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.

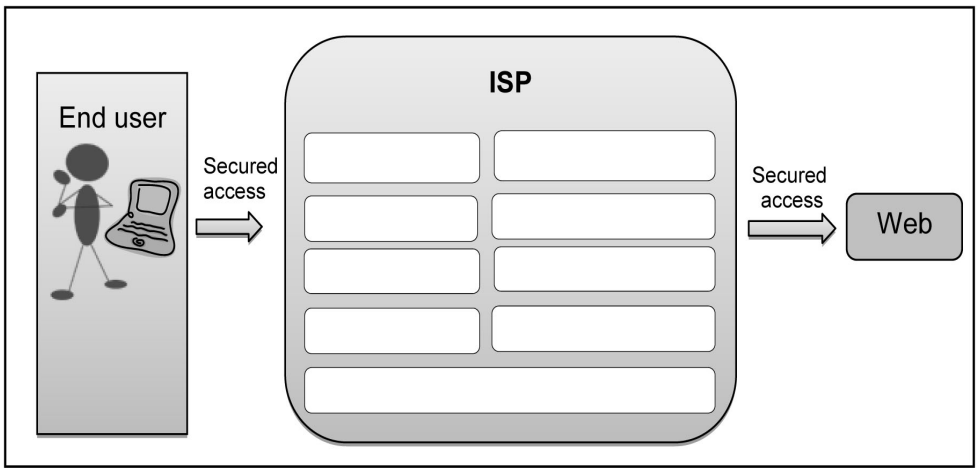
Conclusions

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.

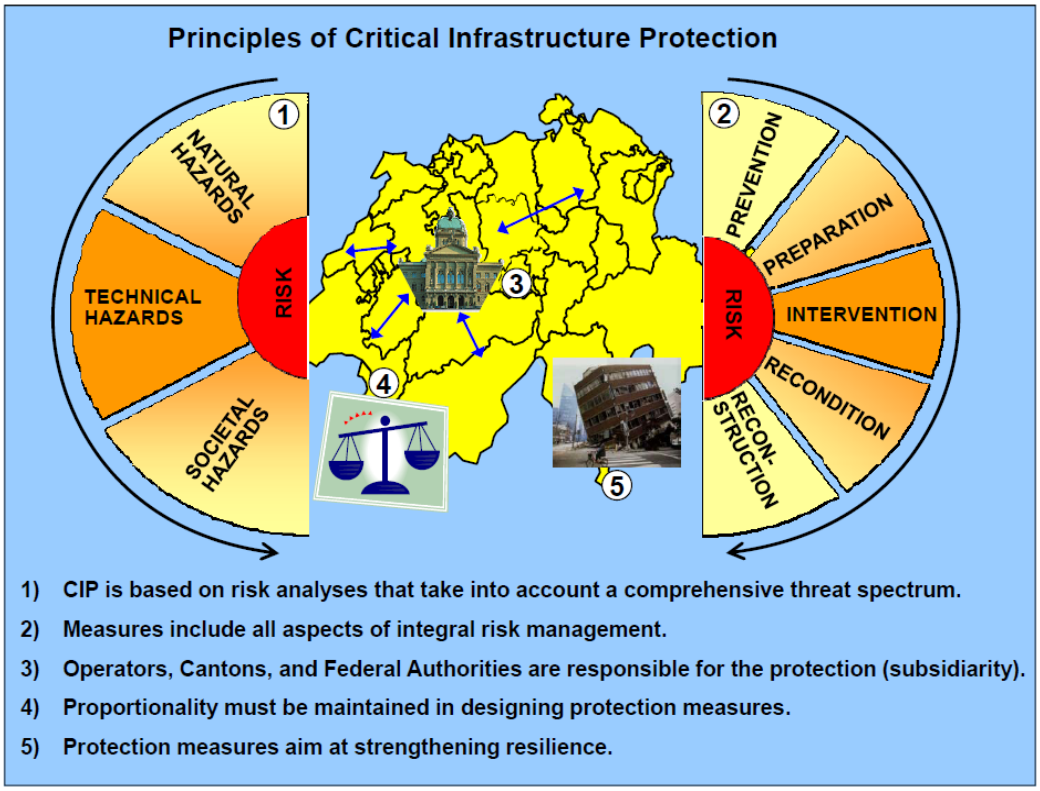


Figure 1

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