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.

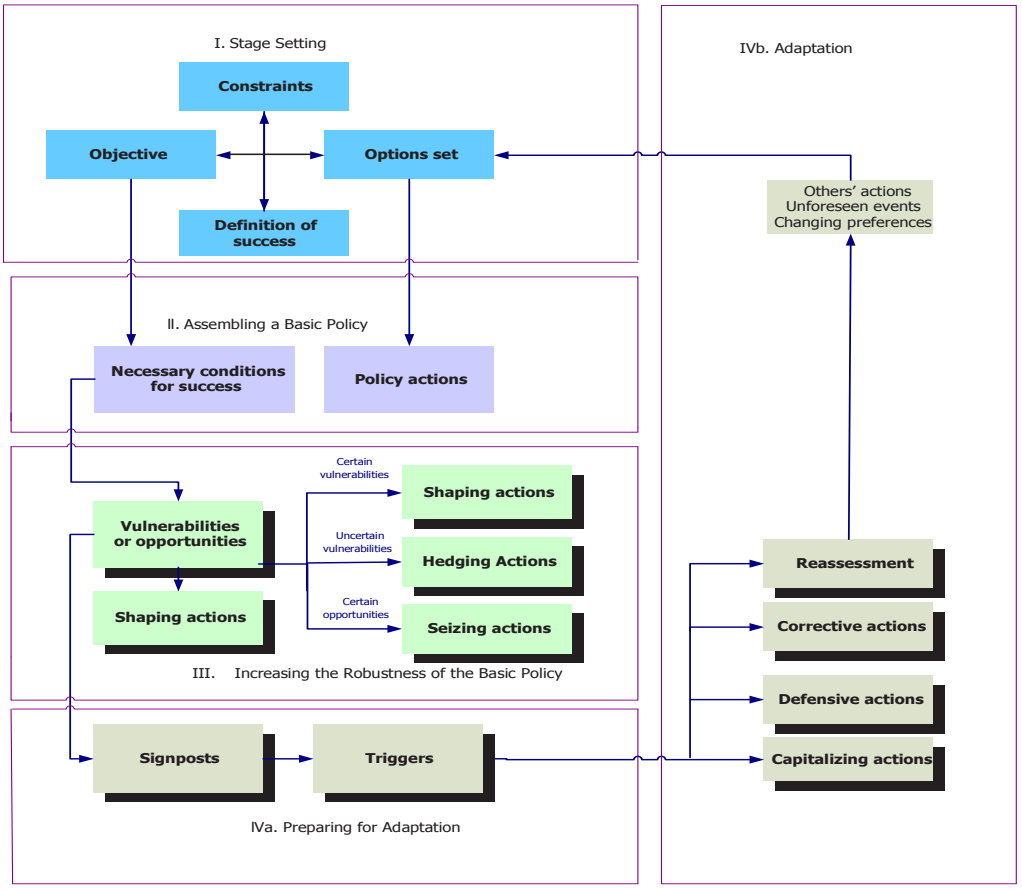
Infrastructure Planning *(Cont. from 6)*

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)*

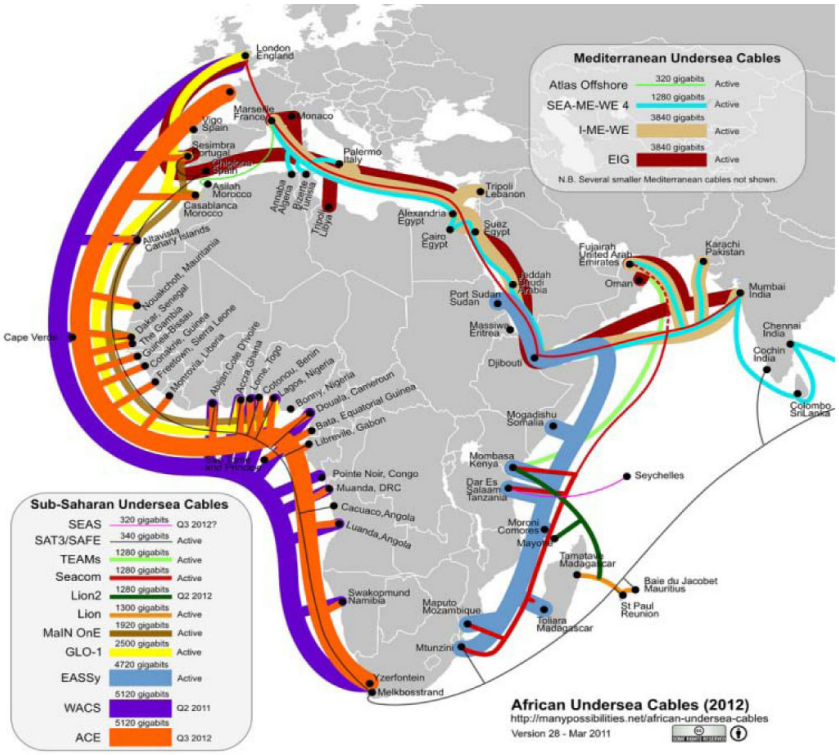
services to far-flung regions within their borders. The prospect of providing a physical link to a remote region is not feasible in many cases. However, the growing use of wireless technologies allows vast areas to be connected by investing in a number of wireless transmitters. Cellular networks, wireless 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.