardized, objective approach for assessing threats and hazards to identify core capabilities and where they are needed, while establishing performance objectives that measure progress towards achieving the Goal. The core capabilities that make up the Goal will represent preparedness priorities that reflect Federal, State, local, tribal, territorial, and private and nonprofit sector perspectives on risk. The threat and hazard identification and risk assessment should consider the range of natural hazards, potential accidents, and terrorist threats and factor in the identification of risks facing States and local communities as well as the Nation as a whole.[3]

Juxtaposed against this new imperative to employ risk as a foundational element of national preparedness policy are the fiscal-year (FY) 2012 appropriations for FEMA's preparedness grants. The House of Representatives recently passed a version of this legislation that would provide nearly $3 billion less than the Obama Administration's request and represent a cut of almost $1.1 billion over FY 2011.[4] The debate around passage of this bill underscored deepening Congressional concern with the lack of metrics for these programs. Rep. Robert Aderholt (R-AL), Chairman of the House Homeland Security Appropriations Subcommittee, had the following to say:

Now, I know there has been some criticism on the funding level this bill is recommending for FEMA's first responder grants. Let me emphasize that not only is there more than $13 billion dollars in the pipeline that has not been drawn down, but FEMA has yet to establish a credible method for measuring the impact of these grants.[5]

The House-passed version of this legislation also creates a single pool of funds out of what had been numerous distinct line items that funded programs like the State Homeland Security Program (SHSP), Urban Areas Security Initiative (UASI), Port Security Grant Program (PSGP), and Transit Security Grant Program (TSGP). The Senate version of this legislation is somewhat less impactful, but the battle lines are drawn. Given the policy direction set forth in PPD-8, the challenges of articulating program effectiveness and the potential need to make difficult decisions about where and how to divide a limited pool of funds, it would seem that the time has come to look anew at how sound risk management principles could contribute to the solution. At the same time, however, history should not be forgotten, as many of the building blocks needed for implementing a risk-based process already exist.

A Path Forward

As noted, many of the components required for a risk-based grants management process already exist, although not all reside within FEMA or in an optimized form. Adopting such an approach would require that FEMA employ a scenario-based risk assessment process to guide its efforts, whether that is a "maximum of maximums" approach or something more like the National Planning Scenarios. The Homeland Threat and Risk Analysis Center (HITRAC) and the Office of Risk Management and Analysis (RMA), both within

(Continued on Page 14)

2. Presidential Policy Directive/PPD-8, (March 30, 2011).
3. Implementation Plan for Presidential Policy Directive 8: National Preparedness, (May, 2011).
4. Herb Jackson, "U.S. House OKs Homeland Security Bill with Cuts," Northjersey.com, (June 3, 2011).
5. Aderholt Statement on FY 2012 Homeland Security Appropriations Act, (May 13, 2011).

Grants *(Cont. from 13)*

DHS's National Protection and Programs Directorate (NPPD), have the capability to assist with providing a national perspective on risk (something the Department is directed to do anyway as part of the implementation of PPD-8). The United States Coast Guard (USCG), Transportation Security Administration (TSA), and Sector Specific Agency Executive Management Office (SSA EMO) could also inform this discussion and help with coordination. Ultimately, and with appropriate technical assistance, this national perspective on risk could be complemented with State and regional inputs, possibly leveraging the DHS-supported fusion centers and existing methodologies like the Maritime Security Risk Analysis Model (MSRAM), Terrorism Risk Assessment Methodology (TRAM), and FEMA's own HAZUS-MH tool.

With a risk baseline established, many elements of FEMA's current grant process could then be aligned to support this approach:

- The Target Capabilities List (TCL), or a successor, could provide the means for identifying gaps between existing capabilities and required capabilities;

- Strategic planning efforts, such as the State Hazard Mitigation Plans, State/Urban Area Homeland Security Strategies, Regional Transit Security Strategies (RTSS), and Port-Wide Risk Management Plans (PWRMP), could provide the mechanism for addressing the identified capability gaps through defined goals, objectives and implementation steps; and

- The C2C initiative, or a successor, could serve as an investment optimization tool in support of the grant application process.

Implementing this approach as a collaboration between FEMA and its State, local, and private sector partners could in turn allow for new efficiencies in the grant application and reporting process. For example, the ability to fund standardized and approved plans, backed by rigorous monitoring and exercise programs, should provide the confidence needed to eliminate such costly and burdensome requirements as the IJ and BSIR.

In addition to these efficiencies, stakeholders at all levels of the process would benefit from the ability to apply common, repeatable, and transparent metrics. One such measurement enabled by use of this new risk management construct would be the ability to gauge program impact as a function of risk reduction and risk reduction return on investment. Adopting such an outcomes-based approach would:

- Help ensure that the focus remains on building capabilities where they are needed;

- Allow states and localities to prioritize investments more effectively by understanding how much risk reduction could be achieved through investment in a particular capability; and

- Provide Federal officials with the basis for measuring and articulating the overall effectiveness of the grants on reducing risk to the Nation.

The effectiveness of these investments could also be further tested through the Homeland Security Exercise and Evaluation Program (HSEEP). HSEEP-compliant exercises would provide additional confidence that the solutions implemented were in fact having their intended impact. Coupled with effective programmatic monitoring, this feedback would also support the iterative application of successive grant rounds to ensure that these funds continued to: 1) target the most pressing risks; and 2) do so in the most efficient and effective manner possible.

Potential Challenges

There are a number of potential challenges to the successful implementation of any new approach in this arena. These include:

- **Visibility:** Since their inception in 1998, these grant programs have benefited every State and territory, most major urban areas, and even many privately owned and/or operated facilities. Their intended purpose —to enhance the Nation's preparedness for large scale terrorist attacks and natural disasters — coupled with the enormous amount of taxpayer funding involved, also contributes to a heightened level of interest and raised expectations at all levels (e.g., H.R. 3980, the Redundancy Elimination and Enhanced Performance for

(Continued on Page 28)

Resilience Engineering: An Emerging Area in Critical Infrastructure

by Nii Attoh-Okine,
Department of Civil and Environmental Engineering, University of Delaware

Introduction

Resilience Engineering is becoming a new paradigm for complex systems performance and maintenance decision-making. The concept of resilience was introduced by Holling[1] in the field of ecology and has been well documented in ecological, social, and in some management cases. The initial definition of resilience is that which determines the persistence of relationships within a system and is a measure of the ability of these systems to absorb change state variable, driving variables and parameters, and still persist. It is the potential of a particular configuration of a system to maintain its structure/function in the face of disturbance, the ability of the system to re-organize following disturbance-driven change, and measure by size of stability domain. It is also the capacity of a system to absorb disturbance and re-organize while undergoing change so as to still retain essentially the same function, structure, identity, and feedbacks. The concept of resilience and its applicability to ecological, social, and business systems compare to engineered systems.

Unfortunately, the application in engineered systems and energy systems is lacking. Resilience Engineering represents a major step forward by proposing a completely new vocabulary, adding one more concept to existing lexicon. Although various definitions of resilience exist, they are dependent on the subject area. Resilience in infrastructure systems is the ability of the system to recover and adapt to external shocks, natural, and artificial technogenic disasters, and failure due to poor design. This ultimately affects the smooth and efficient operation of systems and may demand a shift of process, strategy, and coordination. Infrastructure systems in most cases are interconnected. Thus, the analyses of the system should consider interdependency properties. Dependencies and interdependencies have various effects: cascading effect — when disruption in one infrastructure causes disruption in a second; escalating effect — when disruption in one infrastructure exacerbates an independent disruption of a second infrastructure; and common cause effect — when a disruption of two or more infrastructure occur at the same time. Therefore, it is nearly impossible to analyze the behavior of any infrastructure in isolation.

The basic elements of infrastructure are vulnerable to physical and natural disruption as well as technogenic disasters. The many interrelationships among the infrastructure call for analyses in which various system components are interrelated and for management strategies that allow easy adjustment as more information and data becomes available. The interdependent infrastructure systems share many different characteristics, including but not limited to the following: they are large-scale dynamic, non linear, spatially distributed "system of systems" with various components; they are administered by different agencies with different objectives; they have multiple decision-makers; and sometimes conflicting and competing objectives. Given the general characteristics of these infrastructure systems, each has a unique field of research. The traits of "system of systems" include systems which follow different deterioration patterns, hence different monitoring and maintenance policies.

A critical model of infrastructure dependencies has to address both level and interconnectedness. In most cases, some of the analyses and the methods coincided at various levels. One notable characteristic of

(Continued on Page 16)

1. C.S. Hollings, "Resilience and Stability of Ecological Systems," *Annual Review of Ecology and Systematics*, Vol 4, (1973), 1-24.

Resilience Engineering *(Cont. from 15)*

the hierarchy is that at the top level, socioeconomic, gaming, and scenario techniques are used and at the lower level, more experienced and technical simulation are used. The challenge now is to develop resilience indices that can be used within the "system of systems" framework, given the complexity and some properties of interdependencies of different infrastructure. The resilience indices should be capable of analyzing the resilience of the overall system.

Concepts of Resilience

The concept of resilience has emerged as a characteristic of complex, dynamic systems in a range of disciplines including ecology, economics, and environmental studies. As previously mentioned, the concept of resilience was introduced by Holling in ecology.[2] Holling stated that resilience determines the persistence of relationships within systems and is a measure of the ability of these systems to absorb change of state variable, driving variables and parameters, and still persist. Although there are different definitions, this article will include only a few. These are: a) resilience is the capacity to cope with unanticipated dangers after they have manifested or learning to bounce back; b) the potential for a system to maintain its structure and form in the presence of external events; and c) a series of characteristics, presented by Godschalk, of resilient systems that include:

- **Redundancy**: Systems designed to ensure that failure of a particular node or section will not affect the entire system;
- **Diversity**: Multiple component or nodes against a specific threat;
- **Efficiency**: Positive ration or energy supplied to energy delivered;
- **Capability:** operate independent of outside control;
- **Strength**: Power to resist external events;
- **Interdependence**: Integrated system component to support each other; and
- **Adaptability**: Capacity to learn from experience and flexibility to change.[3]

This model of resilience as a way to cope with uncertainty can have different meanings depending on the system under consideration. These include:

- **Ecological Resilience**: Rate at which a system returns to a single steady or cyclic state following a perturbation;
- **Economics and Business Resilience**: Ability of a local company to retain function, employment, and production in the face of shock both in funds and in personnel;
- **Industrial and Organizational Resilience**: Ability of industry/ organizations to strengthen creation of robust flexible processes in proactive fashion;
- **Network Resilience**: Ability of a network to provide an acceptable level of service in the face of faults and challenges to normal operations;
- **Psychological Resilience**: The capacity of people to cope with stress and catastrophe; and
- **Sociological Resilience**: A function of investments in natural, human, social, and physical capital.[4]

Brand and Jax[5] reinforce the importance of resilience in the context of achieving sustainability and also reviewed variety of definitions for resilience within the context of sustainability science. Their definitions are based on the degree of normativity. The authors divided the definition into three broad concepts: a) Descriptive Concept; b) Hybrid Concept; and c) Normative Concept. Ecological and social science form the Descriptive Concept. The Hybrid Concept is made up of ecosystem — services and socio-ecological system. Finally, the normative concept is made up metaphoric and sustainability-related. The sustainability- related, which defines maintenance of natural capital in the long run, appears to be suitable for infrastructure systems.

The concept has been used in conjunction with vulnerability and adaptation. There is an intuitive

(Continued on Page 17)

2. Ibid.
3. D.R. Godschalk, "Urban Hazard Mitigation: Creating Resilient Cities," *Natural Hazards Review,* 4(3), (2003), 136-143.
4. A. Madni and S. Jackson, *Toward a Conceptual Framework for Resilience, paper submitted to IEEE System Journal* (2008).
5. F. Brand and K. Jax, "Focusing the Meaning of Resilience: Resilience as a Descriptive Concept and a Boundary Object," *Ecology and Society*, 12(1), (2007).

Resilience Engineering *(Cont. from 16)*

similarity between the fields of risk assessment and resilience concepts. Conceptual developments as presented can be extended to general infrastructure systems.[6] The authors summarized and compared the approaches used in risk management and resilience theory. The authors presented the following comparison shown in Table 1.

The authors highlighted that a combined risk and resilience approach has the potential to:

- Overcome the gaps of incomplete prediction and lack of comprehensiveness in risk an assessment approach;
- Improve anticipation of system failure and the ability to respond in an adaptive way;
- Provide a method of evaluating response to unforeseen impacts and disturbances;
- Respond in such way that the resilience of the system is not diminished; and
- Extend the range of responses to allow consideration of alternative, stable system states.[7]

The concept of vulnerability has been a powerful analytical tool and methodology for describing states of susceptibility to harm both physical and social systems and for guiding and developing a framework of normative analysis of actions to enhance the reduction of risk.[8] The concept has its roots in the study of natural hazards and in some cases means susceptibility to harm. From system perspectives, these are some of the ways of evaluating vulnerability:

- Identifying things that actually make individuals, communities, or organizations work on a day-to-day basis;
- Assessing the inherent vulnerability of all these elements;
- Assessing how the interaction of these elements affects their vulnerability; and
- Finding ways of enhancing their ability to cope with crisis situation.[9]

Adaptive capacity or adapting is the ability of a system to respond to changes in its external environment and also the ability to recover from natural and artificial disaster. There have been various definitions with and without strong relationship to resilience. Since different systems differ in their resilience characteristics, the explicit incorporation of differential resilience is a very critical element

(Continued on Page 18)

Risk Management	Resilience
Operational planning and practice	Theory-validation and quantification
Deconstructionist approach	Holistic approach
Clearly defined objectives and measures	Overall measure of sustainability
Likelihood of failure and magnitude	Position adaptive cycle and threshold
Internal causation	External causation
Expected Perturbations	Unexpected perturbation
Failure-man-made thresholds	Collapse breaking point threshold
Laws of science and engineering	Complex systems and stable state
Fast to medium variable	Both fast and slow variables
Adjust performance to avoid collapse	Accepts inevitability of collapse
Encourage maintenance of the known	Multiple stable basin acceptable
Failure triggers corrective action	Collapse is followed by natural reorganization

Table 1: Comparison between Risk Management and Resilience.

6. J.M. Blackmore and R.A. Plant, "Risk and Resilience to Enhance Sustainability with Application to Urban Water Systems," *Journal of Water Resources Planning and Management,* 134(3), (May 1, 2008), 224-233.
7. Ibid.
8. W.N. Adger, "Vulnerability," Global Environmental Change, 16, (2006), 268-281.
9. E.P. Dalziell and S.T. McManus, *Resilience, Vulnerability and Adaptive Capacity: Implications for System Performance*, paper presented at the International Forum for Engineering Decision Making, (2006).

Resilience Engineering *(Cont. from 17)*

of analysis in human-environment systems. Various definitions of resilience entail both strength, which is the ability to withstand external shock, and flexibility, which is the ability to bounce back.[10] Resilience, especially in hazards and disaster literature, is considered as a systematic quality that reflects not only inherent vulnerability and capacity but also decisions and actions. Resilience is a difficult and multidimensional concept that cannot be adequately assessed using a single measure. A framework for measuring resilience based on rapidity, redundancy, and resourcefulness has been presented.[11] For example, a new terminology, "hydropolitical resilience," is defined as the complex human-environmental systems' ability to adapt to permutations and change within these systems and "hydro- political vulnerability" is defined by the risk of political dispute over shared water systems.[12]

Resilience Engineering

Resilience Engineering is emerging as a new concept based on the work edited by Hollnagel, et. al.[13] The initial concept was more towards human errors and machine failures — safety of critical systems involving humans. In the engineering sense, resilience has been referred to as the art of managing the unexpected, or how teams or organizations become prepared to cope with surprises. Also, resilience is the parameter of a system that captures how well the system can adapt in the presence of surprising events. These surprising events can sometimes push the system beyond its boundary condition and operational boundaries.[14] Therefore the purpose of Resilience Engineering is to anticipate the changing potential for failure considering that plans and procedures have limits, gap and unforeseen errors, and the environment is very dynamic.[15]

Sheridan presented some ways necessary to maintain a resilient system:

- Emphasis on anticipating future possible incidents and on what actions were mitigating of negative consequences and aided recovery for past incidents; and
- Monitoring and measurement of states variables.[16]

Resilience Engineering is based on the following premises,

- Performance conditions in most cases underspecified with lots of uncertainty and vague information;
- The interactions of performance variability of a system;
- Safety management is more than error tabulations and calculation of failure probabilities; and
- Safety should be part of the function of the systems and should be achieved by improvements rather than constraints.[17]

The major focus therefore is a set of outcomes for situations that go wrong and right and the aim is not only a preventative measure but also guarantee that the system functions right.

Concluding Remarks

Current resilient infrastructure systems, particularly electric power, water, and health care are crucial for minimizing the effect of extreme events on society. Any infrastructure that can withstand external shocks will have minimum impact on

(Continued on Page 27)

10. T. McDaniels, S. Chang, D. Cole, J. Mikawoz, and H. Longstaff, "Fostering Resilience to Extreme Events Within Infrastructure Systems: Characterizing Decision Contexts for Mitigation," *Global Environmental Change*, 18, (2008), 310-318.
11. M. Bruneau, S.E. Chang, R.T. Eguchi, G.C. Lee, T.D. O' Rourke, A.M. Reinhor, M. Shoozuka, K. Tierney, W. Wallace, and D. von winterfeldt, "A Framework to Quantitatively Assess and Enhance the Seismic Resilience of Communities," *Earthquake Spectra*, 19(4), (2003), pp 733-752.
12. A. McNally, D. Magee, and A.T. Wolf, "Hydropower and Sustainability: Resilience and Vulnerability in China's Powersheds," *Journal of Environmental Management*, 90, (2009), S286- S293.
13. E. Hollnagel, D.D. Woods, and N. Levenson, *Resilience Engineering: Concepts and Precepts,* Burlington, VT Ashgate Publishers, (2006).
14. D.D. Woods, "Resilience Engineering: Redefining the Culture of Safety and Risk Management," Bulletin, *Human Factors and Ergonomics Safety,* 49(12), (2006).
15. E. Hollnagel, D.D. Woods, and N. Levenson. *Resilience Engineering: Concepts and Precepts,* 2006, Burlington, VT Ashgate Publishers.
16. T. B. Sheridan, "Risk, Human Error and System Resilience: Fundamental Ideas," *Human Factors*, Vol 50, No. 3, (June 2008), 418-426.
17. J. Leonhardt, E. Hollnagel, L. Macchi, and B. Kirwan, "A White Paper on Resilience Engineering for ATM," European Organization for the Safety of Air Navigation (9EUROCONTROL), (September 2009).

Anxiety of Decision, Fear of the Future, Perception of Risk, and What Lies Ahead for Critical Infrastructure Protection

by Alessandro Lazari and David Ward

Risk, decision-making, the fear for the future, and the relative premises behind them date back to ancient times. Moreover, risk is part of the human life cycle, and throughout history the features behind it have not only characterized its essence and determined its visibility but also its perception, real or otherwise. From the early days of the naval transport of goods to the modern days of critical information infrastructures, theorists and experts have formulated diverse, different, and numerous approaches to risk management and acceptability. But it has taken a tragedy like that of 9/11 to really accelerate and focus this process and provide the research field of risk with a quantum leap in knowledge and understanding. Yet despite these efforts one other thing appears to be missing and that is the study of the proper interaction between the human being and those same technologies, processes, and standards that are at the heart of many modern critical infrastructures and the services they provide. This short technical note takes a brief look at the evolution of risk perception with the intent to give a human-in-the-loop perspective on what lies ahead for critical infrastructure protection (CIP) and risk management.

Introduction

The studies on risk, in the past as well as of today, attempt to analyze and properly address a universal issue that is rooted in the history of humanity. Undeniably risk, also described as society's answer to the future,[1] made its first appearance in early naval transportation, i.e., in the trading and the export of goods of various kinds.[2]

Exploring the evolution of human interaction with risk and the variables affecting its perception and acceptance brings to mind some keywords and concepts suggested by the German sociologist Niklas Luhmann.[3] He described the risks and decision-making in early naval transport using words such as danger, audacity, chance, involvement, luck, courage, fear, and adventure. These descriptors reflected the interaction between the actors (e.g., seamen), their attitudes, and risk. Attitudes such as courage, audacity, and fear were typical of both the captain and crew when maneuvering their vessel through dangerous waters, tight canals, shallow ports, etc.

Modern vessels and seafarers are now in a completely different state-of-play and playing space because technologies and innovations have been deliberately introduced to drastically reduce risk, examples being GPS, autopilots, weather stations, E.P.I.R.B., etc.[4] In essence, modern society has transferred routine and risky activities from man to machine, where "machine" now also includes computers, networks of computers, and their control.[5] However, this transfer not only mitigates but also shifts risk. Indeed, it is wise to consider the pros and cons of the introduction and use of technologies just as the "old seadog" intimately considered all options before putting his vessel, crew, and cargo at risk no matter what the sea conditions were before maneuvering.

Indeed, experience teaches us that reducing human intervention does not necessarily avoid the need for

(Continued on Page 20)

1. Niklas Luhmann, "*Soziologie des Risikos*," Walter de Gruyter & Co., Berlin, (1991).
2. The attempt to mitigate risk in maritime transportation essentially shaped and initiated the conditions for the emergence of the insurance companies.
3. Idem.
4. EPIRB: Emergency Position-Indicating Radio Beacon.
5. Such as SCADA: Supervisory Control and Data Acquisition.

Prospects *(Cont. from 19)*

risk management or CIP related decisions because there will always be a human-in-the-loop, as an actor or potential victim.

Moreover, the development of more complex and integrated critical infrastructures spurs a new kind of human interaction and intervention because in the event of disruption, failure, or destruction, these can provoke vast economic and public effects. So in spite of our efforts, the anxiety of decision, fear of the future, perception of risk, and what lies ahead for critical infrastructure protection and humanity is still very much present. In fact, some would argue that risks have escalated and not the opposite.

Perhaps the awakening for humanity in this sense came with the 9/11 tragedy and has subsequently been reiterated of late with the Fukushima incident. September 11th proved to be a landmark for CIP awareness, so much so that the scientific community, the political powers, and all the industrialized and emerging countries decided that it was time to work together without borders and frontiers at the back of their agenda and minds. It was no longer about machines: it was about man and society in general.

Just two months after the 9/11 tragedy, key European states, together with some non-European national representatives, gathered in Budapest on the 23rd of November 2001. Their goal was to break away from the previous stalemate and slow routine process of discussing critical infrastructure protection to push it into a completely new playing space, especially with regards to cyber crime and large scale attacks on critical infrastructures. Budapest provided a perfect example of what can be achieved when states are put under pressure and pushed by the general public to "deliver the goods."

However, over the last decade, the same actors have produced wagon loads of legislation, introduced, and summoned for new and better industrial standards, security certification and labeling, multiplied rule-making measures, procedures, protocols, etc. But, it is time to see the effects on supposedly improved CIP and the new risks incurred. Ten years after 9/11, the impression is that in spite of all the efforts made, the state-of-play of CIP is at best foggy, with more perceived risk and essentially aggressively "therapized"[6] infrastructures. Moreover, the human side has been relegated to operations management, surveillance, and the technocratic governance and conduction of CIP.

There is a multitude of diverse and different CIP schools of thought (from all threats to all hazards, from prevention to preparedness, etc.). Furthermore, this has probably been fueled by the differences in the cultural, historical, environmental, experiential, expertise, political, and legislative backgrounds between the actors and stakeholders (private and public, individual or society), especially when it comes to defining "critical infrastructure" and adding the "protection." The end result is that the perception of risk by the general public is both augmented and foggy.

We are also witnessing the cross fertilization of legal and social factors among states and their citizens. This process will influence the decisions made today as well as their acceptance, deployment, and effects on society and humanity in the future. Some repercussions include: EU Directive 114/08/EC (with the identification and designation of European critical infrastructure); the over-kill or implications of integrated societal assets (such as air traffic security); the multiplication of new layers of CIP responsibilities (from national to EU legislation); new bilateral and multilateral critical infrastructure pacts/agreements and the new concept of resilience; the arrival of new waves of technological innovation (e.g., body scanners) and their impact on CIP. The prospect is therefore already here. It is most likely to stay until the "mist clears" and thins-out risk instead of eliminating it.

This situation is captured in the theory that Luhmann explained in his "soziologie des risikos," when talking about decisions taken to avoid risks that could lead to many other unknown and/or unperceived equivalents. He theorized that an important element in risk studies, especially in terms of decision-

(Continued on Page 29)

6. Therapized implies the insistence of using a therapy which defeats or depletes the scope of the therapy in the first place: therapy is also seen as one or more CIP actions.

An End to Terrorism Risk Insurance Regulation?

by Alexia Brunet Marks, Associate Professor of Law,
University of Colorado Law School, Boulder, CO

Scholarly debates over the September 11th attacks focus predominantly on high-profile issues, such as torture, preventative detention, interrogation, privacy, and surveillance. These debates have overshadowed the equally important and far-reaching issue of terrorism risk insurance, which not only involves billions of dollars, but provides powerful incentives to keep us safe. The Terrorism Risk Insurance Act of 2002 (TRIA),[1] was passed following 9/11 and has been renewed twice through the Terrorism Risk Insurance Extension Act, (TRIEA),[2] and the Terrorism Risk Insurance Program Reauthorization Act (TRIPRA).[3] TRIPRA, the final piece in the trilogy of terrorism risk insurance regulation, is set to expire on December 31, 2014, unless reauthorized by Congress. To be sure, regulation set in place after 9/11 balances the financial responsibility for terrorist events between Federal and State governments, and insurers and policyholders, thereby setting an example of how this Nation strikes a balance between private and public responsibility for terrorism. However, the regulatory framework that is in place is far from perfect. What will happen next? Will the Federal government withdraw from this market altogether? Should it? We are three years from the TRIA's sunset and yet discussions on TRIA's fate are starting to heat up.

As fiscal conservatives in Washington and the Obama Administration have been trying to scale back support for the Federal program, the threat of terrorism remains very current and real. Reform efforts have ranged from the predictable — a proposed budgetary decrease for the program[4] — to the unpredictable — an early sunset provision for TRIA in a proposed amendment to the legislation reauthorizing the National Flood Insurance Program.[5] Meanwhile, according to a 2011 Pew Center public survey, terrorism continues to be a top public priority in the United States since 9/11, ranking third among the priorities surveyed as it has for a few years.[6] These survey results do not even account for the under-publicized reality that at least a dozen attacks have been planned, and to some degree carried out against the United States since 9/11. In fact, the nine years since 9/11 have been the most active period in terrorism history.

Discussions on the fate of TRIA will invariably focus on the arguments that led to the original passage of TRIA — whether the market for terrorism risk insurance is sound, healthy, and sustainable without regulation. While the market has improved, it still requires regulation — although arguably not exactly the type of regulation that was agreed upon initially.

A Market for Terrorism Risk Insurance

Developing a sound understanding of the market for terrorism risk insurance is essential to guiding the difficult determination of the appropriate balance between private and public responsibility for preventing and (when necessary) compensating for terrorism.

(Continued on Page 22)

1. The Terrorism Risk Insurance Act of 2002, Pub. L. No. 107-297, 116 Stat. 2322 (2002) ("TRIA").
2. Terrorism Risk Insurance Extension Act of 2005, Pub. L. No. 109-144, 119 Stat. 2660 (2005) ("TRIEA").
3. Terrorism Risk Insurance Program Reauthorization Act of 2007, Pub. L. No. 110-160, 121 Stat. 1839 (2007) ("TRIPRA").
4. *See* U.S. Office of Management and Budget, *Terminations, Reductions, and Savings, Budget of the U.S. Government, Fiscal Year 2010*, available at: http://www.gpoaccess.gov/usbudget/fy10/pdf/trs.pdf, (however, evidence shows that there is little appetite for these changes to be enacted by Congress).
5. *See* Arthur D. Postal, *Wicker Withdraws TRIA-Repeal Amendment Today, But Asks for Future Discussions*, available at: http://www.propertycasualty360.com/2011/09/08/wicker-withdraws-tria-repeal-amendment-today-but-a.
6. Pew Research Center for the People and the Press, *Less Optimism about America's Long-Term Prospects*, (January, 2011), 1, available at: http://people-press.org/files/legacy-pdf/696.pdf.

Risk Insurance *(Cont. from 21)*

What is the market for terrorism risk insurance, what is TRIA, and how could this seldom-discussed type of coverage found in all commercial property and casualty insurance have sparked three rounds of Federal regulation, a Federal Commission, and countless hearings on the Hill? In brief, TRIA is a Federal reinsurance program that is triggered when losses from an act of terrorism exceed 20 percent of an insurance company's earned property and casualty premiums, with an industry cap of $27.5 billion. In such a scenario, the government would pay 85 percent of these losses, up to $100 billion a year, while insurance companies would pay 15 percent, in addition to their 20 percent retention.

At the time TRIA was passed, discussion focused on the insurance industry's ability to sustain a market for terrorism risk insurance. The attacks of 9/11 represented one of the costliest insurance events in American history, amounting to insured losses of some $32 billion in today's dollars. The insurance picture looked bleak. The serious shortage of capital against terrorism meant that for insurers to sell their clients the same level of coverage they offered pre- 9/11, they had to locate other sources of funding. In the days that followed, insurers sought exclusions and limited coverage, making it difficult for commercial policyholders to purchase even basic terrorism coverage. The insurance crisis in turn fueled debate on whether the Federal government should regulate the market for terrorism risk insurance. Congress reacted by passing three pieces of legislation over seven years to address the insurance crisis, all aiming to increase the availability and affordability of coverage for property and casualty commercial policyholders and stabilize insurance markets.

TRIA has been a success story on many fronts. TRIA has increased availability and affordability of coverage for terrorism risk insurance. Even still, it has not cost the government a dime and will not so long as there is not a major terrorist attack in the country. Even if an event does occur, TRIA has a specific cost-sharing approach for the first $100 billion of annual losses by businesses due to terrorist attacks, explicitly leaving it to Congress to make additional choices were an attack to cost even more. A recoupment provision instructs policyholders to repay taxpayers for any funds advanced. The success story does not need to be overstated, as several imperfections continue to exist in the market.

Continued – Though Modified – Regulation

In a paper published earlier this year, the author argues for a continuation of the public-private partnership created post-9/11, with substantive changes to the current regulatory framework. The author argues for a continued Federal role in regulating terrorism risk insurance based on market failure and national security reasoning. First, the insurance market contains imperfections. It still does not have the capacity to absorb an event in the magnitude of 9/11 or greater (such as a nuclear, biological, or chemical attack which may cause damage ranging in the hundreds of billions of dollars) and it still does not have the ability to predict future terrorist events with any accuracy (in this way, terrorist attacks are unlike hurricanes and earthquakes). Next, the Federal government is responsible for ensuring that there are no gaps in coverage, particularly in target-rich environments, like lower Manhattan, for example. Yet changes need to be made to address the moral hazard problem that regulation creates. What is the moral hazard problem?

While TRIA has helped to decrease prices and widen coverage, regulation that interferes with pricing inevitably affects policy-holder incentives to take precautions to avoid or limit loss — the familiar problem of moral hazard. Now that policyholders are able to purchase insurance at subsidized rates, there is no incentive to mitigate risk on their own. The roadmap presented aims to solve the moral hazard dilemma identified above, while delineating the proper boundaries of Federal regulation.[7] The enormous challenges presented by the risk of

(Continued on Page 30)

[7] *See* Alexia Brunet Marks, "Under Attack: Terrorism Risk Insurance Regulation," *North Carolina Law Review*, 89(2), (2011), also available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1588929.

Legal Insights

Legal Risk Management Promotes Critical Infrastructure Resilience

by Gregory J.M. Parry, JD, MPS, Director*
Eagle Risk Management Law Firm, PLLC

Introduction

Law schools use the Socratic Method to teach how to "think like a lawyer." In essence, students learn how to "react like a lawyer." The reactive paradigm is honed by digesting given facts, framing the legal issue; citing applicable laws; blending the facts and law; and reaching a logical conclusion. Recent disasters and threats motivated governmental and business leaders to think proactively. Contemporary lawyers must meet market needs. They must expand "thinking like a lawyer" to a more proactive, prevention focused, risk based mindset. Legal Risk Managers add a key player to the risk management team. They apply legal, economic, social, and enterprise knowledge to identify legal risks and offer counsel on preventing, mitigating, or tolerating risks. Legal futurist, Richard Susskind, underscored the need for, and dearth of, legal risk managers. In his book entitled, *The End of Lawyers? Rethinking the Nature of Legal Services*, Susskind summarized his exhaustive research:

This category of lawyer is sorely needed and is long overdue. Senior in-house lawyers around the world insist that they are in the business of legal risk management — clients prefer avoiding problems rather than resolving them. And yet hardly a lawyer or law firm on the planet has chosen to develop tools, methods, techniques or systems to help clients review, identify, quantify and control legal risk they face. I expect that to change.

The Evolution of Risk Management

9/11 and Hurricane Katrina elevated the topics of prudent disaster/emergency and business continuity planning to board room status. Post 9/11 and Katrina, dozens of political, corporate, and accounting scandals unfolded, elevating compliance and governance risks to the boardroom. Based upon the collective effect of these events, a new seat for Chief Risk Officers was permanently added to boardrooms nationwide.

9/11 inspired political, regulatory, and corporate reforms. President Bush and Congress identified, and focused on, protecting 18 critical infrastructure sectors. Most agree "it's not if but when" the next terrorist attack will occur. The frequency and magnitude of accidental disasters will continue rising in correlation to technology advancements. Natural disasters are certain to occur. Therefore critical infrastructure sectors must undertake lawful disaster/emergency and business continuity planning, and implementing acceptable security programs. The balanced goal is resilience.

Legal Risk Managers (LRMs) foster resilience. LRMs assist critical infrastructure sectors with staying abreast of, and navigating, Federal/State legislative, executive, administrative, and judicial mandates; industry best practices; and compliance and governance duties.

Critical Infrastructure Director and Officer Liability Risks

Director and Officer (D/O) powers and duties are defined in organization bylaws. By law, D/Os owe a fiduciary duty including unbending trust, good faith, confidence, and loyalty. They foster the organization's lawful objectives. To the legal risk side they oversee compliance, follow accepted governance practices, and resilience protocols. D/Os who breach their duties open the company and themselves to liability. This article

(Continued on Page 24)

Legal Insights *(Cont. from 23)*

begins with new legal concerns pertinent to critical infrastructure protection, followed by sample mitigation tools.

Sample Critical Infrastructure Sector Specific Laws

Over 65,000 chemical facilities dot the Nation. The Chemical Facility Anti Terrorism Standards (CFATS) screen, and regulate, high risk facilities. High risk facilities must perform a vulnerability assessment, design a site security plan, and institute risk-based controls. Violations may lead to administrative, civil, and criminal penalties. LRMs may aid with compliance or operational protocols to avoid CFATS.

Following 9/11, the government swiftly moved to block terrorist funding sources. Through existing, and new, anti-money laundering (AML) laws, the Treasury Department's Financial Crimes Enforcement Network, and Office of Foreign Asset Control, was charged with investigating/blocking "property and interests in property" connected to terrorism. Lenders must implement screening protocols, and if verified, refuse/nullify funding. LRMs can assist with drafting policies, unraveling corporate structures, counsel on compliance, and educate directors/officers on AML laws.

Foreigners investing in U.S. entities that provide goods or services with links to national security may ask for approval from the Committee on Foreign Investment in the United States. The Committee, however, may unilaterally review transactions. Disapproved pending investments may be blocked, and if closed, unwound. LRMs may assist with structuring a given transaction and presenting it for Committee review and approval.

The events of 9/11 and Katrina legitimized the return on investment in disaster/emergency and continuity planning (DCP). The 9/11 Commission found the critical infrastructure sectors "largely unprepared." It recommended a voluntary national standard for preparedness. Congress enacted legislation to establish a voluntary "all hazard" standard. DHS approved 3 standards (NFPA-1600; SPC-1-2009; and BS-25999-2:2007). Applying principles of common law negligence, new theories of liability have arisen for failure to plan; negligent plan; and negligent implementation of plan. Recent litigation and legal articles embrace these theories. The author recommends that boards view DCP as legally mandatory. In addition, under Federal and State civil right laws planning, response and recovery, and continuity plans must accommodate people with disabilities. LRMs can counsel directors on the legal risks of failed planning; assist with contracting experts; review plans; counsel on legal risks before, during, and after disasters; and properly document legal compliance.

DHS Secretary Janet Napolitano recently declared that cybersecurity and home grown terrorism are priority threats. The author recommends critical infrastructure sectors consider adopting and implementing meaningful security mandatory. A full discussion of security mandates is beyond the scope of this article. Security plans include structures, cyber assets, employees, contractors, transportation, and links in the supply chain. LRMs can counsel directors on the legal risks of inadequate security; assist with contracting experts; review security plans; counsel the board on legal issues before, during, or after a breach; and document legal compliance with applicable authorities or best practices.

Sample Legal Risk Mitigation Tools

Human and natural disasters are inevitable. Depending upon the critical infrastructure sector and circumstances, LRMs can provide valuable counsel on proactive mitigation tools. Below is a sample list of critical infrastructure sector specific, and generally accepted, mitigation tools.

After 9/11, companies offering antiterrorism products, services, or software pulled out of the market fearing "bet the company" liability if their wares were implicated in a mass disaster. Congress enacted the Support Antiterrorism by Fostering Effective Technologies Act (SAFETY Act). SAFETY Act "designated" that companies were granted liability protections, e.g., lawsuits must be brought in Federal court; liability is capped at DHS-approved insurance coverage;

(Continued on Page 32)

CIRMEI *(Cont. from 2)*

release date and structure of the NRP so it will inform the outcomes and metrics used in the NAR. By linking risks identified in the NRP to our annual assessment and planning process, we will ensure that our efforts are truly risk informed.

Assessing the Impact of Activities through the National Annual Report

The second step is to assess the impact of protection and resilience activities. Traditionally, the NAR qualitatively described risk management activities and its structure changed from year to year. Going forward, the NAR will measure the effectiveness of critical infrastructure protection and resilience efforts by DHS and our critical infrastructure stakeholders through outcome statements and the metrics associated with each outcome. Moreover, one year's NRP will inform the metrics and outcomes of the following year's NAR.

The 2011 NAR — as well as those published in subsequent years — will contain a comprehensive analysis of the metrics data, describe the extent to which the desired outcomes are being achieved, and identify cross-cutting opportunities for improvement in critical infrastructure protection and resilience. The NAR, therefore, will enable NIPP partners to assess where they are in their risk management activities, adjust efforts and resource allocations to increase operational efficiency, and set priorities that are based upon risk and past performance.

Addressing Opportunities to Enhance Protection and Resilience through a Cross-Sector Plan

While understanding risk and measuring progress are essential, they are useful only to the extent that we utilize the knowledge acquired to take decisive action in our budgetary and programmatic activities. Such action will be possible through the development and use of the triennial Critical Infrastructure Risk Management Plan (CIRMP) — an action plan that will detail the short-term and long-term steps the NIPP partnership will take to address specific risks and opportunities highlighted in the NRP and the NAR.

The CIRMP will build on the opportunities identified in the NAR and detail the actions and milestones that will help DHS and its partners meet those opportunities. The collaboratively planned actions among the NIPP community, which are captured in the CIRMP, will inform resource planning so that funding can be directed toward actions that address identified improvement areas and risks to critical infrastructure. Successive NARs will demonstrate success of the CIRMP by measuring progress made toward the outcomes since the previous year. This final step will complete the robust feedback loop in which risks to critical infrastructure can be managed over time.

The Path Forward

DHS has already begun to align its programs and activities to the outcome statements included in the NAR. In the ongoing budgeting process, we are prioritizing those programs that most directly lead to the achievement of desired outcomes for critical infrastructure protection and resilience. The 2011 NAR will report on the achievement of these outcomes and will be submitted to Congress.

The benefits of the CIRMEI to the mission of critical infrastructure protection and resilience are evident — a clearly defined direction for critical infrastructure protection and resilience efforts, a path to get there, and a framework through which we can measure what has been accomplished and make risk-informed decisions in the future.

For more information about the U.S. Department of Homeland Security's critical infrastructure protection activities, please visit www.dhs.gov/criticalinfrastructure. ❖

Infrastructure Systems *(Cont. from 7)*

are the consequences?" (here we add, "what is the time frame?"), can be interdependent. Risk management policy options can reduce both the likelihood of a malevolent threat to a targeted system and the associated likelihood of consequences by changing the states (including both vulnerability and resilience) of the system. The quantification of risk to a vulnerable system from a specific threat must be built on a systemic and repeatable modeling process, by recognizing that the states of the system constitute an essential step to construct quantitative metrics of the consequences based on intelligence gathering, expert evidence, and other qualitative information. The fact that the states of all systems are functions of time (among other variables) makes the time frame pivotal in each component of the process of risk assessment, management, and communication. The risk to a system, caused by an initiating event (e.g., a threat), is a multidimensional function of the specific threat, its probability and time frame, the states of the system (representing vulnerability and resilience), and the probabilistic multidimensional consequences.

The Definition and Quantifying the Risk Function

In 1976, Lowrance,[3] offered the following definition: "risk is a measure of the probability and severity of adverse effects." One common method for the quantification of the risk function is through the product of the two terms in Lowrance's definition; namely, the probability and consequences. A logical question arises as to whether this definition is addressing the probability of the initiating event (e.g., a threat scenario), or the probability of consequences, or of both. Note that not all of the multidimensional consequences (e.g., fatality, monetary loss, business interruption, etc.), resulting from a specific initiating event (threat), would necessarily have the same probability. In other words, since the multidimensional vector of consequences is a function of the states of the system (thus of the vulnerability and resilience of the system), and a specific threat would not necessarily affect all states at the same level, then a specific probability ought to be associated with each element of the consequences. This fundamental premise has significant ramifications on the quantification of the risk function. ❖

3. W. Lowrance, *Of Acceptable Risk,* Los Altos, CA: William Kaufmann, (1976).

Preparedness *(Cont. from 11)*

4. The definition of Key Performance Indicators (KPIs) for all activities involved in order to better (more objectively) identify maturity levels, but also to offer better support to interested parties in the governance of risk management.

5. Wider use of the questionnaires within EU member states to determine strengths and weaknesses of NRM governance throughout the EU.

6. The possibility of implementing a programme of test scenarios in EU member states to investigate NRM preparedness more widely. ❖

Acknowledgements

The author would like to thank all members of the Working Group who contributed to this work, namely: Manuel de Barros, ANACOM, Portugal; Dr. Uwe Jendricke, BSI, Germany; Charalampos Koutsouris and Dr. Zoe Nivolianitou, NCSR, IIT, Greece; Drs. J.C. Oude Alink, Ministry of Economic Affairs, The Netherlands; Rytis Rainys, RRT, Lithuania; Prof. Ingrid Schaumueller-Bichl and Alexander Leitner, University of Applied Sciences, Hagenberg; Austria, Bjorn Scharin, pts, Swede; Pascal Steichen, CIRCL, Luxemburg; Paul Theron, Thales Group, France; Marco Fernandez-Gonzalez, Observer INFSO, European Commission. Many thanks also to Dr. Jeremy Ward and Dr. Guy Bunker, of ExecIA LLP for drafting the final report of the ENISA Working Group.

Resilience Engineering *(Cont. from 18)*

system interaction effects during cascade failure. The resilient systems aim to maintain a constant output value, performance, or a function without fundamentally changing the internal structure or behavior of the system. Networked and lifeline infrastructure appear to be the greatest challenges in the world, especially in the presence of surprise events. It is therefore paramount to have a sustainable and resilient infrastructure. Resilient systems can limit and reduce the probabilities of failures and consequences. Currently, the resilience engineering in networked infrastructure is more qualitative than quantitative, although there are few metrics for evaluation resilience in infrastructure systems considering their interdependencies. There are standards that define universal method of developing and analyzing the resilience indices of networked infrastructure. The challenge is to define more specific measures which are different from resilience computation in ecology or economic or social sciences. The approach needs to be a "system of system" concept. The formulation and analysis can then be used at both planning and design of critical infrastructure. The resilience indices and other related outputs of Resilience Engineering can be used to address more quantitatively the sustainability of the systems. ❖

Grants *(Cont. from 14)*

Preparedness Grants Act). An obvious danger here is having a less than ideal solution dictated. Effectively managing stakeholder relationships and expectations will also be essential to success.

• **Parochial Interests**: One of the reasons why these programs have developed into what they are today is that responsibility is shared among many agencies within DHS — each with its own often competing interests. To succeed in changing this paradigm, there must be unanimity of purpose within the Department.

• **Program Complexity**: Virtually every element of the current grant process has developed within its own unique stove-pipe. Aligning all of these elements will be a complex undertaking that will require patience, collaboration, and resources.

• **Program Focus**: While difficult for many of the reasons discussed, it is essential that a common and clear understanding of the purpose of these programs be developed. The reality is that these grants were established to assist State, tribal, and local government entities, as well as the owners and operators of critical infrastructure, acquire preparedness capabilities they did not previously possess and would not be likely to fund on their own outside of a shared commitment. In recent days, this has become intertwined with discussions about annual investments in routine law enforcement, fire, emergency medical, and emergency management capabilities. Refocusing on the original purpose of these programs, therefore, is also essential and would greatly facilitate the development of the necessary risk-based decision-making framework.

Conclusions

As recent Congressional action indicates, the inability of FEMA to quantify the impact of the preparedness grants has reached a point where it will dominate future discussions until addressed. Fortunately, many of the elements needed to address these concerns already exist. What is currently missing is the risk-based framework within which to have this discussion. By adding this element and realigning/optimizing other elements of its current preparedness programs, FEMA would possess the means to make risk-informed decisions about where and how to invest the available grant dollars, quantify program impact, and reduce the management and oversight burden placed on its staff and stakeholders. This will not be accomplished without strong leadership, a focused approach, and unanimity of purpose across the Department. However, without taking these steps, there is a strong likelihood that decisions will continue to be made that lack essential data — all at a time when the pressure is growing to find additional ways to cut the Federal budget. ❖

Kerry Thomas currently serves as President of the Security Analysis and Risk Management Association (SARMA) and is also Senior Director for Homeland Security Support Programs at ABS Consulting.

Prospects *(Cont. from 20)*

making, are the eventual risks that arise from not taking any decision[7] and the shift from man to machine to reduce risk. In other words, critical infrastructure protection still needs an anthropological perspective because of the centrality of the human being within even super modern critical infrastructures.

The introduction of state-of-the-art technologies reduces human error and has simplified or eliminated many of the routine tasks once assigned to man. But, this has also bred new and often grey areas where new and/or higher risk is lurking. Indeed, translating human control to human surveillance duties does provide more time for man to dedicate his/her intellect to higher level tasks but not necessarily does this improve CIP because it often remains unexploited.

Maybe it is premature to state that "we need to go back to basics" but the future of CIP does still hinge on humanity more than technology. Moreover, the temptation to promulgate too many laws, directives, and industrial standards in CIP is undermining the true human involvement of CIP. This is voiced by many critical infrastructure operators as being a good exercise but that is difficult or worse, impossible to apply in practice.

Accordingly, just as we witnessed for early naval transportation, the elements of human participation and involvement are vital for modern CIP risk reduction as well. As a matter of fact, after an "orgy of technology" in the field of informatics (for example) experts are realizing that security is one thing, but a trusted network is another. Yet, both need to work in tandem to obtain the envisaged "zero" risk and vulnerability in CIIP.[8] This very concept of trusted network hinges on the human-in-the-loop and not just the machine-in-the-loop. So whether we are exchanging machine control data between plant or between humans in a datawarehouse network, the emphasis should be on a more human oriented risk school of thought. In this way, not only will the CIP actors and stakeholders be more ready to implement the governance recently developed but will also help improve it with an anthropological and human-in-the-loop perspective.

The authors feel that this would provide a more stable and reliable perception of risk thus reducing anxiety of decision, fear of the future, and perception of risk and ensure that man and machine work together for the benefit of both, as well as society. ❖

Alessandro Lazari is a PhD Student, Faculty of Engineering - University of Florence, Department of Computer and Telecommunications Systems, Via S. Marta 3, 50139, Florence, Italy, alessandro.lazari@unifi.it.

David Ward, JRC-Ispra, IPSC, Security Technology Assessment Unit TP723, Via E. Fermi 2749, 21027 Ispra (VA), Italy

7. The disruption, failure or destruction of a critical infrastructure or asset is therefore mitigated or amplified depending on the quality of the decision and its timely execution.

8. CIIP: Critical Information Infrastructure Protection.

Risk Insurance *(Cont. from 22)*

terrorism can be addressed only through a coordinated, comprehensive system that melds ex-ante preventative and mitigation measures, insurance mechanisms, and ex-post compensation mechanisms into a national policy.

Solving the Moral Hazard Problem by Linking TRIA with the NIPP

Financial incentives used in the issuance of terrorism risk insurance and tied to compliance with Federal homeland security priorities can reduce our Nation's vulnerability to terrorism and reduce moral hazard. My solution is for policyholders to contract with their insurers to adopt and implement certain mitigation measures (security and emergency management policies) as a condition of receiving discounts on coverage, a practice referred to as "contracting-on-care." One frequent example of contracting on care is for insurance companies to contract with policyholders offering premium reductions conditional upon adoption of protective measures, a practice called "mitigation-based" pricing.[8] For example, there are many examples of mitigation based pricing in the context of personal automotive insurance and health insurance. This author argues for mitigation based pricing in the terrorism risk insurance context, based on adoption of protective measures from prescriptions outlined in national risk mitigation programs administered by the NIPP. This plan has the added benefit of potentially reducing the Federal role over time by increasing the purchase rate for terrorism coverage among businesses, by reducing the costs the Federal government would otherwise bear in the event of a catastrophic terrorist attack, and reducing our Nation's vulnerability to terrorism.

Conclusion

While the role of creating incentives for corporations to increase security and proactively plan for consequences of an attack — practicing risk mitigation — has been added to the list of future modifications to original TRIA,[9] my proposal provides one roadmap for accomplishing this objective. ❖

8. In addition to offering lower premiums, insurance companies could offer more favorable insurance policies, such as those that are longer term, have lower deductibles, or have less exclusion.
9. Comment by Reynold Becker, Vice President, Commercial Lines and Claims, Property Casualty Insurers Association of America, (2007).

Counter-Terrorism *(Cont. from 5)*

many bridges from time to time for maintenance or repair, and therefore traffic is redirected so that the network is not interrupted. Other failures routinely planned for include traffic accidents, severe weather, earthquakes, and equipment malfunctions. In other words, as a matter of course, infrastructure is designed with built-in redundancies and backup systems to ensure resilience in the event of anticipated or unexpected hazards.

There is also a displacement effect, a transfer of risk. Terrorists can choose, and change, their targets, depending on local and immediate circumstances. If the protection of one target merely causes the terrorist to seek out another from among the near-infinite set at hand, it is not clear how society has gained by expending effort and treasure to protect the first.

Relying on standard evaluative measures accepted for decades by analysts, governments, regulators, and risk managers, our analyses suggest, then, that bridges require no protective measures unless, perhaps, there is a very specific threat to them.[5] The same, it is likely, applies to many other individual items of infrastructure. ❖

For additional and wider-ranging assessments of the issues raised and the approaches used, see John Mueller and Mark G. Stewart, *Terror, Security, and Money: Balancing the Risks, Benefits, and Costs of Homeland Security*, New York and Oxford, UK: Oxford University Press, September 2011.

For more information, please contact the authors at:

Mark G. Stewart
Australian Research Council Professorial Fellow and Professor of Civil Engineering
Director, Centre for Infrastructure Performance and Reliability
The University of Newcastle, New South Wales, Australia
+61 2 49216027
mark.stewart@newcastle.edu.au
www.newcastle.edu.au/research-centre/cipar/staff/mark-stewart.html.

Professor Mark Stewart is Director of the Centre for Infrastructure Performance and Reliability at The University of Newcastle, and Professor John Mueller holds the Woody Hayes Chair of National Security Studies at Ohio State University. Their book, Terror, Security, and Money: Balancing the Risks, Benefits, and Costs of Homeland Security, has recently been published by Oxford University Press and will be available in Australia by October.

John Mueller
Professor and Woody Hayes Chair of National Security Studies
Mershon Center for International Security Studies and Department of Political Science Ohio State University, Columbus, Ohio 43201 USA
+1 614 247-6007
bbbb@osu.edu
polisci.osu.edu/faculty/jmueller

[5] It might also be noted that there seems to be little evidence terrorists have any particular desire to blow up a bridge, due in part, perhaps, to the facts that it is an exceedingly difficult task under the best of circumstances and that the number of casualties is likely to be much lower than for many other targets.

Legal Insights *(Cont. from 24)*

punitive damages and prejudgment interest is not permitted; recoveries are reduced by collateral sources; and actions may be filed only against the SAFETY Act designated seller (downstream buyers/users and upstream suppliers/ contractors may not be joined). The LRM can offer counsel on the liability mitigation benefits of the SAFETY Act, and if desired, usher the client through approval.

The LRM can draft, review, and negotiate contracts to allocate risks. For example, real estate agreements require antiterrorism provisions; supply chain agreements should undergo "what if" analysis to address potential interruptions; and cybersecurity outsourcing agreements should be tailored to protect the company. Regarding commercial contracts in general, LRMs can review and proficiently negotiate key provisions including definitions; warranties, representations, and covenants; survival rights; indemnification and hold harmless protection; confidentiality; alternative dispute resolution; force majeure; liquidated damages; and shortened periods of limitation.

Conclusion

The Socratic Method trains law students how to think and react like a lawyer. Recent disasters motivated government, businesses, and now legal leaders to think with a proactive, preventative, risk-based mindset. LRMs bolster the risk management team. LRMs are in short supply, however consistent with Susskind, this is certain to change. ❖

Gregory J.M. Parry, JD, MPS is the Managing Director of Eagle Risk Management Law Firm, PLLC located in Rochester, MI. Eagle Risk Management provides strategic legal risk management and compliance counsel to business clients. Mr. Parry is A-V Rated with 20 years experience. Mr. Parry graduated from Michigan State University College of Law, magna cum laude (1989), and Masters of Homeland Security Leadership, University of Connecticut - in partnership with U.S. Naval Postgraduate School (2009). Contact information: gparry@eagleriskslaw.com.

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