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)

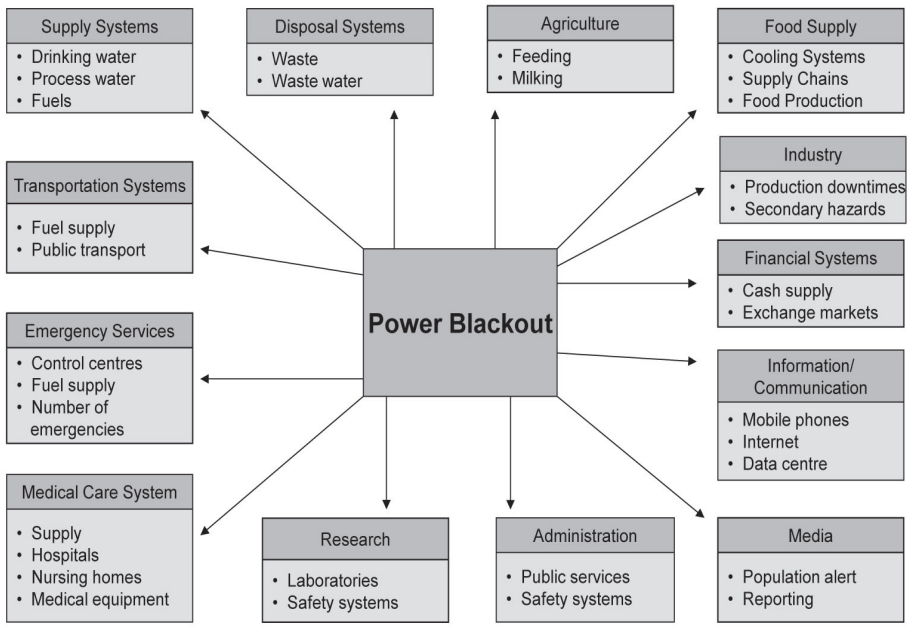
Critical Infrastructure Protection in Germany: Accounting for Inter-infrastructure Dependencies and Facilitating Public-Private Cooperation

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)

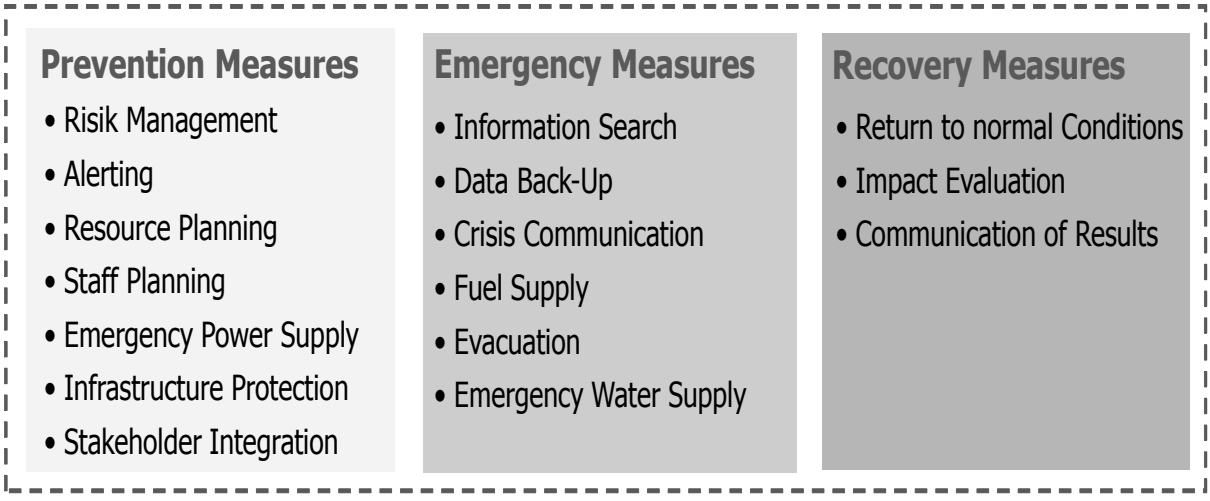


Figure 2: Crisis management measures described within the checklists of the handbook.

[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)

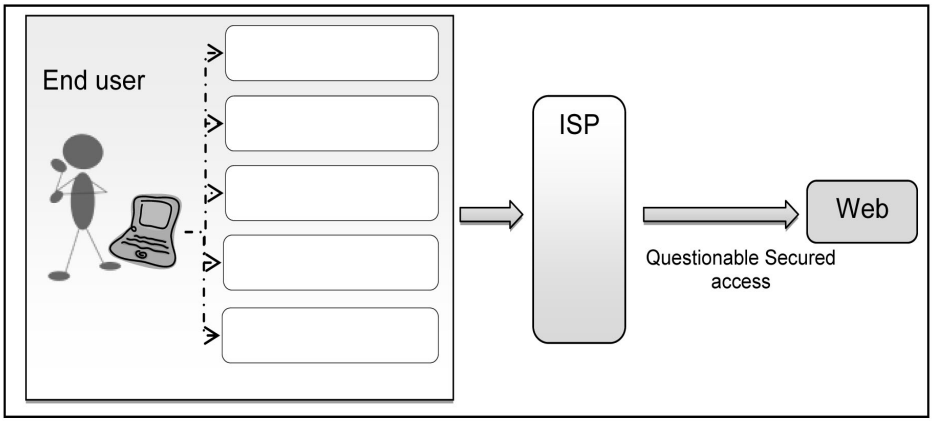


Figure 1: Thick End User/Thin ISP.

[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).