THE CIP REPORT

CENTER FOR INFRASTRUCTURE PROTECTION AND HOMELAND SECURITY

VOLUME 9 NUMBER 12

JUNE 2011

INTERNATIONAL

Global Interdependencies 2
Infrastructure Planning 5
Innovative Policies 8
Crisis Management 9
Developing Countries 10
Good Practices 13
Japanese Infrastructure 15
German Infrastructure 18
ISPs and Africa 21
Swiss Infrastructure 23
Nuclear Infrastructure 26
Legal Insights 27

Contact: dhardy1@gmu.edu
703.993.8591

In this month's issue of *The CIP Report*, we are pleased to present the annual issue on international critical infrastructure protection.

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

First, a distinguished CIP/HS fellow from Australia discusses global interdependencies. Three faculty members from the Delft University of Technology discuss solutions to planning for resilient infrastructure. A researcher from the Center for Security Studies at ETH (Swiss Federal Institute of Technology) Zurich analyzes policy innovations in critical infrastructure protection. A CIP/HS fellow from the Swedish Law and Informatics Research Institute at Stockholm University discusses BRIDGE, an international project to foster cooperation in crisis management. Next, two professors from the University of Johannesburg discuss a community-oriented approach to critical infrastructure protection in developing countries. An international research project on best practices in critical infrastructure protection, led by the Netherlands Organisation for Applied Scientific Research TNO, is then described. The impact of the Tohoku earthquake and tsunami on Japanese infrastructure is depicted by the American Society of Civil Engineers (ASCE) Tohoku Tsunami Reconnaissance Team Leader. Then, faculty from Karlsruhe Institute of Technology (KIT) at the Institute for Industrial Production (IIP) expound upon critical infrastructure protection in Germany. Two professors from the University of Johannesburg and the University of South Africa present an article on the potential role for Information Service Providers (ISPs) in Africa. The Swiss Programme on Critical Infrastructure Protection is expounded upon by the Head of Risk Analysis and Research Coordination at the Federal Department of Defence, Civil Protection and Sport in Switzerland. Finally, the effects of the Tohoku earthquake and tsunami on nuclear infrastructure in the United States are illustrated by an U.S. electrical engineer.

This month's *Legal Insights* assesses the recently released U.S. "International Strategy for Cyberspace."

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

Interdependencies for Resilience

by Rita Parker, ISSR, Australia
Distinguished Fellow, CIP/HS, George Mason University, Virginia
Visiting Fellow, Australian Defence Force Academy, University of New South Wales, Canberra

The significance of natural disruptive events in the 21st century has provided the impetus for public debate about how nations can increase resilience to non-traditional security threats. Historic and more recent disruptions highlight not only the force of nature but also the intersection of social, economic, and political systems which are, in turn, inter-linked to national security. While traditional security threats drive much of the policy debate, increasingly our attention is being drawn to non-traditional security threats.

The security and economic well-being of societies, and ultimately, that of nations relies on the provision of essential goods and services. These are, in many instances, dependent on so called non-essential goods and services which contribute to daily operations and sense of normality.

Non-traditional security threats require a different way of thinking as no two disruptive events are the same. Extremely rare disruptions challenge every precept, maxim, and formerly accepted doctrine of crisis as well as emergency management and security response. Similar to the inter-relationship of essential and non-essential goods and services, community and organisational resilience are also interdependent. These implicit partnerships or dependencies for resilience are even more apparent during times of disruption.

Whether caused by natural or anthropogenic sources, each disruptive event produces stark and compelling images. Such was the case in March 2011, when the world watched as first an earthquake, and then a tsunami were followed by a nuclear crisis in Japan. The unprecedented situation challenged every aspect of Japanese society — politically, socially, economically, and emotionally. The scale and impact of this rare confluence of events is gradually emerging, although they are yet to be fully realised in a country with a population of approximately 128 million. Five weeks later, the severity of impact became apparent. On April 18, Japan's National Police Agency confirmed 13,843 deaths while a further 14,030 remained missing. Over 136,000 people were in shelters and at least 81,447 buildings have been fully destroyed, washed away, or burnt down. The Tohoku Electric Power Company said 140,000 households in the north were still without electricity and the Japanese Health Ministry advised that at least 220,000 households in eight prefectures were without running water. In early May, the toll had increased — 14,898 people were confirmed dead and almost 10,000 still missing. The National Police Agency of Japan continues to issue damage situation reports, including numbers of dead and missing and of property and infrastructure damage.[1]

Radiation levels at the Fukushima Daiichi nuclear power plant had reportedly risen to the same level as the Chernobyl nuclear power plant in the former Ukrainian Soviet Socialist Republic in 1986. While there have been comparisons with the Chernobyl nuclear disaster in Ukraine, the International Atomic Energy Agency stated the two are "absolutely different in view of structure and scale." About 37,000 tera becquerals of radioactive materials were emitted in Fukushima, compared with 5.2 million in Chernobyl. As noted by Yukio Yamashita, Executive Director of Japan National Tourism Organisation's Sydney office in

(Continued on Page 3)

[1] *Damage Situation and Police Countermeasures Associated with 2011 Tohoku District – Off Pacific Ocean Earthquake*, National Police Agency of Japan, (May 8 2011).

Global Interdependencies *(Cont. from 2)*

Australia, "Chernobyl exploded, Fukushima stopped automatically."[2] On April 29, the Japanese Nuclear and Industrial Safety Agency (NISA) reported that over 175,000 people have been monitored for radiation.[3]

Recorded as the worst earthquake to hit Japan and the fifth largest earthquake on record globally, the extent of medium and long-term damage has yet to be realised. An early estimate by the Japanese government of the cost of the material damage from the earthquake, which measured 8.9 on the Richter Scale, and subsequent tsunami could exceed $300 billion, making this event the world's costliest disaster.

The situation in Japan is part of a continuum of natural disruptive events around the world. Only two weeks before the earthquake and tsunami in Japan, Chile experienced an earthquake which measured 8.8 on the Richter Scale. The monsoonal floods in Pakistan in 2010 resulted in 21 million people injured or homeless. In addition, 20 percent of Pakistan's total land area is submerged under water; infrastructure incurred extensive damage, and an estimated economic impact equalled one third of its gross domestic product or GDP. The situation was further compounded by disease and increased activity by the Taliban. On January 12, 2010, a 7.0 magnitude earthquake struck the Caribbean nation of Haiti; its government estimated that 230,000 people were killed, 300,000 injured, and 1.5 million people were made homeless.

Not all disruptions are of such magnitude but their impact is still profound. At the beginning of 2011, Australia and New Zealand experienced unprecedented disruptions. Floods in the Australian State of Queensland covered an area the size of France and Germany combined. Further flooding in the southern State of Victoria affected 1,800 properties while the earthquake, which reduced much of the city of Christchurch in New Zealand to rubble, caused 240 deaths and reportedly brought an estimated 200,000 tonnes of silt to the surface. Ten weeks after the earthquake hit Christchurch, the state of national emergency was lifted; however, part of the central business district remained cordoned off.

These natural disruptive phenomena are not new. The Galveston Hurricane of 1900 was described by the National Climatic Data Center[4] as the greatest natural disaster to hit the United States, claiming about 8,000 lives. Over a hundred years later, Hurricane Katrina in 2005 proved comparable; it was recorded as the third strongest hurricane to make landfall.

Previously dormant for almost two hundred years, the global impact of the 2010 eruptions of the Eyjafjallajökull volcano in Iceland was unprecedented and complex. Although relatively small for volcanic eruptions, they caused enormous disruption to air travel across western and northern Europe and about 20 countries closed their air space.

While some natural disruptive events can be predicted, the intensity and extent of the effect are often unexpected. In 1991, the eruption of Mount Pinatubo in the Philippines, the second-largest eruption of the 20th century, was much larger than Eyjafjallajökull. It sent a sulphuric acid haze into the stratosphere, reducing global average temperatures about 0.9 degrees Fahrenheit over the next year.

The traditional method of assessing threats to security is through evaluation of capability and intent. Natural disruptions and disasters do not possess intent, and consequently, challenge pre-existing precepts and the more conventional constructs of security challenges. As shown by the Eyjafjallajökull eruption, the impact of a disruptive event is often unanticipated. That local disruption in a remote part of Iceland highlighted the extent to which nations are interconnected and interdependent, which in turn makes them increasingly vulnerable through our global system.

The Icelandic eruption impacted

(Continued on Page 4)

[2] Angela Saurine, *Returning to Japan in Wake of Disaster*, Adelaide Now online www.adelaidenow.com.au (May 8 2011).
[3] International Atomic Energy Agency, www.iaea.org/newscenter.
[4] National Climatic Data Center, www.ncdc.noaa.gov/.

Global Interdependencies *(Cont. from 3)*

more people than just travellers and international conference delegates. Many companies which relied on 'just-in-time" inventory management either slowed down or closed. The BMW manufacturing company in South Carolina was forced to slow production because leather seat covers from South Africa and transmissions and other parts from Europe were grounded. Nissan suspended production at two Japanese auto assembly plants and computer maker Dell experienced delays in delivering notebook computers to European customers.[5] The price of oil dropped with the decreased demand for jet fuel. Distant flower growers in Kenya suffered when their produce could not reach international markets in Europe and America. Global postal services ground to a halt while energy supply chains around the world revealed their vulnerabilities.

The impact was not just economic but also had serious security implications. The ash from the volcano was so dense over some countries that not even helicopters could fly through it. The exceptional mass of people concentrated at airports and other transportation hubs caused new and unforeseen security problems. Even fighter jets were unable to take to the skies after a senior diplomat reported that several NATO F-16s sustained engine damage from the ash — leaving Europe indefensible militarily as there existed "no available systems for airborne detection of volcanic ash, and aircraft weather radar cannot detect volcanic ash because the particle size is too small," according to the National Aeronautics and Space Administration.[6]

The earthquake and subsequent tsunami in Japan revealed that some organisations fared better than others. It could be argued that they were "lucky" or, more likely, that they had in place resilience measures, plans, and procedures which were flexible, adaptable, and proved to be reliable. Many companies and organisations assessed their recovery and restoration options, including production and distribution alternatives as part of resilience strategies. Even some of those organisations with "just-in-time" inventory management systems had redundancies and alternative supplier arrangements in place — essential attributes of a resilient organisation. Adaptability and flexibility are also distinctive traits of a resilient organisation. In a statement on March 14, 2011, just days after the earthquake struck Japan, the world's largest maker of digital cameras, Canon, stated that in the event that production operations may be suspended for a month or more, the company would consider making use of alternate sites that were not damaged by the earthquake as a means of continuing production. That forecast was updated in April 2011, when Canon advised that recovery of its supply chain to levels before the disruption would take until June or July. Consequently, it lowered its operating profit forecast for the business year-end December to 335 billion yen ($4.1 billion), 29 percent lower than its earlier estimate. Although initially forced to halt operations at its main camera factory on the southern island of Kyushu in March due to a shortage of parts following the earthquake, Canon Chief Financial Officer, Toshizo Tanaka, stated in April that it had resumed to around 70 percent of capacity.[7]

These major disruptive events have also highlighted that a number of critical infrastructure facilities and systems as well as whole communities depend on organisations which are not classed as critical but which are necessary for operational effectiveness and reliability. Non-essential goods and services can assist in maintaining the resilience of communities and individuals in the face of extreme adversity. If estimates are correct that 80 percent of all small to medium-sized businesses involved in a large scale disruption go out of business in 18 months or less, the impact on affected communities after a major disruptive event could be magnified as goods and services are withdrawn.

Given the extent of societal and business disruption faced in Japan as a result of three consecutive

(Continued on Page 31)

[5] Associated Press, (March 2010).

[6] *In the Shadow of Iceland's Volcano: Will We Be Ready Next Time?* (May 10, 2010), www.realtruth.org/articles/100430-001.

[7] S. Mitra-Thaku, "Canon Slashes Profit Outlook after Japan Earthquake," *Engineering & Technology Magazine*, The Institution of Engineering & Technology, (April 26, 2011).

The Treatment of Uncertainty in Infrastructure Planning

by W.E. Walker, J.H. Kwakkel, and V.A.W.J. Marchau,
Faculty of Technology, Policy and Management,
Delft University of Technology
Delft, the Netherlands

Deep uncertainties about the future pose a significant challenge to infrastructure planning. One dominant approach in infrastructure planning has been to largely ignore the uncertainties or to try and reduce them.[1] Planners forecast the future situation by extrapolating past trends forward and developing static blueprint plans for achieving their desired goals. However, for a multitude of reasons, such plans are rarely successful since the future that materializes usually differs significantly from the forecasted future.[2] More enlightened approaches advocate robustness. That is, the plan should perform well in a few foreseeable alternative futures (called "scenarios"). However, both of these approaches suffer from the problem that they focus on those uncertainties that are "among the least of our worries; their effects are swamped by uncertainties about the state of the world and human factors for which we know absolutely nothing about probability distributions and little more about the possible outcomes."[3] Similarly, Goodwin and Wright demonstrate that "all the extant forecasting methods — including the use of expert judgment, statistical forecasting, Delphi and prediction markets — contain fundamental weaknesses."[4] A RAND study stated that the traditional methods "all founder on the same shoals: an inability to grapple with the long-term's multiplicity of plausible futures."[5] Any infrastructure plan designed on the basis of a few forecasts or a small set of assumptions about the future is likely to perform poorly, and unplanned ad-hoc adaptations are needed to improve its performance.

In response to the deficiencies of traditional planning, an alternative planning paradigm has emerged. This paradigm holds that, in light of the deep uncertainties, one needs to plan dynamically and build in flexibility.[6] According to this paradigm, the solution to planning under uncertainty is to create a

(Continued on Page 6)

[1] E.S. Quade, *Analysis for Public Decisions*, (1982); Dempsey et. al, "An Adaptive Approach to Implementing Innovative Urban Transport Solutions," *Transport Policy*, 15, (2009), 405-412; Van Geenhuizen et. al, "New Trends in Policymaking for Transport and Regional Network Integration," *Policy Analysis of Transport Networks*, (2007); M. Van Geenhuizen and W.A.H Thissen, "A Framework for Identifying and Qualifying Uncertainty in Policy Making: The Case Of Intelligent Transport Systems," *Policy Analysis of Transport Networks*, (2007); and R. Cdaniel and D. Driebe, (eds.), *Uncertainty and Suprise in Complex Systems: Questions on Working the Unexpected*, (2005).

[2] Flyvbjerg et al. *Megaprojects and Risk: An Anatomy of Ambition*, (2003); W. Ascher, *Forecasting: An Appraisal for Policy Makers and Planners*, (1978); Porter et al, *Forecasting and Management of Technology*, (1991); T. Kristof, "Is it Possible to Make Scientific Forecasts in Social Sciences," *Futures*, 28, (2006), 561-574; and M. Batty and P. Torrens, "Modelling and Prediction in a Complex World, *Futures*, 37, (2005), 745-766.

[3] E.S. Quade, *Analysis for Public Decisions*, (1982).

[4] P. Goodwin and G. Wright, "The Limits of Forecasting Methods in Anticipating Rare Events," *Technological Forecasting and Social Change*, 77, (2010), 355.

[5] Popper et al, *Natural Gas and Israel's Energy Future: A Strategic Analysis Under Conditions of Deep Uncertainty*, RAND, (2009).

[6] Walker et al, "Adaptive Policies, Policy Analysis, and Policymaking,"*European Journal of Operational Research*, 128, (2001), 282-289; R.J. Lempert, "A New Decision Sciences for Complex Systems," *Proceedings of the National Academy of Sciences of the United States of America*, 99, (2002), 7309-7313; R. De Neufville, "Dynamic Strategic Planning for Technology Policy," *International Journal of Technology Management*, 19, (2000), 225-245; R. Lempert and D. Groves, "Identifying and Evaluating Robust Adaptive Policy Responses to Climate Change for Water Management Agencies in the American West," *Technological Forecasting and Social Change*, 77, (2010), 960-974; Swanson et al, "Seven Tools for Creating Adaptive Policies," *Technological Forecasting and Social Change*, 77, (2010), 924-939; IISD, *Designing Policies in a World of Uncertainty, Change and Surprise - Adaptive Policy-Making for Agriculture and Water Resources in the Face of Climate Change – Phase I Research Report*, (2006); and L. Albrechts, "Strategic (spatial) Planning Reexamined," *Environment and Planning B: Planning and Design*, 31, (2004), 743-758.

Infrastructure Planning *(Cont. from 5)*

shared strategic vision of the future, commit to short-term actions, and establish a framework to guide future actions.[7] A plan that embodies these ideas allows for the dynamic adaptation of the plan over time to meet the changing circumstances. This planning paradigm, in one form or another, has increasingly received attention in various disciplines. In infrastructure planning, the need for adaptivity and flexibility is increasingly recognized. For example, in air transport, the developments of the last decade, including various terrorist attacks, SARS, Mexican flu, and the second Gulf war, have highlighted this need. Combine this with the impacts of privatization and liberalization, the rise of airline alliances, mergers, takeovers, and the emergence of new players in the industry, such as low cost carriers, and it is obvious that it is next to impossible to plan for the long-term development of an airport based on a prediction of the size and composition of future demand. In response to these uncertainties, the need for dynamic adaptive planning has been forcefully argued.[8] A similar line of reasoning can also be found with respect to port development.[9] Another argument for dynamic adaptation in the transport domain comes from research on transport innovations. The implementation of innovations, such as advanced driver assistance systems and innovative approaches for intra-city logistics, is hampered by a variety of uncertainties, including uncertainties about the technology to be implemented and about the future structure of the transport system itself. Dynamic flexible implementation plans have been put forward as a way to overcome these problems.[10] In other domains, the need for adaptivity and flexibility is argued on very similar grounds. For example, in integrated river basin management, the omnipresence of uncertainties in both the environmental system and the societal system is used as an argument for adaptivity and flexibility.[11] Policy-making with respect to climate change is yet another area in which dynamic adaptation and flexibility are suggested as the appropriate approach for policy design.[12]

Figure 1 (on page 7) shows a framework that operationalizes the high level outline of the new planning paradigm, which we call dynamic adaptive planning (DAP). DAP can be divided into two phases: a policy design ("thinking") phase, and a policy implementation phase. The policy design phase consists of four steps — one step (Step I) that sets the stage for policy-making. Three steps (Steps II, III, and IVa) for designing the portions of the adaptive policy that is implemented initially (at time t = 0), and one step (Step IVb) that designs the portions of the adaptive policy that may be implemented in the future (at unspecified times t > 0). The implementation phase consists of two parts — implementation of the portions of the policy that are implemented initially (the portions that were

(Continued on Page 7)

[7] L. Albrechts, "Strategic (spatial) Planning Reexamined," *Environment and Planning B: Planning and Design*, 31, (2004), 743-758; and Walker et al, "Adaptive Policies, Policy Analysis, and Policymaking," *European Journal of Operational Research*, 128, (2001), 282-289.

[8] R. De Neufville, "Dynamic Strategic Planning for Technology Policy," *International Journal of Technology Management*, 19, (2000), 225-245; Kwakkel et al, "Adaptive Airport Strategic Planning," *European Journal of Transportation and Infrastructure Research*, 10, (2010), 227-250; R. De Neufville and A. Odoni, *Airport Systems: Planning, Design, and Management*, (2003); G. Burghouwt, *Airline Network Development in Europe and its Implications for Airport Planning*, (2007); and Walker et al, "Adaptive Policies, Policy Analysis, and Policymaking," *European Journal of Operational Research*, 128, (2001), 282-289.

[9] Taneja et al, "Implications of an Uncertain Future for Port Planning," *Maritime Policy & Management*, 37, (2010), 221-245.

[10] V.A.J.W. Marchau and W. E. Walker, "Dealing with Uncertainty in Implementing Advanced Driver Assistance Systems: An Adaptive Approach," *Integrated Assessment*, 4, (2003), 35-45; Marchau et al, "An Adaptive Approach to Implementing Innovative Urban Transport Solutions," *Transport Policy*, 15, (2009), 405-412; J. Van Zuylen and K. Weber, "Strategies for European Innovation Policy in the Transport Field," *Technological Forecasting and Social Change*, 69, (2002), 929-951; and E. Erikson and K. Weber, "Adaptive Foresight: Navigating the Complex Landscape of Policy Srategies, *Technological Forecasting and Social Change*, 75, (2008), 462-482.

[11] Pahl-Wostl et al, "New Methods for Adaptive Water Management Under Uncertainty - the NeWater Project," (2005); and Pahl-Wostl et al, "Managing Change towards Adaptive Water Management through Social Learning," *Ecology and Society*, 12, 30, (2007).

[12] Wardekker et al, "Operationalising a Resilience Approach to Adapting an Urban Delta to Uncertain Climate Changes," *Technological Forecasting and Social Change*, 77, (2010), 987-998; Dessai et al, "Do We Need Better Predictions to Adapt to a Changing Climate"? EOS, 90, (2009), 111-112; and J. Smith, "Setting Priorities for Adapting to Climate Change," *Global Environmental Change*, 7, (1997), 261-266.

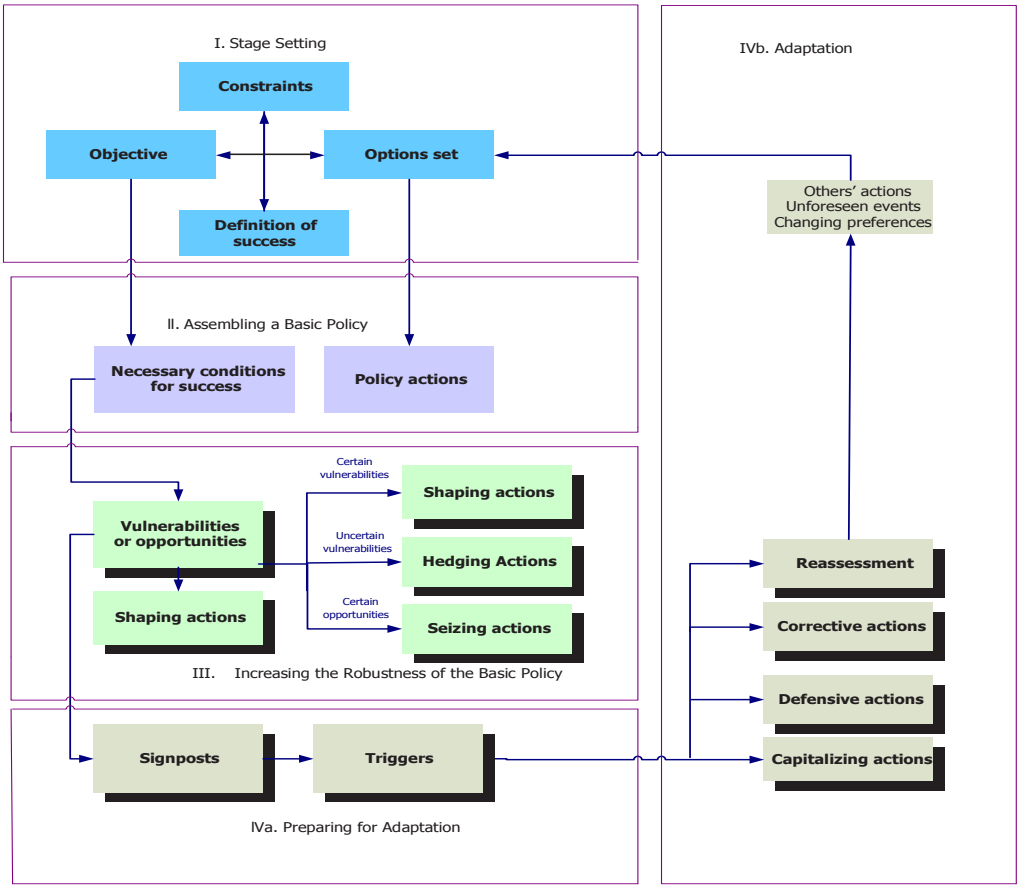
Infrastructure Planning *(Cont. from 6)*

designed in Steps II-IVa) and adaptation of the initial policy (taking the actions that were designed in Step IVb).

In short, in Step I, the existing conditions of an infrastructure system are analyzed, development goals are specified, and necessary conditions for the policy's success are laid down. In Step II, the way in which this is to be achieved is specified. This basic plan is made more robust through four types of actions, which are specified in Step III: *mitigating actions* are actions to reduce the *certain* adverse effects of a plan; *hedging actions* are actions to spread or reduce the risk of *uncertain* adverse effects of a plan; *seizing actions* are actions taken to seize certain available opportunities; and *shaping actions* are actions taken to reduce the chance that an external condition or event that could make the plan fail will occur, or to increase the chance that an external condition or event that could make the plan succeed will occur. Even with the actions taken in Step III, there is still the need to monitor the performance of the plan and take action if necessary. This is called contingency planning, and is specified in Step IVa. *Signposts* specify information that should be tracked in order to determine whether the plan is achieving its conditions for success. Critical values of signpost variables (*triggers*) are specified, beyond which actions should be implemented to ensure that the plan keeps moving the system in the right direction and at a proper speed. There are four different types of actions that can be triggered by a signpost (Step IVb): *defensive actions* are taken to clarify the basic plan, preserve its benefits, or meet outside challenges in response to specific triggered that leave the basic plan remains unchanged; *corrective actions* are adjustments to the basic plan; *capitalizing actions* are actions triggered to take advantage of opportunities that improve the performance of the basic plan; and a *reassessment* of the plan is initiated when the analysis and assumptions critical to the plan's success have clearly lost validity.

In the policy implementation phase, the actions to be taken immediately (Step II and Step III) are implemented, and a monitoring system (Step IVa) is established. Then time starts running, signpost information related to the triggers is collected, and actions are started, altered, stopped, or expanded in response to this information. After implementation of the initial actions, the implementation of other actions (Step IVb) is suspended until a trigger event occurs. For a more detailed explanation of this framework, see Kwakkel et al., Marchau et al., and Walker et al.[13]

Figure 1: The steps of dynamic adaptive planning (Kwakkel et al., 2010).



(Continued on Page 32)

[13] Kwakkel et al, "Adaptive Airport Strategic Planning," *European Journal of Transportation and Infrastructure Research*, 10, (2010), 227-250; Marchau et al, "An Adaptive Approach to Implementing Innovative Urban Transport Solutions," *Transport Policy*, 15, (2009), 405-412; and Walker et al, "Adaptive Policies, Policy Analysis, and Policymaking," *European Journal of Operational Research*, 128, (2001), 282-289.

Policy Innovation in Critical Infrastructure Protection

by Manuel Suter, Center for Security Studies, ETH Zurich

Practitioners in critical infrastructure protection (CIP) are confronted with a variety of questions in creating and developing CIP policies. How can the critical sectors and key resources (CIKR) be identified? Which are the most relevant threats and risks for the individual critical infrastructures? How can these risks be managed, especially when different infrastructures depend on each other?

These and similar questions highlight the complexity of CIP. The risks are hard to assess, the environment is constantly evolving, and critical systems are increasingly interdependent. Thus, it is not surprising that protection policies are under constant development. Over the years, a variety of different concepts have been introduced to describe and measure specific facets of CIP. Examples for such concepts are "criticality," "interdependence," "vulnerability," or the recently popular "resilience." Likewise, there have been several innovations on the operative level: public-private partnerships have been promoted to improve collaboration between the government and the owners and operators of critical infrastructure, dedicated CIP programs have been initiated to ensure a coordinated approach with regard to the protection of CIKR, and new specialized agencies have been established.

Of course, such policy innovations do not emerge out of the blue. In the following article, two sources of innovative CIP policies will be discussed in order to gain a better understanding of how CIP policies develop and the likely origins of new trends.

Policy Learning in CIP

The first and probably the most important source for policy innovation in CIP is exchange among experts. A synopsis of various CIP policies reveals that the building blocks of these policies are very similar across different countries. They identify similar sectors as critical, use similar concepts for their risk management in CIP, and have often established similar organizational frameworks to implement protection policies. These similarities show that policy-makers are learning from each other. They observe the developments in other countries and adopt successful strategies. Ideas and concepts are frequently shared at conferences and meetings or are presented in international publications.

Mutual learning between countries was particularly strong during the early stages of CIP policy development at the end of the 1990s. Given that the United States was, in many regards, leading the way in CIP, U.S. concepts were adopted by other countries. Today, policy learning is especially relevant for emerging countries that have not yet established CIP policies, but are increasingly confronted with the need to protect essential infrastructures.

Policy Transfers

However, mutual learning is not the only source of innovation. Many concepts and approaches that are applied today in CIP have originated in other areas. This is evident in the concepts used for risk management in CIP, especially since the importance of risk analysis and mitigation has long been acknowledged in various other fields of public policy. The risks related to interdependencies, for example, have been extensively discussed in economics, and the terms "vulnerability" and "resilience" are traditionally used for the purpose of risk management related to technical systems.

Likewise, the organizational responses to the challenges of CIP have been inspired by the solutions found for other fields. For example, public-private partnerships as an institutionalized form of collaboration between the public and the private sector were in use for financing and maintaining public buildings and infrastructures

(Continued on Page 33)

International Cooperation in Crisis Management: A European Perspective

by Peter Wahlgren, LL.D.*

Large scale crises, such as natural disasters, technological accidents, or terrorist attacks, can influence many countries simultaneously as they may occur in or involve multinational regions. The international aspect is also of vital importance when an affected country's resources are insufficient and international relief operations have to be initiated.[1] Therefore, it follows that in crisis management and rescue operations, different organizational traditions, lack of standards, varying proceedings, and multilingual cultural aspects must be taken into consideration. Difficulties concerning coordination may relate to technical components, communication standards, data formats as well as social, ethical, and legal aspects.

Many of these questions form the basis for the activities in a recently initiated large-scale research project in the European Union. BRIDGE (bridging resources and agencies in large–scale emergency management) is a project with the objective to create a system to support interoperability in large-scale emergency relief efforts.[2] The project engages researchers from 14 organizations in seven countries, representing academic institutions, higher education, private companies, and research organizations. There is also an advisory board representing end-user-organizations responsible for different aspects of crisis management (e.g. civil agencies, police, international association of fire and rescue services, health, and European standardization). BRIDGE, launched in April 2011, will have a duration of 48 months.

With the overall objective to increase the security and safety of European citizens, BRIDGE seeks to develop methods and tools that can support run-time intra- and inter-agency collaboration. Another explicit objective is to advance human-computer interaction techniques for simple exploration of high-quality information in a context where incoming data is imprecise, fragmented, and erroneous and where communication differs in medium and modality (image, text, audio, eyewitness testimony, language, etc.).

The intention is to develop a common user interface that presents the combined fragments of data that conforms to human cognitive strengths and weaknesses, facilitates shared situational awareness, and enables users to obtain, filter, share, and annotate information with a targeted subset of individuals.

At a higher level, the system should help to mediate the activities of the command and general staff, including strategic decision-making. At the lower level, the system will help to merge the systems and resources from different agencies into a consistent whole.

The project is basically a technical project. However, given that one of the objectives is to facilitate multi-agency collaboration in international large-scale relief efforts, the team also comprises legal, sociological, and ethical expertise. In this respect, the assignment is to investigate mutual dependences of technology, organizational dynamics, human factors, ethical, legal, as well as societal issues, risks, and difficulties. The purpose is also to make an inventory of privacy issues, develop possible strategies for handling potential legal infringements, and to

(Continued on Page 37)

[1] As of March 14, 2011, three days after the earthquake and tsunami of March 11, following a direct appeal from the government of Japan, the country had received help from Urban Search and Rescue Teams from 14 countries and was offered help from a large number of additional countries, international organisations and volunteers. *Mega Disaster in a Resilient Society: The Great East Japan (Tohoku Kanto) Earthquake and Tsunami of 11th March 2011: Synthesis and Initial Observations*; International Environment and Disaster Management Graduate School of Global Environmental Studies, Kyoto University (25 March 2011).

[2] BRIDGE is a collaborative project funded by the seventh framework programme of the European Union (FP7-SEC-2010-1, Grant Agreement 261817).

A Community-Oriented Approach to CIIP in Developing Countries

by I.D. Ellefsen, Academy for Information Technology, University of Johannesburg, and Professor S.H. (Basie) von Solms, Academy for Information Technology, University of Johannesburg*

Critical information infrastructure protection (CIIP) is an area that must be addressed in developing countries. The traditional role of a Computer Security Incident Response Services (CSIRT) must be redesigned to operate in an environment that has a unique and wide-ranging set of requirements. This research project aims to identify potential frameworks and models for CIIP in developing countries by identifying potential risks, areas of concern, and possible solutions.

Introduction

The role of CIIP in developing countries is a vital question that must be answered. As developing countries invest a large number of resources into interconnecting technologies, these regions are beginning to feel the need to create structures responsible for maintaining their critical infrastructure. Developing countries, such as those in Africa, are particularly vulnerable to cyber attack due to a combination of factors, including increasing Internet penetration rates, high levels of computer illiteracy, and ineffective legislation. These factors all expose the critical infrastructure in developing countries to higher levels of risk. In the following section, we will elaborate on these risk factors, and then discuss a potential model to address these concerns.

Factors Driving Increased Risk in Developing Countries

As developing countries enter the global stage, there are a number of factors that drive increasing risk. Each of these risk factors (described below) affects the ability of a country to protect their critical infrastructure. That is not to say that these are the only factors that play a role; however, they do provide a good cross-section of the types of risks that are observed.

Increasing Bandwidth

Traditionally bandwidth available to developing countries has been limited. However, this is no longer the situation. In recent years, Sub-Saharan Africa has experienced a growth in the number of fibre-optic cables that have made landfall.[1] This has had a dramatic effect on how governments, companies, and individuals interact with Internet-based technologies.

With the increasing bandwidth, there is a drive for governments and businesses to adopt and implement eServices. This has the promise of allowing these companies to interact with their customers in a more efficient manner. Along with adopting Internet-based technologies for the provision of services, there is also a drive to utilise these technologies to provide interconnection for a number of critical systems. The development of these interconnecting systems allows developing nations to compete more effectively in an increasing interconnected world.

To illustrate the scope of future interconnection within Sub-Saharan Africa, Figure 1 (on page 11) shows how the introduction of a number of undersea cables has dramatically increased available bandwidth in a relatively short period.[2] With the growth in capacity, there is also an observed increase in the use of related technologies.

Increasing Use of Wireless Technologies

Developing nations have long experienced problems in providing

(Continued on Page 11)

[1] *African Undersea Cables*, redistributed in terms of a CC-BY-2.0 Licence, http://creativecommons.org/licenses/ by/2.0/deed.en, (February 2010), http://manypossibilities.net/ african-undersea-cables.

[2] Ibid.

Developing Countries *(Cont. from 10)*

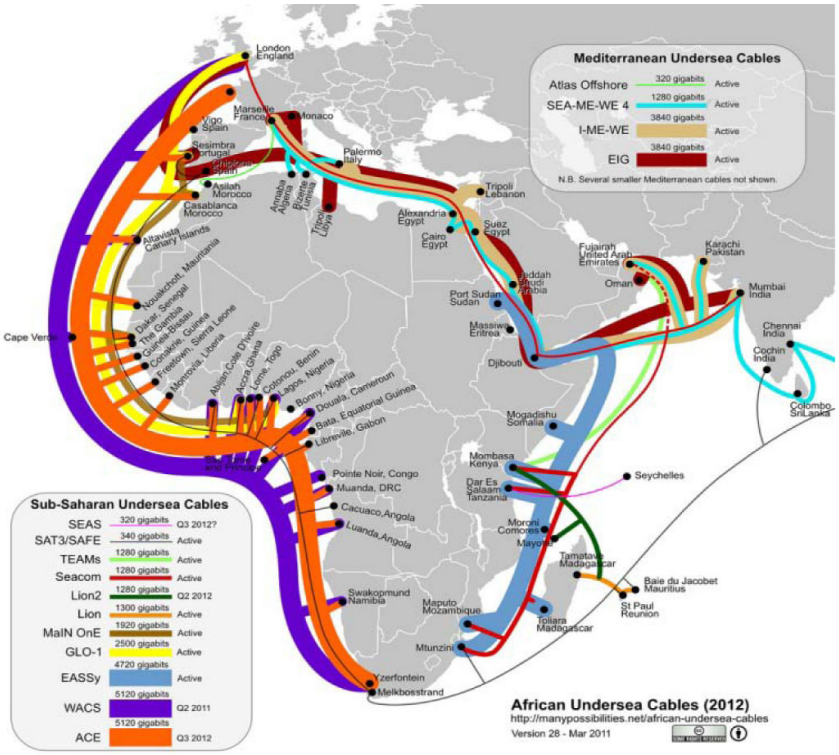
services to far-flung regions within their borders. The prospect of providing a physical link to a remote region is not feasible in many cases. However, the growing use of wireless technologies allows vast areas to be connected by investing in a number of wireless transmitters. Cellular networks, wireless mesh networks, and similar technologies are connecting communities at a much greater pace than what would have been possible using traditional means. Wireless technologies often present an attractive alternative for developing countries.

Statistics of mobile telephone users support these observations. As outlined in a report published by Cisco Systems, of the 4 billion cellular telephone users worldwide, 75 percent of those are in developing countries.[3] The use of these new technologies creates a wider user base; however, these new users often do not have the computer security skills that in turn increase the overall risk in developing countries.

Lack of Awareness

Developing nations are often seen has having poor literacy rates. Consequently, there is a severe lack of computer literacy and computer security awareness. In order to access eServices, new users must utilise the Internet without being equipped with the necessary skills to identify well-known threats (such as phishing). Attackers are now able to reuse old techniques, as users in developing nations have not experienced this type of attack before.[4] To illustrate this point, reports indicate that spam accounted for 79.1 percent of email traffic in South Africa.[5] Although this factor is a global problem, the shear size of the increasing user base in developing countries amplifies the problem.

Figure 1: Showing predicted fibre-optic cables in Africa by 2012



Ineffective Legislation and Policies

Legislation and policy in developing countries often do not adequately address Internet-based technologies. This prevents any CIIP structure from having the required legal backing to operate effectively. Furthermore, there might not be adequate policies in place that allow national CIIP structures to function. The development of effective legislation and policies is essential to create effective CIIP structures. Although there are efforts to create policy documents to address this need,[6] the resulting documents often do not address all areas required for an effective CIIP solution.

All of the discussed risk factors expose developing countries to

(Continued on Page 12)

[3] *Cisco 2009 Annual Security Report,* Technical Report, Cisco Systems Inc., (2009). http://www.cisco.com/en/US/prod/vpndevc/annual_ security_report.html.

[4] Ibid.

[5] *March 2011 Intelligence Report,* Symantec, (March 2011). http://www.messagelabs.com/mlireport/MLI_2011_03_ March_Final-EN.pdf.

[6] South African Department of Communications, *Draft Cybersecurity Policy of South Africa*, Government Gazette, No. 32963, Republic of South Africa, (February 2010).

Developing Countries *(Cont. from 11)*

cyber attacks. In the following section, we will discuss the potential for cyber attacks on developing countries.

Developing Nations and Cyber Attacks

Cyber attacks can have devastating effects on governments, companies, and individuals worldwide. Nobody is immune to the effects of cyber attacks. Cyber attacks present a completely different threat than their traditional counterpart, where the ability to wage war was in the domain of governments. Cyber attacks can be initiated by any individual with the necessary skills.

With reference to the previous section, it is not difficult to predict a possible outcome of interconnecting a vast number of users in a relatively short period of time. Developing countries are now experiencing the impact of cyber attacks, with an increasing number of attacks targeting users in these countries.

Protection structures in developed nations have evolved over the past 20 years. With the initial development of the Computer Emergency Response Teams (CERTs) in the 1980s, these structures have grown and matured alongside the development of the Internet.[7] However, this is not true in developing nations. With only a limited ability to connect to the Internet, and therefore to connect internal systems, developing countries had little need to develop such structures. Given the limited number of cyber attacks they experienced, developing countries might have considered themselves "immune" to cyber attacks. However, they now find themselves in a position to address this concern. The unique requirements in developing countries require unique solutions. In the following section, we will reflect on why an alternative approach is required.

A Different Approach to CIIP in Developing Countries

Due to the unique challenges that are present in developing nations, especially in Africa, there must be a different approach to CIIP. There are many existing models with a variety of different benefits; however, these models are tailored for the environment in which they are deployed. As such, these models are not directly suited for developing countries.

The risk factors discussed above highlight this fact: the challenges experienced in developing countries are wide-ranging and unique. Solutions have to be developed with this in mind. In the following section, we will discuss a potential solution to address the needs of developing countries.

Community-Oriented CIIP

Traditional methods of CIIP often take the form of a Computer Security Incident Response Team (CSIRT)-like structure, although it is known by various names. The basic concept is that of a coordinating structure responsible for overseeing CIIP within a country. Generally, these structures are "top-down" with a focus on governments, and large industry as the primary constituent. Depending on the implementation, there will be various other bodies that assist CSIRT in achieving its core service.

With such a varied environment, a traditional CSIRT structure would not effectively provide CIIP for all stakeholders. That is not to say that there is no place for a CSIRT structure in a developing country, only that any protection structure should be supplemented so that it can holistically address the challenges that are faced.

Any society is made up of a number of related communities, be they a community of individuals, small businesses, or large industries. These communities will have their own set of requirements when conducting business, and as a consequence, they will have a set of requirements for computer security. This idea of related communities can be used to form the bases for a CIIP model. This model has a direct focus on a related community of members, rather than a high-level overview. This idea of community involvement has been explored before;[8] however, within the context of a developing country, it

(Continued on Page 29)

[7] G. Killcrece, *Steps for Creating National CSIRTs*, CERT® Coordination Center, (August 2004). http://www.cert.org/archive/pdf/NationalCSIRTs. pdf.

[8] J. Harrison and K. Towsend, "An Update on WARPs." *ENISA Quarterly Review*, 4(4):13–14, (December 2008). http://www.warp.gov.uk/downloads/enisa_quarterly_12_08.

RECIPE – Good Practices for CIP Policy-Makers

by Eric Luiijf, Marieke Klaver, and Albert Nieuwenhuijs,
Netherlands Organisation for Applied Scientific Research TNO

All European Union Member States are obliged by European Council Directive 2008/114/EC to identify and designate European critical infrastructure (ECI) and to assess the need to improve their protection. This obligation stimulated Member States to also look at their national critical infrastructures. However, it was discovered that there is a limited exchange of experience and knowledge between nations about how to develop CIP policies and how to successfully implement them. Therefore, nations sometimes reinvent the CIP "wheel" or find themselves trapped in the same pitfalls explored and experienced by other nations.

A project named "Recommended Elements for Critical Infrastructure Protection for Policy-Makers in Europe" (RECIPE) was established to remedy the lack of information exchange among different nations. The policy approaches towards CIP in a number of nations were collected and analyzed. The Good Practices document for CIP policy-makers is currently in its final review phase. This article presents a short description of the approach. An outline of the final document will be published in June 2011.

A TNO-led consortium consisting of the Netherlands Ministry of Security and Justice, the Slovakian Ministry of Transport, Construction and Regional Development, the Austrian Institute for International Affairs (OIIP), and the Estonian Ministry of the Interior undertook the European Commission sponsored RECIPE project. All consortium partners were involved in one way or another in earlier development and/or application of national CIP policy. At the same time, the project team built on bilateral and multinational networks of CIP policy contacts in Europe and abroad. Rather than immediately approaching these contacts, the team first undertook a major desk research effort. This effort concluded that CIP policy-makers face six key challenge areas: identification of critical infrastructure; critical infrastructure dependencies; public-private partnerships; information sharing; risk management; and crisis management. From the inception of the RECIPE project, it was clear that specific CIP good practices in policy will not fit all nations. A nation will have to compose its own set of CIP policies, tailored to its specific needs and possibilities. Differences in CIP maturity, historic and legal backgrounds, and many other reasons require selective picking and adaption of good practices. As such, the RECIPE manual is more of a cookbook with various recipes under each of the six themes. Based on the desk research, for each of the six themes the team selected an initial set of promising CIP good practices stemming from various nations in Europe, Australia, Canada, Singapore, and the United States. The team realized that the added value of RECIPE is not just the collection of good practices, but in the understanding of less successful or even failed CIP policy initiatives and projects. These too

(Continued on Page 14)

Good Practices *(Cont. from 13)*

provide valuable experiences, especially when they indicate fundamental problems. As nations are not proud of their unsuccessful initiatives, the lessons identified are not found in the public. Nevertheless, the RECIPE team members assembled a set of unsuccessful initiatives to study.

Team members contacted CIP policy-makers in selected nations to acquire deeper insight into the main reasons for (lack of) success of a certain approach. Strict confidentiality was promised to the interviewed policy-makers to enable frank and open answers. The team was blessed by the professional attitude of the interviewed national CIP policy-makers willing to share even their negative experiences. This information helped the team compose an introductory text on each theme highlighting the essential conditions for a successful implementation of good practices.

Last, but certainly not least, the team analyzed the challenges for CIP policy-makers related to CIP policy transplantation. A CIP good practice may look great at first glance, but they may not fit for implementation in a specific nation. The team identified four cross-cutting dimensions that are of essence in determining whether a specific good practice can be adapted to a nation: (1) the level of involvement of private parties in CIP; (2) the level in which the co-operation structure is mandated by law or is on voluntary basis; (3) the maturity in the nation of CIP policy approaches and implementations; and (4) an indication of the amount of resources required for successful implementation.

Each of the 22 identified good practices is tagged with an indicator for each of the first three elements. When a nation is not yet used to intense interactions between public and private parties, good practices that indicate little need for public-private partnership structures will probably be more suited to them. When a nation generally requires a statutory decree to pass Parliament before a CIP-related activity may be initiated by a government agency, good practices which are tagged "mandated" are probably better suited. Also, when just starting to develop CIP policies, the CIP policy-maker may want to look for CIP good practices tagged with a low required level of CIP maturity.

As previously mentioned, the good practices are organised along six key themes.

The first theme, "identification of critical infrastructure," discusses the benefits and drawbacks of top down and bottom up approaches to identify critical infrastructure. Following the European Council Directive approach, the manual explains four basic steps to identify critical infrastructure. The manual includes four different good practice approaches to identify critical infrastructure, each with their pros and cons. These practices include: (1) operator-based; (2) service-oriented; (3) asset or hybrid-based; and (4) bottom-up cross-border approaches. In the first case, the government designates companies as a critical infrastructure operator, requiring them to perform a risk assessment and to develop security plans. The service-oriented approach starts from identifying and designating services which are critical to the society. The asset or hybrid-based approach is based on designated critical assets in which criticality is regularly evaluated by a risk assessment process. For the bottom-up, cross-border approach, the U.S.-Canadian cross-border critical infrastructure identification and designation approach was taken as good practice.

The second theme, "critical infrastructure dependencies," first explains why there is a need for critical infrastructure dependency analysis. The concept of dependencies is explained, along with some important notions stemming from various theoretical models such as critical infrastructure disruption and recovery characteristics. Attention is drawn to different modes of critical infrastructure operation, as the set of critical dependencies may become completely different when the critical infrastructure mode of operation shifts away from normal. For example, a critical infrastructure is not dependent on diesel fuel and fuel transport until the electric power is disrupted and one starts the backup generator. Various methods to map critical infrastructure dependencies are discussed.

Three good practices were identified for this theme: (1) identifying critical infrastructure dependencies using intersectoral workshops; (2) performing a qualitative analysis; and (3)

(Continued on Page 30)

Impacts of the March 11, 2011 Tohoku Tsunami on Defensive Elements of Japan's Critical Infrastructure

by Gary Chock, Structural Engineer, ASCE Tohoku Tsunami Reconnaissance Team Leader, and Chair, ASCE 7 Standard - Tsunami Loads and Effects Subcommittee

Japan has a long history of experiencing great earthquakes and tsunamis. In fact, as evidenced in Table 1, it is the country with the highest frequency of tsunami attacks in the world. Beginning after the 1933 Showa Sanriku Tsunami and accelerating after the 1960 Chile and 1993 Hokkaido-Nansei-Oki Tsunamis, many tsunami-resistant countermeasures were explicitly implemented in Japan, including breakwaters, seawalls, tsunami-resistant development plans, and evacuation procedures. Tsunami protective structures along the Sanriku coast (the three prefectures of Miyagi, Iwate, and Aomori) constituted critical infrastructure that were vital to the protection of life, property, and economic assets of these coastal communities. However, the March 11, 2011 2:26 pm moment magnitude (Mw) 9.0 local earthquake and tsunami was unprecedented in tsunami height and spatial extent along the coast of the main island of Honshu. In this article, we discuss the impacts of the tsunami on these elements of tsunami countermeasures for risk reduction are discussed.

ASCE Structural Engineering Institute (SEI) and Coasts Oceans Ports and Rivers Institute (COPRI) deployed three teams to examine tsunami damage, including critical infrastructure. The author was the leader of the ASCE Tohoku Tsunami Reconnaissance Team that traveled with several Japanese research collaborators during April 16 to May 1, focusing on structures and overall tsunami impacts. At the time of this article, the ASCE Tsunami Team is working towards a July 1, 2011 report release. Therefore, these comments herein are preliminary. The COPRI teams for detailed assessments of coastal structures, ports, and harbors have just recently returned and will be issuing their reports at a later date. It should be noted that these observations were made for a country with significant tsunami protective structures and mitigation measures in place. The lessons to be learned may have even greater importance for the United States, where the vulnerability of our critical infrastructure along the west coast is just beginning to be recognized outside of the scientific community. The ASCE Tsunami Team was able to observe examples of structural countermeasures along the most severely affected coastal region (see Table 2 on page 16).

Date	EQ Magnitude	Name	Max Height of Runup in Japan	Fatalities
January 27, 1700	9	Cascadia	3 m	?
October 28, 1707	8.4	Hoei	10m	?
June 15, 1896	7.2	Meiji Great Sanriku	25-30+m	22,000
September 1, 1923	8	Great Kanto	12m	2,000
March 2, 1933	8.4	Showa Sanriku	28m	3,000
December 7, 1944	8.1	Tonankai	10m	1,251
December 21, 1946	8.4	Nankaido	11m	1,330
May 24, 1960	9.5	Chile	5m	142
March 26, 1983	7.7	Japan Sea	10 m	107
July 12, 1993	7.8	Hokkaido-Nansei-Oki	10m in Hokkaido	202
March 11, 2011	9.0	Tohoku	38.9m	24,000

Table 1: List of Major Historical Damaging Tsunamis Affecting Japan

It appears that tsunami height design criteria in Japan has evolved over the years; recently, by utilizing

(Continued on Page 16)

Japanese Infrastructure *(Cont. from 15)*

either the largest past tsunami from which credible evidence on runup could be obtained, or modeled inundation depths for the possible tsunamis caused by the largest earthquake that can be assumed to occur. The Mw 9.0 Tohoku Earthquake, also known (in Japan) as the Great East Japan Earthquake, far exceeded the maximum credible earthquake that was anticipated. This may have lessons for the United States on the question of whether tsunami design criteria should have a "deterministic maximum limit" based on judgment of the capacity of the seismic source, as is presently done for earthquake design on the west coast, or whether the tsunami design level should be entirely probabilistically based. (For more information on the impact of the Tohoku earthquake and tsunami on U.S. nuclear facilities, see page 25. The reasoning to use a probabilistic approach for tsunamis for risk management is that *the consequences of tsunami height underestimation are quite severe*.

Table 2: Structural Countermeasures along the most severely affected coastal region

Structural	Countermeasure	Locations Observed
	Seawalls and Tsunami Gates	Kuji, Noda , Fudai, Tarou and Miyako, Otsuchi, Kamaishi, and Rikuzentakata
	Breakwaters	Hachinohe, Kuji, Otsuchi, Kamaishi, Ofunato, Minamisanriku
	Tsunami Mitigation Forests	Rikuzentakata, Natori south of Sendai Airport
Evacuation	Vertical Evacuation Buildings	Kamaishi, Kesunnuma, Minamisanriku, Rikuzentakata
	Evacuation Sites on Higher Ground	Miyako, Rikuzentakata, Minamisanriku, Onagawa
	Evacuation Signage & Warning sirens	Numerously observed in all locations visited

Irrespective of population, the majority of coastal communities along most of the areas north of Sendai had seawalls designed for tsunami mitigation. These seawalls would have had a considerable range of construction date vintages. The tsunami protection walls mainly consisted of either earth filled dikes protected by concrete slabs on both the offshore and onshore slopes, or of massive gravity seawalls constructed of monolithic unreinforced concrete. However, with few exceptions, seawalls were overtopped by a significant margin (sometimes up to twice their height) which subsequently created a breaching failure. There have been undermining failures due to massive scour of the onshore toe of the sea-wall due to overtopping. In other cases, some concrete gravity seawalls were overturned by the return flow following inundation, rather than by the incoming tsunami. Seawalls were equipped with heavy steel gates and the majority of these gates seem to have resisted the incoming flow but not necessarily the outward return flow. The tsunami height was greatly affected by the coastal bathymetry and local topography, and in all cases so far exceeded the design height of tsunami defensive walls and gates. The resulting damage was near complete destruction to most low-rise buildings in low-lying communities. However, there could have been even greater spatial extent of damage had there been no seawall protection at all.

Notable exceptions to this were seawalls experiencing only a moderate amount of overtopping; these structures still appeared to provide a pronounced mitigating effect on tsunami damage, provided they did not undergo a structural failure. The tsunami defensive wall for the town of Fudai was quite successful in mitigating the effects of an 18.5 meter tsunami water depth. Even though the gated wall was overtopped by about three meters, the extent of damage on the lee of the wall to the town was minimal. Another case of demonstrable effectiveness was seen in the city of Miyako. In this city, we examined areas of the town outside of the seawall and the portions within. The difference was remarkable, with the unprotected area essentially more than 90 percent destroyed and the portion behind the seawall having damage that was mostly localized. This was in spite of the fact that various sections of the protective wall were overtopped by about two meters.

Most offshore breakwaters failed in the tsunami, as evidenced by either remote sensing or on-site

(Continued on Page 17)

Japanese Infrastructure *(Cont. from 16)*

observation of breakwaters (and their disappearance). The tsunami mitigation forests appeared to be ineffectual on their own, since trunks were snapped off or uprooted, and merely provided large wooden debris missiles brought inland by the tsunami.

Every community has tsunami road signs indicating when you enter and leave the potential tsunami inundation area. These signs appear to have been conservatively located such that the destructive part of the tsunami occurred within the zone, even when most seawalls and breakwaters were severely overtopped or destroyed. Therefore, it seems tsunami evacuation and awareness policy implementation for public safety did not assume that tsunami effects would always be prevented by these seawalls.

Warnings for the occurrence of the most severe category of tsunami were being issued beginning approximately three minutes after the Tohoku Earthquake. Communities utilized vertical evacuation buildings as well as locally higher ground sites as evacuation centers as a part of their local disaster management plan. In the northern Sanriku coastal areas, there were communities where the tallest buildings were not higher than four or five stories. There were several cases where up to four-story buildings were overtopped by the tsunami, including some tsunami evacuation buildings, a hospital, and local emergency management centers, resulting in loss of life amongst those who expected to be safe in those buildings. News reports indicate that over a hundred evacuation buildings or evacuation sites were inundated. Some emergency evacuation centers, such as in Minamisanriku and Onagawa, were seismically robust low-rise structures (for example, a fire station) that were manned by those issuing the tsunami warnings and broadcasting real-time accounts of the tsunami to the towns, and perished while fulfilling that mission. In these cases, the building structures survived but most of their occupants did not. In one case in Rikuzentakata, such real-time reporting resulted in abandonment of a tsunami evacuation center to move to even higher ground before the four-story building was inundated, thereby saving several dozens of primary school children. Several tall high-rise reinforced concrete buildings that served as tsunami evacuation buildings were visited and they performed well, the evacuees furnishing a number of spectacular videos of tsunami flow destroying neighboring buildings around them.

Seawall gate protected Fudai in Iwate Prefecture despite being overtopped. *Photo courtesy of Gary Chock.*

Japan's tsunami response plan did not rely on physical countermeasures alone. It is apparent that the effective tsunami warning system and evacuation indeed saved thousands of lives. The population in the tsunami-affected coastal areas in Honshu was over 250,000. Of this, there were 24,000 fatalities or missing persons with over 130,000 buildings collapsed or partially collapsed per police records. From the level of damage observed in the tsunami-inundated areas, it would be difficult to expect even a

(Continued on Page 31)

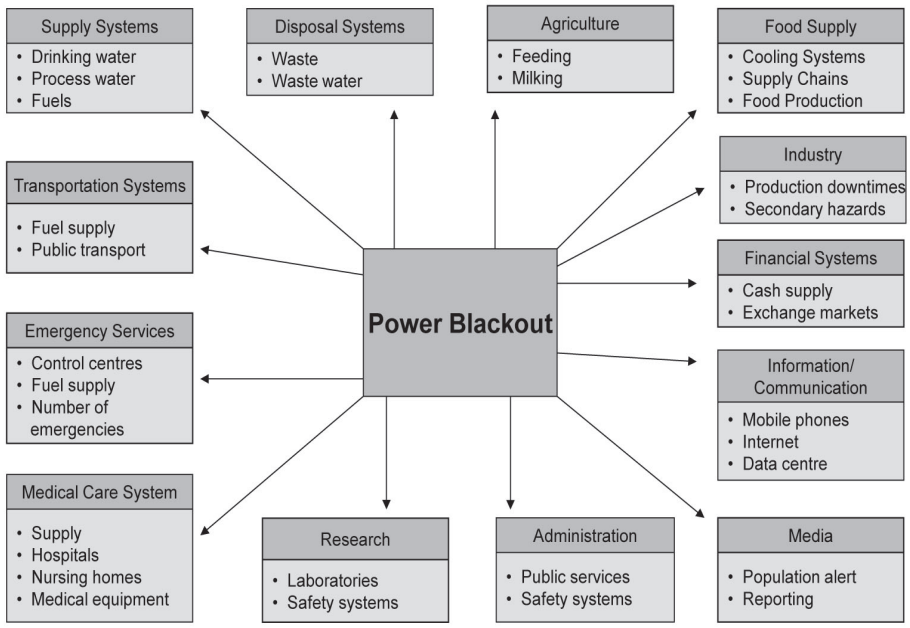
Critical Infrastructure Protection in Germany: Accounting for Inter-infrastructure Dependencies and Facilitating Public-Private Cooperation

by Mirjam Merz, Michael Hiete, and Frank Schultmann*

Modern societies largely depend on the safe and secured operation of critical infrastructure systems such as electricity and water supply, transportation, and communication systems but also health care, banking and finance, primary industry, and administration. Since almost all social, economic, technical, and administrative activities depend on the undisturbed availability of electricity, the power supply system takes an exceptional position. Even if the service security of power supply in Europe, especially in Germany, is relatively high, power supply is inherently vulnerable against technical or human failure, natural disasters, sabotage, and acts of terrorism as well as against grid overloads and imbalances in the power system.[1]

During the past few years, several real power blackouts and a power disruption scenario, practiced by the German Federal Office of Civil Protection and Disaster Assistance within a national crisis management exercise (LÜKEX 2004), revealed that power disruptions lead to considerable physical, social, and economic damages within infrastructure systems and other sectors of society (see figure 1). Due to the increased level of interdependencies between the different infrastructure systems, cascade-effects play an important role and disruptions might be propagated from one infrastructure system to another.[2]

Figure 1: Impacts of power blackouts within Critical Infrastucture and Social Sectors.



Power supply disruptions, especially for the healthcare sector and the industrial production sector, pose a challenge. For example, in the health care sector, the breakdown of medical devices and building services, such as elevators and cooling systems, as well as the reduced availability of pharmaceuticals and the disruption of water, heat, and food supply, constitute a major problem. Whereas in Germany hospitals are generally well prepared with respect to shorter electricity outages due to obligatory emergency power, outpatient medical care, nursing homes, and in particular home-care nursing are affected by power supply disruptions.[3] Within industrial production sites, power blackouts may trigger significant business interruptions which lead to considerable economic losses in industrial supply chains.

(Continued on Page 19)

[1] M. Hiete and M. Merz, *Critical Infrastructure and Industrial Supply Chain*, ECN, European CIIP Newsletter, 4 (3), 24-26.
[2] A.T. Murray and T.H. Grubesic, *Critical Infrastructure - Reliability and Vulnerability*, Springer, Berlin, (2007).
[3] Hiete et al., "Scenario-based Impact Analysis of a Power Outage on Healthcare Facilities in Germany," *International Journal of Disaster Resilience in the Built Environment*, (2011, in press).

German Infrastructure *(Cont. from 18)*

Furthermore, in industry, secondary hazards might occur (e.g., the breakdown of control and cooling units may cause explosions or the release of hazardous materials).

The complexity of the interdependencies between critical infrastructure systems makes it hard to predict the potential impacts of power blackouts.[4] Therefore, within critical infrastructure protection programs, the inter-infrastructure dependencies are often neglected.[5]

In Germany, various structural changes in the energy market and shifts in the national energy policy exert considerable influence on the protection of the power supply system. The liberalization of the European electricity market since the late 1990s abolished the monopolistic structures of the German electricity market and enabled a competition among different electricity providers.[6] This resulted in reduced back-up power, making the system more vulnerable. The deregulation of the electricity market has led also to a more complex stakeholder structure. At present, in Germany, almost all critical infrastructures are operated by private companies and the total number of stakeholders in the electricity market has increased considerably.[7] Thus, not only public authorities but also a high number of private companies are now responsible for the protection of critical infrastructure systems. Furthermore, the German energy policy fostering renewable energy, influences the security of power supply as integration of renewable energies (e.g., wind energy, solar energy) will lead to a more decentralized structure of the electricity network. This involves new requirements with regard to energy storage and the transmission grid[8] as well as an increased need for balancing electricity to compensate supply fluctuations of wind and solar energy. In the end, this increases the vulnerability of the power system and may lead to an enhanced occurrence of power blackouts.[9]

Requirements for Integrated Critical Infrastructure Protection

In light of the dependency of almost all critical infrastructure systems on power supply, a well-structured risk and crisis management for power supply disruptions plays an important role within critical infrastructure protection. The main objectives of risk and crisis management should be:

- A fast *restoration of power supply* (e.g., by the implementation of emergency power systems);
- The *minimization of potential damages* in interdependent infrastructure systems (e.g., water supply, transportation, etc.) and other sectors of a society (e.g., by the implementation of organizational prevention measure and the installation of redundant systems); and
- The *protection of the population* (e.g., by providing emergency plans for medical institutions).

In order to meet these requirements and to reduce the overall impact of critical infrastructure disruptions, an integrated approach which takes into account the above mentioned conditions is needed. Thus, in the field of power supply, for the selection and implementation of appropriate prevention as well as emergency and recovery measures, a proper risk and crisis management should focus on:

(1) The identification of *inter-infrastructure dependencies* in order to evaluate, characterize, and prevent potential impacts of power blackouts, and

(2) A well-planned and structured *cooperation of public and private stakeholders* (e.g., between

(Continued on Page 20)

[4] Zhang et al., "Social Network Analysis of the Vulnerabilities of Interdependent Infrastructures, *International Journal of Critical Infrastructures*, (2008).

[5] Commission of the European Communities, Green Paper on an European Program for Critical Infrastructure Protection, Brussels, (2005).

[6] Weber, Ch., Electric Power Industry, Deregulation and Markets in Electricity Industry, Springer, (2006).

[7] Federal Office of Civil Protection and Disaster Assistance Germany, Indikatoren zur Abschätzung von Verwundbarkeit und Bewältigungspotenzialen am Beispiel von wasserbezogenen Naturgefahren in urbanen Räumen, Bonn, (2011).

[8] International Energy Agency (IEA), Wind Energy, Annual Report (2008).

[9] Erlich et al., "Advanced Grid Requirements for the Integration of Wind Turbines into the German Transmission System," IEEE International Energy Conference & Exhibition, (2006).

German Infrastructure *(Cont. from 19)*

authorities, operators, and main users of critical infrastructures).

Structured Decision Support for Risk and Crisis Management as an Example for Integrated Critical Infrastructure Protection in Germany

To support the cooperation of different stakeholders within risk and crisis management and to facilitate the selection and implementation of adequate prevention and emergency and recovery measures for critical infrastructure disruptions, structured decision support in terms of guidelines and handbooks is helpful. In Baden-Württemberg, a Federal State of Germany, the Ministry of the Interior and the Federal Office of Civil Protection and Disaster Assistance (BBK), in cooperation with an energy supplier and the Karlsruhe Institute of Technology (KIT), developed a "risk and crisis management handbook for large-area power blackouts."[10] The handbook can be used for decision support within operative and strategic risk and crisis management in the event of large-area power blackouts. Target users of the handbook are electricity suppliers and public authorities as well as affected companies (e.g., operators of other infrastructures) and social institutions (e.g., hospitals, nursing homes, etc.). The handbook consists of two parts. The first part contains background information on the power supply system, legal regulations, a description of German crisis management structures, and general information about the protection of critical infrastructures. A detailed impact analysis is depicted showing the potential consequences of different power blackout scenarios reflecting different outage durations in selected infrastructure systems and other societal sectors (health care, water supply, water disposal, industrial production, and communication). Within the second part of the handbook, checklists are provided in order to support the identification and planning of risk and crisis management measures.

The work on the handbook revealed that for a successful risk and crisis management and for the protection of other critical infrastructure systems in the event of power disruptions, prevention measures as well as emergency measures must be planned. Furthermore, it became evident that in the aftermath of a power blackout, specific recovery measures are necessary as well. Therefore, the handbook contains checklists describing measures for each risk and crisis management phase. Within the checklists of the handbook, general measures which can be implemented by all types of users as well as user-specific measures are provided (e.g., special prevention measures for water suppliers). Figure 2 gives an exemplar overview of topics covered by the checklists.

The use of the handbook within crisis management authorities on different levels showed that the handbook delivers structured support to plan and implement risk and crisis management measures for protecting critical infrastructures. Due to the

(Continued on Page 37)

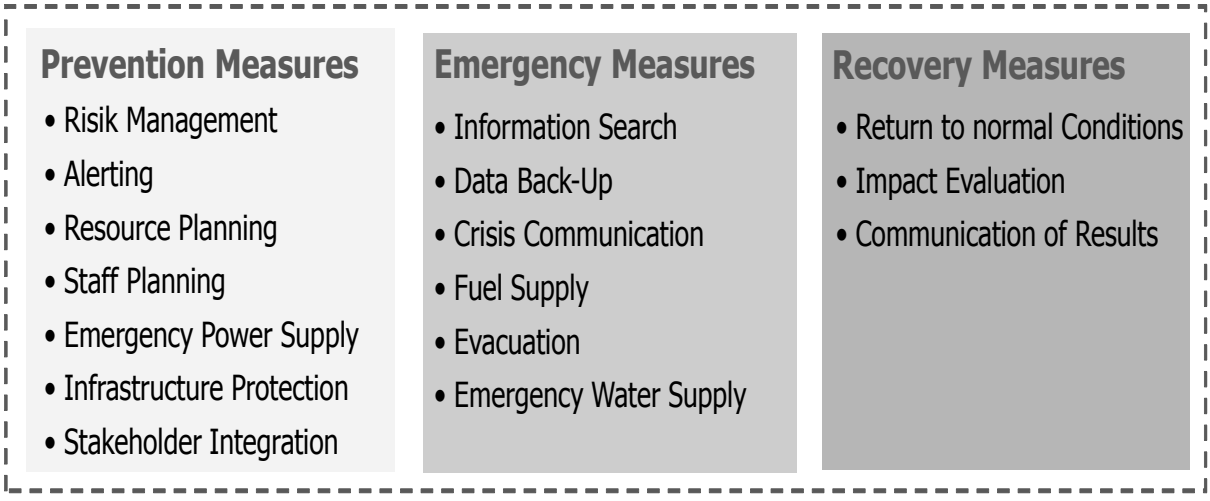


Figure 2: Crisis management measures described within the checklists of the handbook.

[10] Hiete et al, Krisenmanagment bei einer großflächigen Unterbrechung der Stromversorgung am Beispiel Baden-Württemberg, Ministry of the Interior, Federal State of Baden-Württemberg, Germany, 2010.

A New Role for Information Service Providers (ISPs) as Part of Critical Information Infrastructure Protection in Africa

by Professor SH (Basie) von Solms, Academy for Information Technology, University of Johannesburg, and Dr. Elmarie Kritzinger, School of Computing, University of South Africa

This research project investigates the role that Information Service Providers (ISPs) can play in relation to the CIIP of a country with special reference to the situation in Africa.

Introduction

More and more information technology (IT) applications are using the Internet, both from the private and public (government) environments. More and more private businesses, of which the banking industry is a prime example, are creating IT systems based on the Internet. The move to "e-Government" integrates the Internet with national public systems covering areas like emergency, health, tax, and many other citizen oriented applications.

Web based client facilities allows customers, patients, and clients to access IT systems covering the whole spectrum of daily life, via the Internet. All these IT systems form part of a country's critical information infrastructure, and by the nature of this infrastructure, it must be protected.

It is therefore crucial for the end user to be secure and protected from cyber risks because any compromise of the end user is a potential compromise to the CIIP of that country.

The Cyber Security Position in Africa

The following quote paints a bleak picture:

Africa: The Future Home of the World's Largest Botnet?

IT experts estimate an 80% infection rate on all PCs continent — wide (in Africa), including government computers. It is the cyber equivalent of a pandemic.

Few can afford to pay for anti-virus software, and for those who can, the download time on a dial-up connection makes the updates out of date by the download is complete. Now, with the arrival of broadband services delivered via undersea cables, …there will be a massive, target-rich environment of almost 100 million computers available for botnet herders to add infected hosts to their computer armies.[1]

The quote may be a little "over the top," but it highlights the type of problems going on in Africa. The aggressive roll out of mobile banking facilities in Africa to a customer base, which is not as cybersecurity aware as most developed countries, adds to these risks.

The Challenge in Africa Related to Cybersecurity and CIIP

In Africa, it is, and will continue to be, more and more difficult for end users to protect themselves by implementing proper cybersecurity measures like updated anti-virus packages and personal firewalls — not just due to cybersecurity awareness, but also because of financial reasons. Other models are therefore needed to ensure the cybersecurity awareness and technical protection of end users in Africa.

One such model is by placing more responsibilities in the Internet Service Providers (ISPs) in Africa.

Information Service Providers (ISPs)

ISPs come in many forms and sizes, but basically they all have one thing in common — *they are gatekeepers to the Internet.*[2] It therefore seems logical that any model for end user awareness, security, and CIIP

(Continued on Page 22)

[1] Jeffrey Carr, *Inside Cyber Warefare*, O'Reilly Media, Inc. (December 23, 2009).

[2] BCS, The Chartered Institute for IT (formerly known as British Computer Society), *What Future for Internet Service Providers?* 2009, available at http://www.bcs.org/server.php?show=ConWebDoc.24111.

ISPs and Africa *(Cont. from 21)*

involving the Internet should involve ISPs.

This notion is not new. In 2008, the Controller of the Communications Authority in Zambia urged ISPs to "protect their customers from fraud and thefts that may arise as a result of sharing personal information online."[3] Or, as Clarke et al. states, "ISPs should be required to do more to keep our nation's portion of the cyber ecosystem clean."[4]

From Thin ISPs to Thick ISPs (or from Thick End Users to Thin End Users)

In an active research project, this approach is being investigated and a prototype is being developed. The prototype will basically perform two major functions:

Function 1: The ISP will enforce a level of cybersecurity awareness by forcing end users to first complete an Internet Security Driver's License test and exam. Only after successfully passing this course, will a user be given access to the Internet. This model is fully described in Kritzinger et al, 2010.[5]

Function 2: The ISP will be responsible for most, if not all, security mechanisms needed to prevent malicious software infection. Such mechanisms include anti-virus checking, checking for phishing attacks, killing hosted phishing sites, etc. This function is fully described in Kritzinger et al, 2011.[6]

The idea is therefore that the "new" type of ISP will ensure that the end user is information security aware, and then move the security responsibility away from the end user, who is actually not in a position to handle such responsibility anyway. As Schneier wrote, "[i]t's unrealistic to expect home users to be responsible for their own security. They don't have the expertise, and they're not going to learn."[7]

The proof-of-concept prototype is being developed as a post-graduate project, and it is envisaged that it will be operational by the last part of 2011.[8] The idea is to change the situation for the "thick" end user to a "thin end user" — in the process changing the ISP from "thin" to "thick." This is illustrated in Figure 1 (below) and Figure 2 (on Page 34).

Evaluation and Summary

The proposed new model for "African ISPs" will field a lot of criticism, including a decrease in reaction time, extra resources at the ISP, legal consequences, etc. Of course all such criticisms are valid, but if a country is serious to protect its citizens as well as its own critical infrastructure, it will need different options to implement, and the "new" ISP model can be one such option. ❖

Professor SH (Basie) von Solms can be contacted at the Academy for Information Technology, University of Johannesburg, Johannesburg, South Africa at basievs@uj.ac.za. Dr.

(Continued on Page 34)

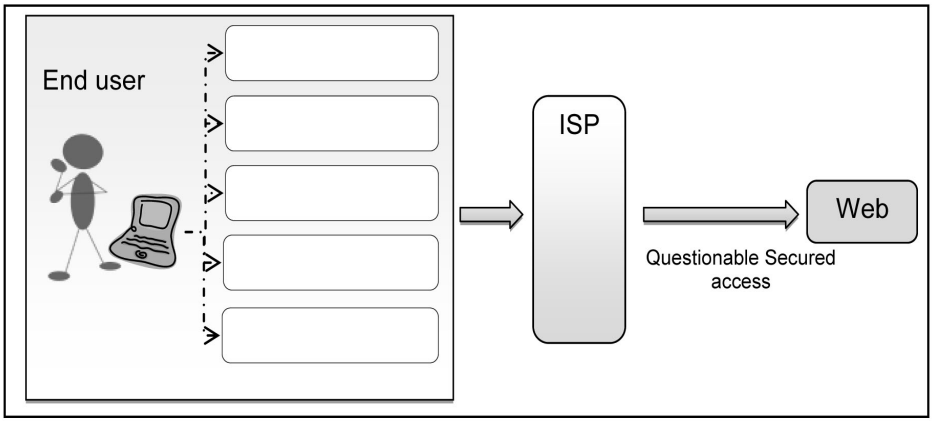


Figure 1: Thick End User/Thin ISP.

[3] Lusaka Times, Internet Services Providers Urged to Fight Cyber Crime, (2009), available at http://www.lusakatimes.com/?p=7049.
[4] R.A. Clarke and R.K. Knake, *Cyber War – The Next Threat to National Security and What to do About It*, HarperCollins, (2010).
[5] E. Kritzinger and S.H. von Solms, "Cyber Security for Home Users: A New Way of Protection through Awareness Enforcement," *Computers & Security* 29 (2010), 840-847.
[6] E. Kritzinger and S.H. von Solms, *Thick, Intermediate and Thin Information Security Home Users*, In preparation,' (2011).
[7] B. Schneier, *Home Users: A Public Health Problem?* Schneier on Security blog entry written on September 14, 2007, http://www.schneier.com/blog/archives/2007/09/.
[8] S.H. von Solms and J. Roussel, *An ISP for African Cyber Security*, In Development, (2011).

The Swiss Programme on Critical Infrastructure Protection

by Stefan Brem, Head of Risk Analysis and Research Coordination,
Federal Department of Defence, Civil Protection and Sport
Federal Office for Civil Protection, Policy Division

As other modern societies, Switzerland is highly dependent on the continuous operation of critical infrastructures that ensure the supply of crucial goods and services. Disruptions may have rapid repercussions for the population and the basis of its livelihood and can affect other critical infrastructures through domino effects. For instance, a large scale power blackout will also disrupt the water supply, telecommunications, and rail transport. The overarching goal of the Swiss Programme on CIP is therefore to maintain the operability of these critical infrastructures.

At the national level, Switzerland identified ten critical sectors, including energy, transport, and financial services. They are further divided into 28 sub-sectors, such as power, oil, and natural gas supply within the energy sector. Advanced protection measures are already in place for some individual sub-sectors. However, for a long time, cross-sectoral coordination and a consolidated approach at the national level were lacking. Therefore, in June 2005, the Federal Council — Switzerland's Federal cabinet – mandated the Federal Office of Civil Protection (FOCP) to co-ordinate efforts in the area of CIP and to establish a CIP Working Group (CIP WG) in which all relevant Federal authorities and two cantonal representatives are brought together.

The CIP WG subsequently submitted a report to the Federal Council in July 2007 in which it defined the most important terms, identified the (sub-)sectors considered to be critical for Switzerland, and determined the next steps. The Federal Council approved this report as well as a number of projects as a basis for the elaboration of a national CIP strategy. Based on the project insights, the CIP WG drafted a Basic CIP Strategy that serves as a framework for the future national strategy. Among other things, it outlined the strategic goals as well as the relevant principles. It also described four specific implementation measures (described below) within the CIP Programme. The Federal Council approved the Basic CIP Strategy on 5 June 2009, while simultaneously endorsing a second report that provided information on the state of work in the various projects and the achieved results.

Measures for Critical Infrastructure Protection

In the Swiss CIP Programme, the following four measures are currently being implemented according to the Federal Council's Basic CIP Strategy:

1. Prioritizing Critical Infrastructures: In order to be able to use resources efficiently, critical infrastructures must be prioritized. The Swiss CIP Programme covers ten critical sectors that are grouped into 28 sub-sectors. The 28 sub-sectors are weighted for criticality and categorized into three groups (see table on page 25). Furthermore, individual critical infrastructure elements are identified based on a standardized method and uniform assessment. A "CIP Inventory" with critical infrastructures of national importance is compiled and regularly updated in cooperation with the responsible authorities of the Federal administration, the Cantons, and the operators. The classified inventory mainly serves as a basis for planning and decision-making processes at the various administrative levels and the critical infrastructure facility.

2. Protection through Comprehensive Approaches: Critical infrastructures are protected through comprehensive concepts that include specifications as to protection goals, protective measures, and implementation

(Continued on Page 24)

Swiss CIP *(Cont. from 23)*

plans. The specific protective measures are oriented towards a comprehensive risk spectrum and take into account various aspects of the entire risk management cycle. The protection concepts relate to critical sectors as well as the infrastructure elements of national significance that are listed in the CIP Inventory. They complement the existing protection concepts in the critical sub-sectors. The development of protection concepts follows a standardized process. Initially, the existing responsibilities and regulations are reviewed, and protection goals are defined. In the next step, an in-depth analysis of threats and vulnerabilities is conducted. Subsequently, the risk analysis and the existing regulations are taken as the baseline to verify whether the protection goals have been achieved. If not, appropriate measures are elaborated. Finally, political decision-makers must determine which of these measures are to be implemented. Once the measures have been implemented, they will be reviewed to assess whether the protection goals have been met or further adjustments are required. This entire process is repeated periodically.

3. Establishing Research Foundations: Basic research in the field of CIP is of great importance as many challenges such as mutual dependencies and cascading effects in case of disruption still need additional investigation. This also supports the formulation of comprehensive and concerted countermeasures. In the area of basic research, close cooperation with various research institutes, such as Switzerland's universities, is important. Another significant feature is the exchange with the international research community.

4. Fostering Risk Communication: Awareness of the significance of critical infrastructures and the possible implications of failures as well as countermeasures is crucial. Therefore, risk communication directed to work operators of critical infrastructures, corporate actors, representatives of different administrative levels, and the general public covers possible risks and threats in connection with critical infrastructures as well as rules of conduct and ways of protecting themselves. This is done in various ways, including fact sheets and the CIP website (www.infraprotection.ch), which also provides information about the CIP Programme in general, upcoming CIP events, and CIP-related news and publications.

Expanding the Basic Strategy into a National CIP Strategy

The Basic CIP Strategy will be

(Continued on Page 25)

Glossary

Infrastructures
This is a general term which refers to facilities and organisations, which deliver goods and services to society, the economy and the state.
The infrastructures are classified in three levels:
- Sectors: e.g. energy, financial services, public health
- Sub-sectors: e.g. power supply, oil supply, natural gas supply
- Individual objects/elements: e.g. pumps, pipelines, dams, high-voltage lines, control systems

Critical infrastructures
Critical infrastructures are infrastructures whose disruption, failure or destruction would have a serious impact on the functioning of society, the economy or the state.

Critical Infrastructure Protection
The goal of critical infrastructure protection is to reduce the likelihood of occurrence and the impact of a disruption, failure or destruction of critical infrastructure and to minimise downtime.

Swiss CIP *(Cont. from 24)*

Sectors	Sub-sectors
Energy	Natural Gas Supply
	Oil Supply
	Power Supply
Financial Services	Banks
	Insurance
Information- & Communication Technology (ICT)	Information Technology
	Media
	Telecommunication
Industry	Chemical and Pharmaceutical Industry
	Mechanical and Electrical Engineering Industries
Public Administration	Foreign Representations and Headquarters of International Organizations
	Cultural Property
	Parliament, Government, Justice, Administration
	Research Institutes
Public Health	Medical Care and Hospitals
	Laboratories
Public Safety	Armed Forces
	Civil Defense
	Emergency Organisations (Police, Fire Service, Emergency Medical Service and Rescue Services)
Transport	Air Transport
	Water Transport
	Postal Services
	Rail Transport
	Road Transport
Water and Food	Food Supply
	Drinking Water Supply
Waste disposal	Waste
	Wastewater

	Very high criticality
	High criticality
	Regular criticality

General Framework

→ All sub-sectors are critical.
→ Criticality refers to the importance of the sub-sector in terms of interdependency, the population, and the economy (not its general importance or its mission-criticality).
→ Even sub-sectors whose criticality is regular may contain highly critical individual elements.
→ Weighting is based on an ordinary threat level.

Contact
Federal Office for Civil Protection FOCP
Monbijoustrasse 51A
CH-3003 Bern
www.infraprotection.ch
ski@babs.admin.ch

November 2010 (update May 2011) Pictures: FOCP, News services

(Continued on Page 36)

Nuclear Infrastructure Implications of the Fukushima Event

by Dwight E. Baker, PE*

The subsea earthquake which occurred on March 11, 2011 was rated at about 9 on the Richter Scale, substantially in excess of the design basis earthquake for the Fukushima site. This caused all operating units to trip, and also caused a failure of the power grid in northern Japan. All onsite emergency diesel generators started and provided power for the emergency cooling systems for about an hour, when the 46 foot high tsunami arrived at the site. This substantially exceeded the site design basis tsunami of about 21 feet. Since the diesels and electric switchgear were located in the basement for earthquake resistance, they were quickly flooded and only battery power remained available to some Direct Current (DC) busses.

After about eight hours, the batteries became exhausted and all cooling was lost, resulting in the reactor cores overheating. After power was lost, boil off in the open spent fuel pools may have uncovered the fuel assemblies stored there. Unit 4, which included a full core offloaded for maintenance about 100 days earlier, would likely have become uncovered first. In subsequent days, all four units underwent varying degrees of fuel clad oxidation (which produces hydrogen gas), melting of the uranium dioxide fuel elements, and zirconium fires in the spent fuel pools. Hydrogen explosions occurred at three of the four units that extensively damaged the exterior of the reactor buildings, and the other unit likely experienced a hydrogen explosion inside containment.

In many ways, this event points out the inherent safety of light water reactor technology. Even with extensive core damage and loss of containment due to venting steam or burning spent fuel cladding in the exposed pools, there is adequate time available for modest emergency response actions to minimize or even totally avoid radiation casualties. This "slow motion" feature of accident progression results from the fundamental chemical and physical properties of the materials of construction and their geometry, which places limits on accident consequences regardless of procedures or operator actions. This contrasts favorably with many other types of energy facilities, which tend to produce large explosions, fires, and mass casualties in a matter of seconds after an event.

Although some earlier media coverage indicated deaths from radiation were expected, the best information at the time of this article indicates a maximum worker dose of about 17 roentgen equivalent man (rem), well below the 25 rem emergency dose limit, or 600-1000 rem where fatalities are expected. The response from most world governments and the public has been notably measured. Even at this early stage, many people recognize these are among the earliest nuclear plant designs and they did not have some modifications that have been implemented elsewhere that might have helped mitigate the event. It is also widely recognized that all power sources have risks, and this event does not demonstrate any previously unknown phenomena. The safety regulator defines event magnitudes or environmental limits within which the owner must demonstrate acceptable performance in order to reduce and manage risk. Outside these limits, the risk is assumed by the public. The Fukushima event demonstrates that it is in the best interest of all concerned that plans and procedures not stop at the defined regulatory limits. The best analysis limit for high hazard facilities, especially where rare natural phenomena are concerned, may be damage so extensive that there is no one left alive within the area that might be affected by the facility in question. There may be events on this scale outside regulatory requirements but short of total destruction. In these situations,

(Continued on Page 35)

Legal Insights

U.S. International Security Policy: Not Always Waiting for Law to Catch-Up

by Jeremy Rabkin, Professor of Law
George Mason University

On May 1, the White House announced that Navy SEALs had raided the Pakistani hide-out of Osama bin Laden and killed the terrorist mastermind. Less than three weeks later, the White House released its "International Strategy for Cyberspace."

Both events reflect a common premise: that in today's world, what happens in obscure places, half way around the world, can have direct implications for the safety of Americans in the United States. Furthermore, both reflect a common response: the United States, while welcoming international cooperation, will sometimes act in advance of a formal or universal international understanding of what security measures are currently lawful.

Pakistani officials protested the raid on Osama's hide-out as a violation of their sovereignty. U.S. officials defended the raid as a lawful extension of the war in Afghanistan, but acknowledged that the normal international rule — respecting the exclusive authority of national governments in their own territory — would normally require the United States to seek local consent before sending a raiding force into a third country. Still, Obama administration officials insisted that in the proper circumstances (left unspecified), the United States might feel justified in resorting to a similar raid of this kind.

Cyber attacks may seem an altogether different category of threat than Al Qaeda bombings. But, a sufficiently well executed cyber attack might prove more devastating than any conventional explosive. An effective, large-scale cyber attack on the U.S. air traffic control system might trigger plane crashes and the grounding of all air traffic for some time thereafter. An effective cyber attack on the American banking system, or some crucial central component of it, could paralyze the economy.

There remains the difference. Tracing the ultimate source of a cyber attack may be much more difficult than tracking the human agents in a bomb plot. The cyber attack might be effectuated through network connections running many different countries, without ever stopping for passport checks or leaving DNA samples. Therefore, a number of advocates have urged the world to formulate a new cyber-treaty, clarifying the rights and obligations of states in dealing with such threats.

The first notable point about the new cyberspace strategy is that it does not call for a new treaty or even a world-wide conference to begin negotiating such agreed upon ground rules. One obvious reason for the reticence is evident on the face of the document. The Strategy embraces American support for "fundamental freedoms of expression and association, online as well as off." So the United States supports "an Internet accessible to all" through "end-to-end interoperability." This is not the preference of all countries.

China already goes to great lengths to screen what ordinary Chinese can see on the Internet. In Egypt, earlier this year, the Mubarak government tried to shut down the Internet altogether (within Egypt) to hinder the mobilization of anti-government protests. Protesters managed to communicate anyway, using cell-phone connections to foreign sites. In the end, Mubarak was forced from power. American policy (and the practice of many private entities operating in the United States) is to help local dissidents. Repressive governments around the world, fearing threats from wired protest movements,

(Continued on Page 28)

Legal Insights *(Cont. from 27)*

will seek international support for their efforts to control Internet usage in their own countries. In today's world, efforts to negotiate a comprehensive international treaty would generate many rules the United States could not support.

The deeper problem is similar to the problem posed by the raid against Osama bin Laden's lair in Pakistan. The United States is not prepared to commit to precise limits on its capacity to respond to a cyber-attack. The most serious attack would probably be organized by a hostile state, with the resources to develop a particularly insidious virus or to strike simultaneously throughout a large system. But, a hostile power might operate through intermediaries in other countries, with or without the knowledge of governments in these countries. The Strategy announces that the United States "reserves the right to use all necessary means … to defend our Nation, our allies, our partners and our interests." It promises to "exhaust all options before military force *whenever we can*" and to seek "broad international support *whenever possible*" [emphasis added]. However, it does little to clarify what conditions would justify exceptions implied by those "whenever" clauses.

So instead of precise rules, the Strategy emphasizes American hopes to "establish an environment of expectations, or norms of behavior, that ground foreign and defense policies and guide international partnerships." The one international treaty which the Strategy mentions is the 2001 Budapest Convention on Cybercrime. The Convention encourages international cooperation in tracking down cyber-offenders and providing parallel criminal standards to facilitate extradition or reliable national action on transnational offenders.

But only 30 countries have ratified the Budapest Convention to date. Apart from the United States, all the other parties are members of the Council of Europe. The Council of Europe is already accustomed to harmonizing their laws with each other. Less developed countries may be far less eager to embrace the Convention's provisions on copyright protection and suppression of "racist" or "xenophobic" expression. So the Strategy talks of "encourag[ing] … current non-parties [to] use the Convention as a basis for their own law … preparing them for the possibility of accession to the Convention in the long term." In short, the United States will use the Budapest Convention to promote developing "norms" in this area, which can be used "to investigate and prosecute terrorist and other criminal misuse of the Internet."

Current efforts to deal with threats from cyberspace might be usefully compared with efforts, launched after 9/11, to deal with threats from ocean commerce. The United States worked through the International Maritime Organization (IMO) to develop new international standards, the International Port and Ship Facility Security Code, which went into effect in 2004. It eventually received the support of over 100 countries in the IMO. But, the code seeks to standardize precautions against terror attacks on shipping. It does not prescribe or authorize responses when the precautions are not maintained or when they fail.

During the same years, the United States also launched a parallel U.S. policy — the Container Security Initiative (CSI), by which seaborne containers can be inspected by U.S. officials in foreign ports. It allows the United States to stop suspicious cargoes before they enter an American port. Apart from European Union states, only a dozen or so other countries have negotiated bilateral agreements with the United States under CSI, but those countries provide the largest share of container shipping into American ports. Containers shipped from other countries will likely be searched more carefully when they arrive.

More controversially, the United States launched the Proliferation Security Initiative (PSI) in 2003, with the aim of mobilizing cooperation to stop shipment of weapons of mass destruction to unauthorized parties. Over 90 nations have expressed general support for the aims of PSI but only nine have signed bilateral agreements authorizing U.S. high seas interdiction and inspection of their ships on the high seas. These nine include major flaggers of convenience (Panama, Belize, Liberia, Cyprus) — countries that open their national registries to

(Continued on Page 34)

Developing Countries *(Cont. from 12)*

can be expanded to produce an effective "bottom-up" model to operate alongside the traditional "top-down" approach.

A potential construct for addressing this notion of communities is a Community-Oriented Security, Advisory, and Warning (C-SAW) Team.[9] This model derives from a CSIRT, but is designed around the idea of protecting a medium-sized, related community of members. A C-SAW is able to interface between a community and a CSIRT; however. it is not subordinate to a CSIRT. It should be considered an equal partner in the structure, and thereby bridging the gap between a "top-down" CSIRT and the small-stakeholder.

Due to the focused nature of a C-SAW, and the relationship with a community, the C-SAW is able to directly address the risk factors mentioned above. In order to gain the maximum benefit of C-SAW structure, many C-SAW Teams can be deployed to create a "net of protection" in a wider CIIP structure. Further research into the organisational structure of a C-SAW, its role, and responsibilities is on going.

Conclusions

The development of CIIP structures in developing countries is essential to address the growing needs in these countries. The future role of developing nations cannot be overlooked, and countries are beginning to realise this. With the amount of available bandwidth and the number of connected users growing steadily, developing nations could potentially have a dramatic effect on the nature of the Internet.

However, the structures required to address this rapid expansion are not simple to realise. There are a number of limitations that are specific to developing countries that prevent existing platforms from being directly imported. Structures have to be specifically tailored to operate in an environment different from what has been experienced before.

In order to address the set of requirements, a comprehensive CIIP structure must be developed. This structure must be able to address the needs of the developing country. A potential solution is to create structures to address the needs of related communities. Each community is then able contribute to a holistic CIIP structure. However, it is a matter of dedication from all stakeholders to ensure that developing countries create effective protection structures that will allow them to continue to play a part in an increasingly interconnected world. ❖

ID Ellefsen and Professor SH von Solms may be contacted at the Academy for Information Technology, University of Johannesburg, Johannesburg, South Africa at iellefsen@uj.ac.za and basievs@uj.ac.za.

[9] I.D Ellefsen and S.H von Solms, "C-SAW: Critical Information Infrastructure Protection through Simplification in What Kind of Information Society? Governance, Virtuality, Surveillance, Sustainability, Resilience," IFIP, Advances in Information and Communication Technology, (328) 315–325. Springer Boston, (2010). doi: 10.1007/978-3-642-15479-9 30. http://dx.doi.org/10.1007/978-3-642-15479-9_30.

Good Practices *(Cont. from 14)*

performing a quantitative analysis. The qualitative approach is, for instance, used by Sweden to map the dependencies of their critical societal functions.

The third theme, "public-private partnership," discusses the range of PPP governance models for CIP. It outlines the critical factors for their success: trust, respect, transparency, clear framework, neutrality, common interest, realistic expectations, and understanding each capabilities and limitations. Various PPP models are discussed from a loose organizational structure to mandatory required co-operation. Four good practices were identified: (1) a strategic CIP Board; (2) common funding for CIP measures (which eases the willingness to partner in a PPP); (3) compelling co-operation; and (4) attaining voluntary co-operation of the private sector through the provision of CIP expertise by the government. Examples of the latter are the fusing of threat information by a government agency and providing that to the critical infrastructure sectors or selected critical infrastructure operators.

The fourth theme, "information sharing," discusses the need for sharing information to improve the protection of critical infrastructure. This includes information about threats, vulnerabilities, risk factors, measures, good practices, incident data, and "weak signals." Before information sharing takes place, relationships based on trust have to be built and secured and trusted ways of handling classified and/or sensitive information need to be established. Four good practices were identified: (1) building (small) trust communities; (2) the Traffic Light Protocol (TLP); (3) electronic information exchange; and (4) cross-border information sharing.

The fifth theme, "risk management," discusses the need for risk management as part of CIP. The difference with normal risk management is that there is a need to aggregate the outcomes of risk management, including the assessment of critical infrastructure dependencies at the company level to the critical infrastructure sector level, and to the national or even multinational level. The three risk management good practices are: (1) risk management guidelines and tools; (2) enforced risk management; and (3) national risk assessment (NRA).

The last theme, "crisis management," discusses why it is important that crisis and emergency management authorities and their processes take care of critical infrastructures during an incident or emergency. Issues concerning the smooth co-operation of emergency management structures with critical infrastructure operators include: clear responsibilities, mutual benefits, understanding each other's professional jargon, joint exercises, and limiting the freedom of information act with respect to sensitive private company data handed over to government agencies as part of addressing an emergency.

Four good practices were identified: (1) crisis management legislation in relationship to critical infrastructure sectors and critical infrastructure operators; (2) CIP expertise being a support function to crisis management; (3) joint PPP exercises with critical infrastructure operators; and (4) critical infrastructure sector embedding in the national and regional crisis management structures. With respect to CIP expertise as a support function to crisis management, the RECIPE manual points to the U.S. Department of Homeland Security Homeland Infrastructure Threat and Risk Analysis Center (HITRAC) and the Australian Critical Infrastructure Program for Modelling and Analysis (CIPMA) functionality. These examples clearly show that the RECIPE team used a broad view to locate good practices.

To conclude, the RECIPE project team is convinced that the manual will be a great help to both the novice CIP policy-maker and the CIP policy-makers more experienced in one or more of the six key CIP themes. Using and adapting these good practices for one's own national CIP approach may avoid the pitfalls previously identified by other nations. This allows nations to quickly catch-up with the CIP front-runner nations. ❖

Eric Luiijf, Marieke Klaver, and Albert Nieuwenhuijs can be contacted at P.O. Box 96864, The Hague, The Netherlands at {eric.luiijf,marieke.klaver,albert.nieuwenhuijs}@tno.nl.

Japanese Infrastructure *(Cont. from 17)*

five percent survival rate for a population that would not have evacuated. There are limits to what society can do to prevent damage in regions subject to large tsunamis. However, tsunami warnings and evacuation systems with conservative tsunami evacuation zones can significantly improve public safety, and the experience in Japan should be considered successful given the unprecedented height of the Tohoku Tsunami.

For more information, please visit: http://www.asce.org/Headlines/ASCE-Assessment-Teams-Travel-to-Japan/. ❖

Devastated Tarou town behind failed seawall in Iwate Prefecture. *Photo courtesy of Ian Robertson.*

Global Interdependencies *(Cont. from 4)*

disruptive events, the Japanese government was stretched to ensure all aspects were addressed. Japan's most powerful business group, the Kidanren, claimed the government has been focused on the nuclear disaster and been too slow to move to recovery mode.[8] Yet many organisations survived and thrived. While many individuals and communities were in a state of shock, there were countless accounts of people rallying to help others. This is a familiar story. Charities, such as Save the Children, which has been working in Japan for 25 years, acted quickly to establish multiple child-friendly spaces in evacuation centres in Sendai City for displaced families. Child-friendly spaces provide children with an opportunity to play with other children, freeing up parents to work on the recovery and to provide respite as well as a sense of normality for the children. In the Queensland floods in Australia, masses of volunteers emerged to help with the clean-up. The Queensland State Government acted as a broker to bring together businesses with communities. Local councils and clubs partnered to restore services. These implicit interdependencies are starting to be explicitly recognised as part of a necessary public debate about how nations can increase resilience to such non-traditional security threats. ❖

[8] K. Snowdon, *Business Recovery 'Too Slow' in Devastated Japan*, ABC News, www.abcnews.com.au (April 14, 2011).

Infrastructure Planning *(Cont. from 7)*

From the foregoing, we conclude that uncertainty is a central problem in long-term infrastructure planning. A large body of literature exists that argues that in order to handle these uncertainties, infrastructure planning needs to shift from the static rigid policy-making paradigm to the dynamic adaptive policy-making paradigm. One possible approach is DAP, which offers clear structure and tools for thinking about and evaluating uncertainties and making explicit trade-offs. While we may not be able to foresee all of the consequences of an uncertain future, dynamic adaptation offers a way to protect ourselves from nasty surprises and unforeseen contingencies, and to begin to implement a policy to address the problem right away.

DAP helps to develop more robust plans by accepting uncertainty and acknowledging that we cannot predict the future (even probabilistically). The approach calls for implementing a basic policy based on what we know today, and constructing a system for monitoring the (unpredictable) developments that could impact the effectiveness of the chosen policy. The resulting policy is dynamic; the element of time and the possibility of learning are explicitly taken into account by the policy. Whereas other approaches are based on the notion that policy-making is a discrete one-time event and that the resulting policy is static, dynamic adaptation is explicitly defined as a continuous process in time that involves monitoring and making pre-specified changes to existing policy in response to unforeseen developments.

DAP has not yet been implemented in practice. More research is required before this will happen. First, its validity and efficacy needs to be established. This will be difficult to do since, as Dewar et al. have pointed out, "nothing done in the short term can 'prove' the efficacy of a planning methodology; nor can the monitoring, over time, of a single instance of a plan generated by that methodology, unless there is a competing parallel plan."[14] Nevertheless, evidence is being gathered through a variety of methods, including gaming and computational experiments (see, for example, Kwakkel, et al., forthcoming).[15] Also, the costs and benefits of dynamic adaptation measures compared to traditional policy-making approaches need to be studied. Finally, the implementation of dynamic adaptation will require significant institutional/governance changes, since some aspects of these policies are currently not supported by laws and regulations (e.g., the implementation of a policy triggered by an external event). Lempert and Light provide some suggestions about a governmental framework at the national level in the United States that could support the implementation of this type policymaking.[16]

Nevertheless, the DAP framework offers several advantages over other approaches. Most important of these are (1) it does not ignore uncertainty; it acknowledges that we cannot know the future and bases policy on this assumption, and (2) it institutionalizes the process of ex-post policy evaluation and monitoring. As Nassim Nicholas Taleb has written: "it is often said that 'is wise he who can see things coming.' Perhaps the wise one is the one who knows that he cannot see things far away."[17] ❖

[14] Dewar et al., *Assumption-Based Planning: A Planning Tool for Very Uncertain Times*, RAND, (1993).
[15] Kwakkel et al, "Assessing the Efficacy of Adaptive Planning of Infrastructure: Results From Computational Experiments," *Environment and Planning B,* (forthcoming).
[16] R.J. Lempert and P.C. Light, "Evaluating and Implementing Long-Term Decisions," in *Shaping Tomorrow Today: Near-Term Steps Towards Long-Term Goals*, RAND, (2009).
[17] Nassim Nicholas Taleb, *The Black Swan: The Impact of the Highly Improbable*, (2007).

Innovative Policies *(Cont. from 8)*

long before the term gained currency in the field of CIP.

There are several other examples for policy transfers from other areas. Since CIP is a relatively new field of public policy, concepts and ideas are frequently adopted from other areas. The advantage of such policy transfers is that the concepts and approaches are already well established given that they have been discussed in other areas, and are therefore easy to understand. This advantage also explains why such concepts often spread very quickly. The term "resilience," for example, was almost unheard of in connection with CIP only a few years ago, but today, it is omnipresent. This rapid adoption was due to the widespread use of the concept in other fields. Furthermore, it is less risky to implement policies that have proven to be effective in other areas. Policy-makers can refer to the examples in other areas to highlight the benefits of the solution they are advocating, and they can profit from experiences made by other actors.

Perils of Policy Learning and Policy Transfers

Undoubtedly, mutual learning and policy transfers are very profitable sources for policy innovations in CIP. They help policy-makers recognize new challenges and adopt and implement new protection policies in a timely manner. However, neither policy learning nor policy transfers are entirely unproblematic. First, policy-makers may be overzealous in adopting the substance of other country's policies and neglect to take into account the specificities of their own country. CIP policies must be embedded in the broader societal, political, and economic context. These contexts can be highly diverse across different countries. The levels of risk that societies are willing to accept and the expectations that the general public has of the government differ across countries. In addition, the level of privatization of critical infrastructures and the degree of economic freedom determine which models of public-private collaboration make sense. If CIP policies are not adjusted to the specific circumstances of the country in question, they are likely to fail.

Second, the transfer of concepts from other policy areas to CIP may give rise to false expectations. Again, this can be highlighted with the example of the use of the label "public-private partnership" (PPP) for CIP. Most PPPs in this field cannot be compared to the PPPs that are created for the financing of buildings or infrastructures. Unlike these PPPs, partnerships in CIP are usually not contract-based, but are characterized by the need for constant dialog. This form of collaboration is much more demanding, and it is misleading to compare the effectiveness of PPPs for CIP with PPPs for the building and maintenance of infrastructures. However, since both forms of partnerships use the same label, this comparison is all too often made.

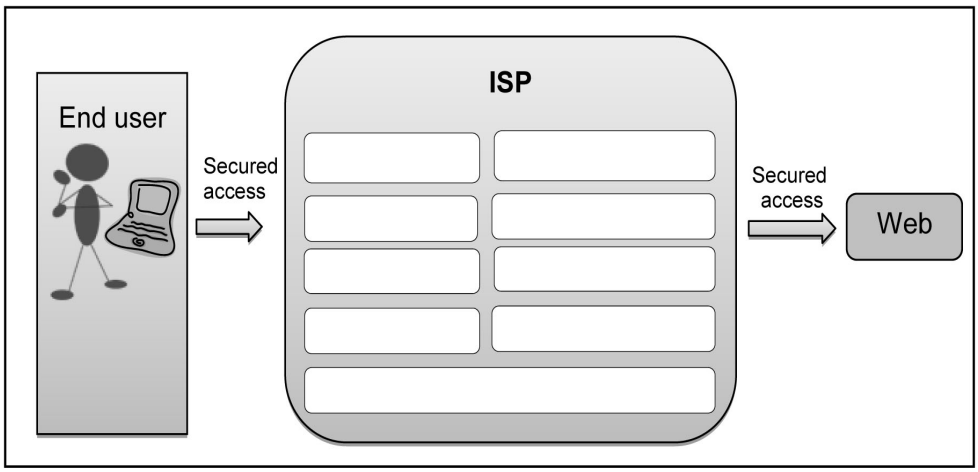
Conclusions

In order to understand how CIP policies are developed and to assess their quality, it is important to know where the concepts and approaches used in these policies are emanating. Innovative policy-makers will always strive to learn from the experiences of other actors, be they CIP experts from other countries or policy-makers in other areas. Such innovations are essential for successful CIP policies. Progress in CIP can only be made if policy-makers continue to look for concepts and solutions to describe new problems and deal with current challenges. Nevertheless, it has also been shown that it is important to be judicious when adopting ideas for CIP. Policy innovations can only be successful if they are adapted to the specific contexts of a country and the specific features of CIP in general. ❖

ISPs and Africa *(Cont. from 22)*

Elmarie Kritzinger can be contacted at the School of Computing, University of South Africa, Pretoria, South Africa at kritze@unisa,ac.za.

Figure 2: Thin end user/Thick ISP



Legal Insights *(Cont. from 28)*

foreign commercial vessels. Others might be brought along to accept a less formal "norm" of high seas interdiction in special circumstances.

Fearing this development, major countries, notably including China and Indonesia, have denounced PSI as a threat to freedom of the seas, which is enshrined in the 1982 United Nations Convention on the Law of the Sea. The United States has endorsed almost all provisions of that treaty — in its understanding of them. It has not formally ratified the treaty, partly from concerns about its provisions for mandatory international arbitration of disputes over shipping rights.

In cyberspace, as on the high seas, the United States seeks to protect an open environment and therefore seeks legal standards supporting open exchange — as much as possible. American security policy seeks to expand international agreements, when feasible, to promote less formal understandings as a fall-back. But, as a last resort, still reserves American claims to operate independently. ❖

Nuclear Infrastructure *(Cont. from 26)*

small investments in backup equipment and procedures can make a big difference in consequences. Such investments can often be justified as prudent risk management even in the absence of regulatory requirements.

To some extent after the Three Mile Island event in 1979, and even more so after the events of September11, 2001, the U.S. nuclear industry has implemented measures to deal with such "beyond design basis" events. This probably explains the U.S. government's measured response to the Fukushima event, since the results of a similar natural event at a U.S. plant of similar vintage would likely be much less severe. Other infrastructure sectors should not wait for a similar high consequence event to consider how this type of resilience might benefit them.

With the exception of one planned new reactor project (which was being partly funded by Japanese entities impacted by this event), there have not been any announced delays or cancellations of new nuclear plants in the United States subsequent to the Fukushima event. The temporary shutdown of seven older reactors in Germany appears to be the most significant governmental action taken to date. Based on the statements that have been made recently by world business and political leaders, the most likely outcome may be a relatively brief pause in some construction programs while the investigation of the event details occur and lessons learned are applied to the new designs, if needed. A few of the oldest plants may be decommissioned if the remaining life is short and needed upgrades are too expensive.

Most likely, modifications to the current new nuclear plant designs, or even those completed in the United States in the 1980s, will be relatively minor. There will likely be increased interest in the advanced "inherently safe" designs. There may yet be some good ideas on how to mitigate extreme events that can be identified and shared. In the United States, the Critical Infrastructure Protection Advisory Council (CIPAC) appears to be an excellent forum for sharing information on such measures and exploring consensus on the most efficient division of labor between industry and government. ❖

Mr. Baker is a Lead Operations Analyst at the MITRE Corporation He has BS and ME Degrees in Electrical Engineering from the University of Virginia and held a Senior Reactor Operator License on a large commercial nuclear power plant for six years. He is a licensed Professional Engineer in Mississippi and Virginia. The author's affiliation with The MITRE Corporation is provided for identification purposes only, and is not intended to convey or imply MITRE's concurrence with, or support for, the positions, opinions or viewpoints expressed by the author.

Swiss CIP *(Cont. from 24)*

expanded into a national CIP Strategy by the end of 2011. To this end, the definitions, principles, and measures of the Basic Strategy will be reviewed and adapted where necessary.

The focus will be on the following activities:

- advancement of definitions, principles, and measures listed in the Basic Strategy;
- definition of responsibilities and organisational structure;
- arrangements for funding the implementation of the measures;
- evaluation of the legal foundations of the national CIP strategy; and
- elaboration of instruments for evaluating the national CIP strategy.

Within the implementation of the measures, the optimization of information sharing between the Federal authorities, the Cantons, and the operators of critical infrastructures is crucial. Moreover, the strategy provides inputs on how the protection of critical objects on the national level as listed in the CIP Inventory can be improved. In addition to the development of comprehensive protection concepts, the CIP Programme focuses on the optimization of processes, which will allow the prioritization of national critical infrastructures.

The Sectors and Sub-sectors of Critical Infrastructure

Originally, the Basic CIP Strategy of 2009 identified 31 sub-sectors within ten sectors that are identified as critical national importance. The methodology to assess the criticality includes the damage to be expected from a failure of the critical sub-sectors, which is determined by the effects on other critical sub-sectors (interdependencies), on the population, and on the economy. As a preparation to the actual identification of the individual critical elements and objects, the classification has been reviewed and consists now of 28 sub-sectors. Applying this methodology, eight sub-sectors of overriding importance in the field of CIP were identified (see table on page 25). ❖

For more information about the Swiss Programme on CIP, please visit the Critical Infrastructure Protection section on the Federal Office for Civil Protection (FOCP) website at www.infraprotection.ch.

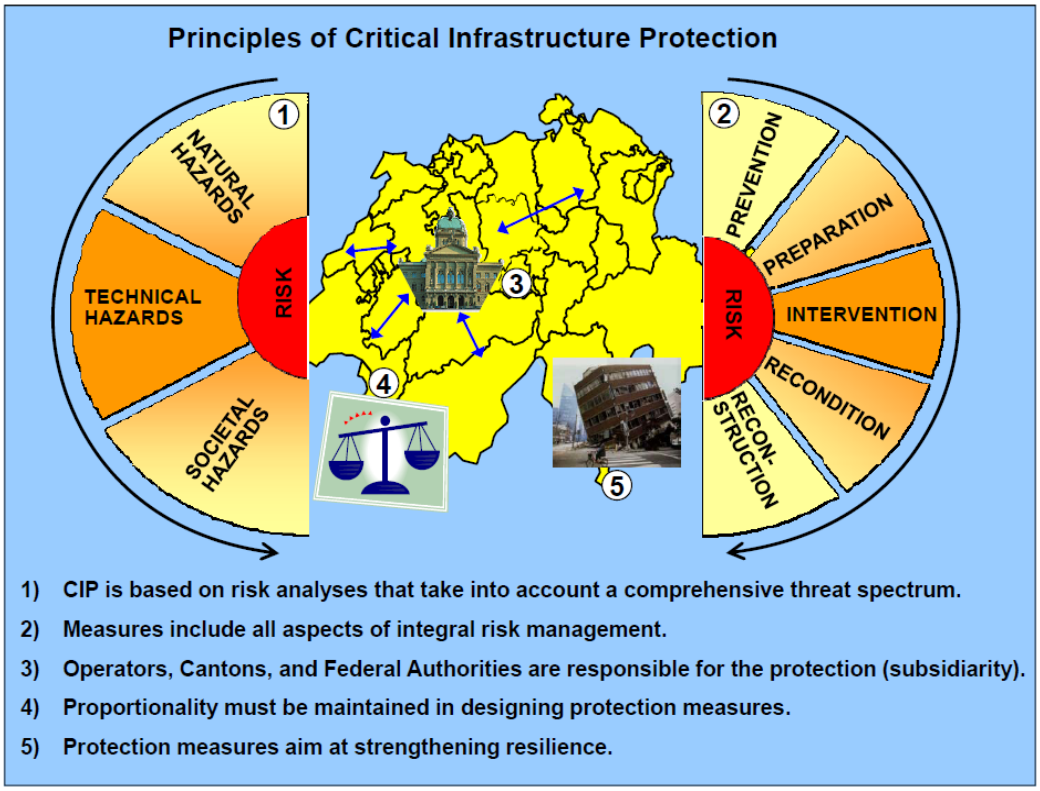


Figure 1

Crisis Management *(Cont. from 9)*

contribute to academic and public debates about social, ethical, and legal issues.

As for the latter, as in all system developing projects, a large number of legal issues have to be observed. Some examples relate to:

- How the system should be designed (e.g. the need to comply with data protection rules, security regulations, privacy issues, and intellectual property rights);

- How the system development process proceeds (e.g. contracting, responsibilities for specifications, documentation of changes and alterations, confidentiality issues, use of subcontractors, marketing and reporting);

- How the system is being implemented (e.g. the need to adjust to international standards, design international agreements concerning use of the system, establish new authoritative command, and control structures, teaching/training etc.); and

- How the system performs (e.g. liability for system malfunctioning, such as aggregating devastation and loss of lives due to poor performance, allocation of responsibilities, need of back-up facilities, etc.).

Many of the above mentioned issues should preferably be dealt with as early as possible during the design process as proactive (imbedded legal compliance) solutions are far more rational than traditional, reactive legal remedies. In addition, various organisational traditions, as well as cultural and ethical issues, need to be taken into consideration. This usually indicates that various forms of trade-offs between operational efficiency, social acceptance, legal requirements, and political concerns may become relevant. ❖

Peter Wahlgren, LL.D. is a Professor in Law and IT at The Swedish Law and Informatics Research Institute, Faculty of Law, Stockholm University, Fellow, The Center for Infrastructure Protection and Homeland Security, Georg Mason University. His contact information is as follows: peter.wahlgren@juridicum.su.se.

German Infrastructure *(Cont. from 20)*

consideration of inter-infrastructure dependencies among the considered sectors, the decision support is based on a sound decision basis. Furthermore, the cooperation and the communication among the different stakeholders in critical infrastructure protection are supported in a constructive way. ❖

Mirjam Merz, Michael Hiete, and Frank Schultmann can be contacted at the Karlsruhe Institute of Technology (KIT), Institute for Industrial Production (IIP) at Hertzstraße 16, 76187 Karlsruhe, Germany at mirjam.merz; michael.hiete; and frank.schultmann@kit.edu.

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