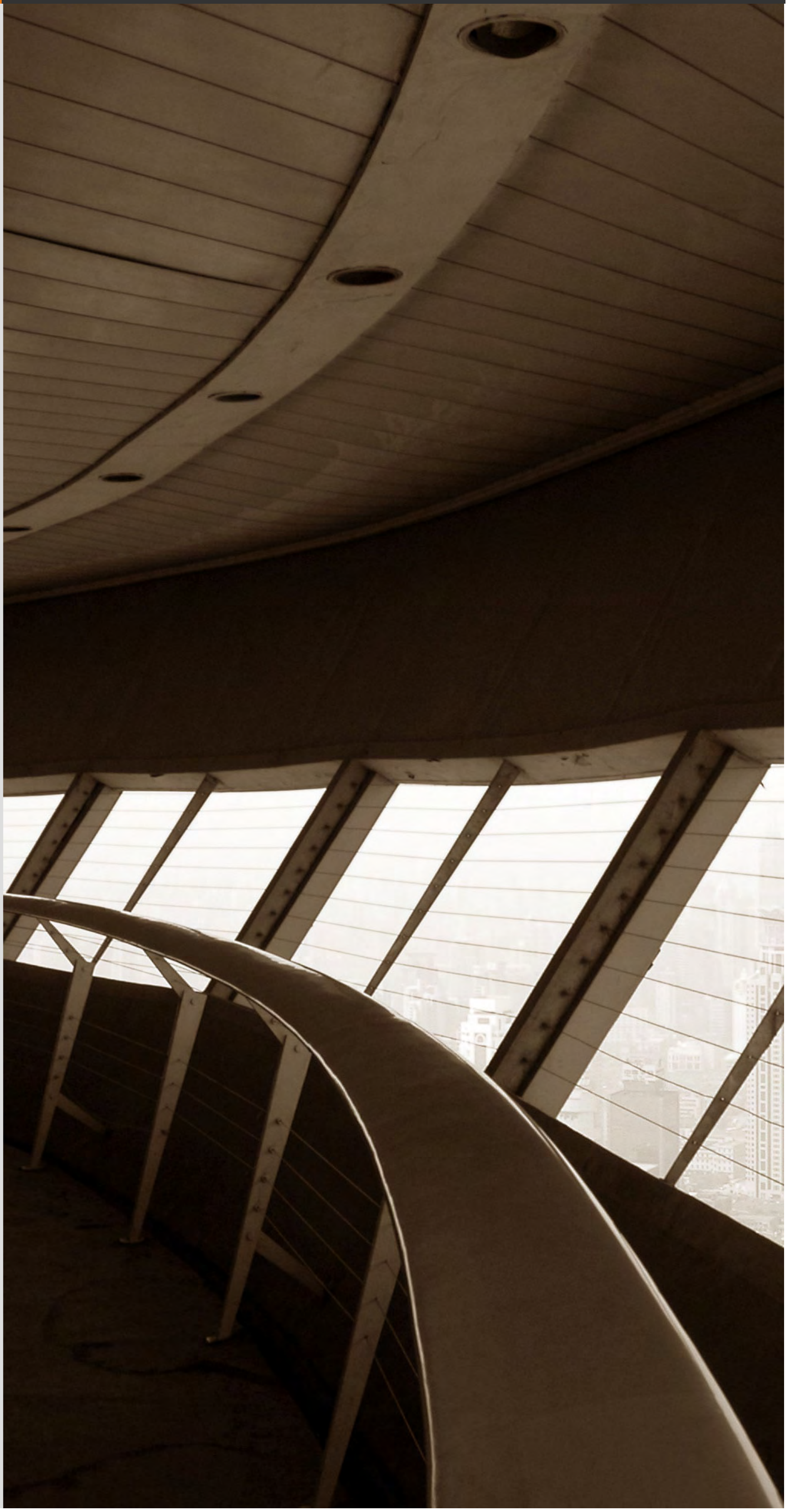
October / November 2006, Volume 2, Number 3

ECN

European CIIP Newsletter

CI^{2}RCO



> About ECN
ECN is co-ordinated with
The European Commission, was initiated by Dr. Andrea Servida,
and is now coached and supervised by Angelo Marino
For 2005-2006, ECN is financed by the CI^{2}RCO project
The CI^{2}RCO project is an IST FP6 Co-ordination Action,
funded by the European Commission
under the contract no 015 818

>For ECN registration send any email to:
subscribe@ciip-newsletter.org

>Article can be submitted to be published to:
submit@ciip-newsletter.org

>Questions about articles to the editors can be sent to:
editor@ciip-newsletter.org

>General comments are directed to:
info@ciip-newsletter.org

>Download site for specific issues:
http://www.ci2rco.org

>Founder and Editors
Eyal Adar CEO iTcon, ***eyal@itcon-ltd.com***
Bernhard M. Hämmerli, HTA, Initiator and Main Editor ***bmhaemmerli@acris.ch***
Eric Luiijf, TNO, ***eric.luiijf@tno.nl***

>Country specific Editors
For Germany: Heinz Thielmann, Prof. emeritus, ***heinz.thielmann@t-online.de***
For Italy: Louisa Franchina, ISCOM, ***luisa.franchina@comunicazioni.it***
For France: Michel Riguidel, ENST, ***riguidel@enst.fr***
For Spain: Javier Lopez, UMA, ***jlm@lcc.uma.es***
*For Finland: Hannu Kari, HUT****, kari@tcs.hut.fi***

> Graphics and Layout
Florian Widmer florian_widmer@gmx.net

> Spelling:
British English is used except for US contributions

ECN European CIIP Newsletter

Table of Contents

Introduction

European Activities

Country Specific Issues

Methods and Models

News and Miscellaneous

Selected Links and Events

EU funded projects and conferences boost CIIP

CIIP problem description is now understood by experts. New is the challenge of SCADA insecurity which has an increasing importance. On other, more classic CIIP domains, some pretty good approaches were shown lately in conferences.

Dr. Bernhard M. Hämmerli

Professor in Information Security
Founder of the Executive Master Program IT Security, FHZ
President ISSS
bmhaemmerli@hta.fhz.ch
bmhaemmerli@acris.ch

About this Issue

The first two articles of this ECN issue discuss two different analysis methods for CIP. Both methods – one analytical and one scenario-based – are developed by the EU funded Project IRRIIS *(Integrated Risk Reduction of Information-based Infrastructure Systems).*

The next article discusses the NESSI working group Trust, Security and Dependability (TSD) which aims to create a unified trust, security and dependability framework on software and services to be used by the European research community.

A new Finish approach to dependability evaluation methods for IP networks is very broad. The stakeholder community of the approach includes engineers, independent regulators, and users.

The start of the Israel CERT was not easy. It had to prove itself to too many other CERTs. The breakthrough came with the Tehila project which is described in this issue.

How serious lead workshops contribute to the development of CI(I)P is shown in the contribution about the third international EAPC/PfP workshop with the thematic priorities "Interdependencies & vulnerabilities of Energy, Transport and ICT" held late August in Zurich.

Only a limited set of surveys exist about the state of national information security activities. Recently, ETHZ has published one. Brief insights into the methodology and results are shown.

The International Federation IFIP WG 11.10 has initiated a Working Group on Critical Information Protection. As an initial activity the working group starts with a conference in the United States.

The *International Conference on Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA)* reports on their recent conference in 2006 and invites you for the next conference in 2007.

About the Link Collection

This time the focus of the link collection is related to the articles and related papers. It was astonishing how much material can be found on the Internet through the articles.

The complete link collection of all ECN issue can be found on www.ci2rco.org (within the download section)

Authors willing to contribute to future ECN issues are always very welcome! Please contact me. Further information about the ECN and its publication policies can be found in the introduction of the first ECN, see www.ci2rco.org.

From next issue on, the ECN can be found on the IRRIIS webpage. However we hope, that all ECN mirror sites including the CI^{2}RCO website will be maintained further.

Enjoy reading the ECN!

Towards a holistic metamodel for systems of Critical Infrastructures

The Implementation-Service-Effect (ISE) metamodel describes Critical Infrastructures from different perspectives in a well-defined way to provide a sound basis for the analysis of their dependencies and interdependencies

Uwe Beyer

Uwe Beyer is the head of the department Adaptive Reflective Teams (ART) at the Fraunhofer Institute Intelligent Analysis and Information Systems (IAIS) and acts as the IRRIIS Project Manager

Felix Flentge

Felix Flentge is in charge of all IRRIIS activities inside the Fraunhofer IAIS. He is leading one of the IRRIIS subprojects and the work packages dealing with the SimCIP simulation environment.

The aim of the European Union *Integrated Project IRRIIS (Integrated Risk Reduction of Information-based Infrastructure Systems)* is to increase the dependability of large and complex critical infrastructures. In order to achieve this goal a common, well-defined modelling approach is needed. The *ISE (Implementation – Service – Effect) metamodel* provides a modelling framework taking the various view-points from different sectors and professions into account. But the ISE metamodel is not limited to this specific project. It provides rather a general modelling approach for systems of critical infrastructures. While not neglecting the technical basis, it provides the necessary abstractions needed for risk or emergency management of critical infrastructures in a complex environment.

Risk management of CIs needs sound models taking the whole CI system into account.

Current Problems in Critical Infrastructure Modelling

The modelling of complex infrastructure systems together with their dependencies is a big challenge and there is no general methodology to accomplish this task. There are several problems one typically has to face:

- The *data-chicken-egg-problem*: Many research projects have severe problems getting the data needed for research. Due to sensitivity concerns no data is available unless risks have been identified. But risks can only be identified, if relevant data is available.

- The *level-of-abstraction-problem*: It is difficult to find the right level of abstraction to match the modelling purpose. If the level is too high, only trivial results can be achieved. If the level is too low, there is too much data and interesting structures may not be found (“Seeing a lot of trees, but no forest.”).

- The *particular-answers-problem*: As the system-behaviour is dependent on many low-level technical facts, small changes can have big effects on the overall system-behaviour. So, it is difficult to assess the validity of results.

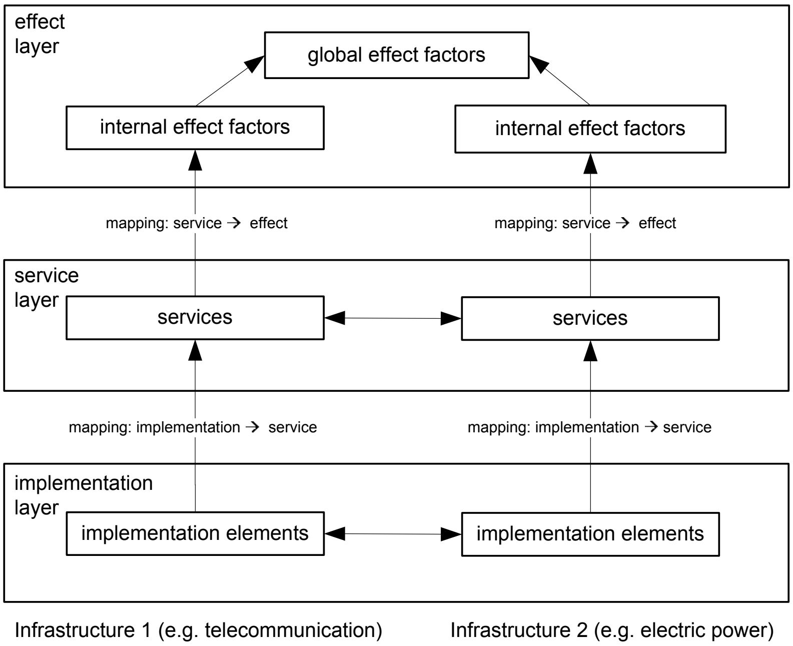
- The *different-views-problem*: Naturally, the management of an infrastructure operator has a very different view on the same infrastructure as a technical engineer. Experts from different sectors use different terminologies. But in the end all these views and terminologies relate somehow to the same system of critical infrastructures.

Another problem is concerned with the analysis that follows the modelling process. Again, there are no general methods for systems of complex infrastructures and their dependencies (apart from the usual methods from complexity science dealing only with very abstract networks). The lack of a common modelling methodology and analysis methods makes it difficult to share models and compare results.

The ISE metamodel provides a way to minimise these problems to some extent by providing a stepwise modelling approach that links the different views on critical infrastructures. By giving a sound mathematical foundation, systems of dependent critical infrastructures can be described in a well-defined way and analysis using well-established methods from other fields is possible.

The ISE Metamodel

An ISE model is composed of several ISE sub-models. Each of the sub-models consists of three kinds of elements: *implementation elements*, *services (public and internal)* and *internal effect factors*. A full ISE model is created by combining several of these sub-models, describing their *dependencies* (within and across sub-models) and adding *global effect factors*. The model consists of three layers: the *implementation layer*, the *service layer* and the *effect layer*. The relationships between these layers are described by two mappings: the *implementation-service mapping* and the *service-effect mapping*. The general structure of an ISE model for two infrastructures is shown in the figure on this page. A simple example for telecommunication and electric power infrastructure service and implementation layer is given on the next page (dependencies between layers are not shown for clarity).


effect layer
global effect factors
internal effect factors
internal effect factors
mapping: service → effect
mapping: service → effect
service layer
services
services
mapping: implementation → service
mapping: implementation → service
implementation layer
implementation elements
implementation elements
Infrastructure 1 (e.g. telecommunication)
Infrastructure 2 (e.g. electric power)

The *service layer* is the central layer. Services are either delivered to the end-consumer, to some other critical infrastructure (public services) or to some other part of the same infrastructure (internal services). As public services are products that are sold and delivered to customers and are usually accompanied by service level agreements, they should be easy to identify and provide a good starting point for modelling. Internal services usually can be identified by looking at the internal organisation of the individual company.

Services are realised by implementation elements at the *implementation layer*. Implementation elements are everything that is necessary for the provision of a service: physical equipment, operators, procedures, single infrastructure components but also whole systems.

The *effect layer* describes the effects of the successful delivery of services or of the failures to do so. Effects could e.g. be measured with money, risks or effected people. Besides the internal effect factors of each sub-model there are global effect factors to combine other effect factors (e.g. to describe economic or societal effects).

It is important to note that in an ISE model dependencies between elements of different sub-models can only appear within the same type of layer. Dependencies within one sub-model are always within the same layer or appear in a clear top-down manner. All of these dependencies can be described as directed graphs. All in all there are five graphs:

- The *implementation dependency graph* on the elements of the implementation layers.
- The *service dependency graph* on internal and public services
- The *effect dependency graph* on internal and global effect factors.
- The *implementation service dependency graph* between services and implementation elements.
- The *service effect dependency graph* between services and effect factors.

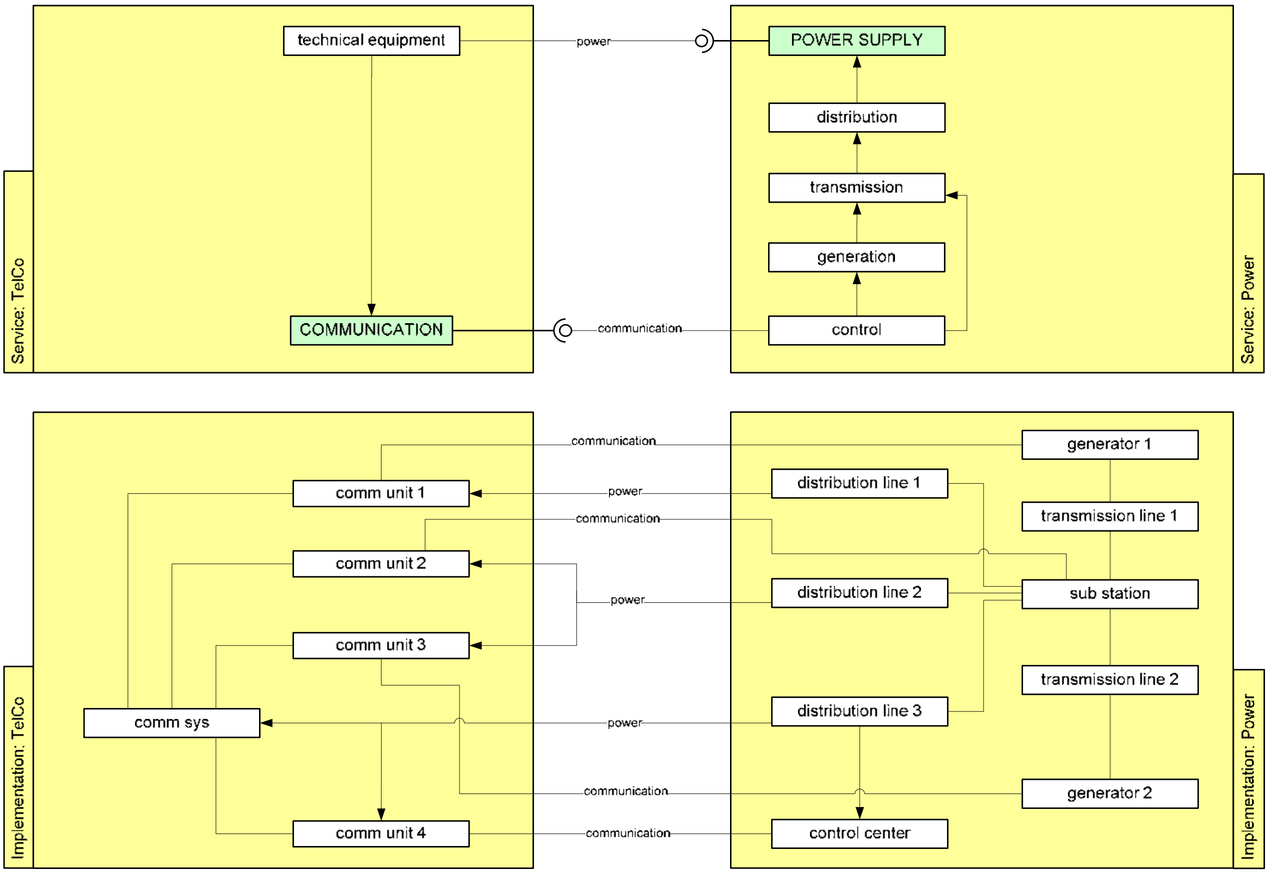
With this rather general structure a huge amount of different actual models of critical infrastructures can be realised. ISE does not prescribe a certain level of detail and not all layers have to be included in the actual model. One can start with very simple models on only one layer and include other layers or split single elements to several elements during successive refinement steps.

Analysing Critical Infrastructures with ISE

Based on the principal structure of the ISE metamodel and the nature of the dependency descriptions, different types of actual models and different kinds of analysis are possible.

- *Topological Models*

The graphs on the different layers can be analysed using methods from graph theory and complexity science. In addition, each dependency on the service layer must have its counterpart on the implementation layer and vice versa.



These relationships can be described in terms of graph theory and be used to check the model's consistency and to relate dependencies on one layer to elements and dependencies on the other layer. Taxonomies of interdependencies can be built, general structures can be detected and general strategies to deal with interdependency problems may be derived.

- *Boolean Models*

While topological models can only indicate where problems might occur, Boolean models go a step further. In a Boolean model the status of each element is described by a Boolean value (working / not working). In addition, there is a Boolean expression for each element to determine its value based on the current values of the preceding elements. By changing the values or expressions of specific elements a "what-if-analysis" to investigate the spreading of failures can be performed.

- *Numerical Models*

Real values or vectors can be assigned to each element. Values should be calculated based on the values of the preceding elements. These dependencies can be described by difference equations or differential equations and may also include random variables. It may be possible to analyse these models mathematically but usually their behaviour will be simulated over time and investigated with stochastic methods.

- *Simulation Models*

In simulation models each element may carry arbitrary attributes of any kind. The attribute values are dependent on the attribute values of the preceding elements. The way of interaction is described in form of algorithms attached to each element. These models can be simulated in a computer, e.g. using agent-based simulations. The results from the simulation can then be analysed using all kinds of stochastic methods and visualisation techniques.

Summary

The ISE metamodel provides a generic way to model critical infrastructure systems for different purposes. It is able to bridge the gap the engineering and the business view on critical infrastructures. Dependencies are described in a well-defined way which allows all kinds of analysis. This model will be applied in the IRRIIS project but could also be well-suited for other projects dealing with critical infrastructures or the delivery of services in general. Especially, the application in the context of risk or emergency management seems to be very promising. The development of an agent-based simulation environment called SimCIP (Simulation for Critical Infrastructure Protection) based on the ISE principles is currently under way at Fraunhofer IAIS.

Contact & Information:
www.irriis.eu

Acknowledgment:

IRRIIS is partly funded within the European Community's Sixth Framework Programme. However, all views expressed above are purely those of the authors and the Community is not liable for any use that may be made of the information contained therein.

Overcoming of CIP obstacles by scenario management

Our world has become more dynamic, more complex, more dependent and more vulnerable. Strategic planning and corporate governance need new instruments like scenario management to be prepared for future challenges.

Walter Schmitz

is senior consultant of IABG in the area of CIP. He was the scientific coordinator of the European Commission´s ACIP (Assessment of Critical Infrastructure Protection) project and is member of the EC´s VITA (Vital Infrastructures Threats and Assurance), CI^{2}RCO (Critical Information Infrastructure Research Co-ordination) and IRRIIS (Integrated Risk Reduction of Information-based Infrastructure Systems) projects. This article is based on the IRRIIS deliverable "Scenario Analysis" and on ISBN 3-593-36714-9 "Erfolg durch Szenario-Management".
Phone: +49 (0)89 / 6088-3331
E-mail: schmitz@iabg.de
Internet : http://www.iabg.de

Abbreviations:

CI	**Critical Infrastructure**
DG	**Distributed energy Generation**
DSO	**Distribution System Operator**
ICT	**Information and Communication Technology**
RES	**Renewable Energy Sources**
TSO	**Transmission System Operator**

Critical infrastructures like electricity and telecommunications have undergone drastic changes in the last decades. The ubiquitous use of ICT has pervaded all traditional infrastructures, rendering them more intelligent, increasingly interconnected, complex, interdependent, and therefore more vulnerable. Due to the ICT-dependence, infrastructures have also become more dependent on each other, especially on telecommunication including Internet. The economic and societal relevance of the dependability and resilience of critical infrastructures is obvious: infrastructure malfunctioning and outages have far-reaching consequences, and may hamper economic growth, create a widespread public dissatisfaction, and cause distrust within the society. The existing knowledge and understanding of the ICT-related dependencies and interdependencies of critical infrastructures and their services as well as the related potential risk of cascading effects is still insufficient. As our education is mainly focused on single disciplines, interdisciplinary thinking and training have not been developed sufficiently to design and manage complex, interdependent systems at various architectural levels with adequate risk reduction and security improvement. All the more as new market developments, technologies, threats and vulnerabilities are emerging - which planner would not like to look into the future in order to know earlier than his competitors what technologies will be successful, whether novelty threats will emerge, and what countermeasures should be taken? But nobody knows the future and planners waver between two extremes: Asserted certainty with unperturbed extrapolation of the traditional planning and total uncertainty without any indication for the future characterised by its credo "a strong position now and here is the best preparation for the uncertain future." Both attitudes negate the range of limited uncertainty between these both extremes. In the space between them, the future can also not be predicted but thought ahead. For this purpose three obstacles have to be overcome:

Thinking the future and overcoming of important obstacles

(1) The imagination that we deal with an exactly predictable future
(2) The hard rule of cause and effect in a highly complex world
(3) Sole focusing on the current success that can lead into a future flop.

Critical infrastructures are highly complex and interdependent aiming at survivability by economic behaviour. Realisation of future profit is only possible when the essential factors of success can be identified today and the development of the organisation will be directed to them. Organisations like critical infrastructures have to pay attention to their environment and have to consider the benefit of their stakeholders today more than ever before. Critical infrastructures will be considered as successful if they are able to balance the interests of their different stakeholders in the long run whereas the benefit of the shareholders remains an important factor. But other aspects like environmental sustainability or security of employment have also to be considered in a multi-dimensional system of objective functions.

But everyone who tries to overcome the three obstacles has to keep in mind that he will tangle with three powerful groups:

- Traditional planners, market-researchers and controllers will shake their heads and explain why useful concepts can not be designed considering several futures.
- The shirt-sleeved wrights will argue that networked thinking is an intellectual baublery.
- And the successful colleagues will point to their impressive balance sheet.

But nevertheless future oriented organisations should not neglect three new approaches

(1) Thinking and acting open for each possible future: CIs have to consider alternative developments of influence factors. Basic principle will be the imagination of a multiple future.

Scenario Management: a new approach for CIP

(2) Networked thinking and acting: Today's CI owners and operators must consider the behaviour of other interdependent CIs for their strategic planning and for the subsequent realisation.

(3) Strategic thinking and acting: organisations which want to be successful in future should not focus exclusively on the current success but their strategic orientation has to look after creation and sustainment of the prerequisites for future success.

These central control factors are referred to as success factors. The inter-linkage of networked thinking and openness for each possible future leads to the item "scenario". In our context, scenario means alternative descriptions of future complex systems like CIs. Knowledge of the individual parts of a system is not enough to be able to assess a complex system. It is also important to know their cross-linking and behaviour in a changing environment. The integration of such scenarios into the process of the strategic management leads to the item of "scenario management".

Scenario management applies alternative scenarios in order to identify and tap new success factors.

Early Detection

Organisations that want to be successful in the future have to be not only faster but also able to detect and process weak signals of new developments earlier than their competitors. But the question is how to detect and process them in a goal-oriented way in order to enable the organisation to react quickly and adequately? The answer is: we need a strategic early detection capability characterised by the following internal processes:

(1) Scanning: Weak signals will be detected by scanning of the whole environment of the organisation resulting in trends that could influence the development of the organisation.

(2) Examination: Identified signals will be screened how relevant they will be with respect to the development of the organisation. Then interrelationships between the trends will be revealed and assessed by means of the networked thinking.

(3) Observation: Critical factors – e.g. crisis indicators – will have to be systematically observed.

(4) Scenarios: Lastly projections of the recognised trends will be elaborated and combined into scenarios in a systematic way.

Such a process of early detection provides new insights concerning dangers but also chances. Insofar, the fast and well directed integration of the insights into the planning process represents an important success factor. Its most important advantages are:

(1) The early detection of weak signals prolongs the time required for decision making.

(2) The efficient integration of the detected signals into the decision process enlarges the scope of design and control.

(3) And last but not least decisions based on relevant data of early detection are not pressed by time anymore.

Scenario building for CIP

Technology foresight and technology assessment is a process, where experts produce, share, analyse and use explicit knowledge to form a justified understanding of the future developments of critical infrastructures. According to the IRRIIS project the scenario building process is carried out in following steps:

(1) Description of the state of the art of the CI to be considered;

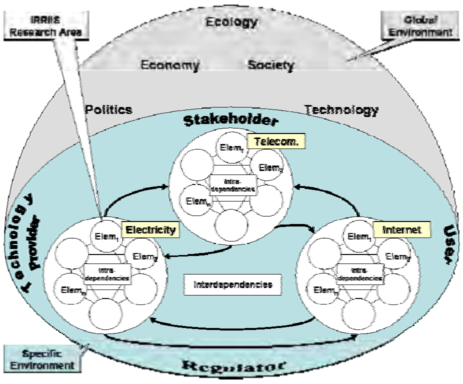
(2) Identification and description of trends and their projections impacting the future developments of the CIs;

(3) Analysis and selection of essential trends;

(4) Combination of the trends into consistent scenarios.

Identification of trends

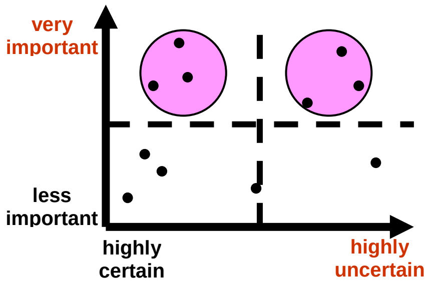
Within the IRRIIS project the identification and description of trends – called key factors – was mainly based on literature research, brainstorming and discussions. The factors identified during the process, covered an extensive bunch of different phenomena varying from mega trends like "globalisation", to more specific trends like "distributed energy generation". Trends have been derived from the areas of politics, economy, technology, society and ecology as represented in the figure below.



A detailed description of each factor, its actual status and two opposite projections reflecting the possible ways of future development of the factors were given (IRRIIS deliverable "Scenario Analysis"). Afterwards the factors were processed by two analysis phases: Impact - uncertainty analysis and influence analysis, both aiming at selection of essential key factors.

Impact-Uncertainty analysis

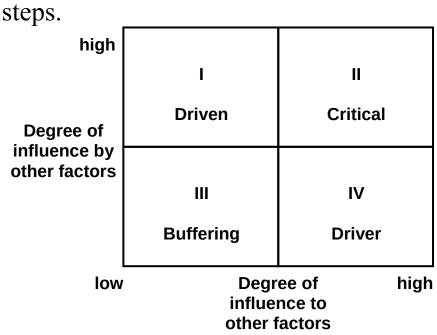
The impact-uncertainty analysis is a method to rank the identified key factors according to their importance and uncertainty (see figure below).



Those of the identified factors that have been located into the quadrant “very important – highly uncertain” are good candidates for the next steps of the scenario construction process. Those factors located in the area “very important – highly certain” should be included into the scenarios as well. Factors located in the area “less important” are candidates to be neglected in the scenarios.

Influence analysis

The influence analysis reflects the relationship between the key factors. It subdivides them into driver elements (drivers), driven elements, critical elements and buffering elements. The attention of the subsequent scenario steps should be focused mainly on drivers, driven elements and critical elements. Buffering elements are candidates to be neglected in the subsequent scenario steps.


high
Degree of influence by other factors
I
Driven
II
Critical
III
Buffering
IV
Driver
low
Degree of influence to other factors
high

At the end of the impact - uncertainty and influence analysis the following factors have been selected as key factors to be utilised in the IRRIIS scenario descriptions:

- Liberalisation of CI Markets
- Reliance on energy sources outside EU
- Protection of environment and energy saving
- Security management
- Business models
- Energy market dynamics
- Distributed energy generation and renewable energy sources
- Skills of personnel
- Complexity and dependences
- Sophisticated and converging networks based on the Internet
- Information security of ICT.

As already mentioned, two potential projections into the year 2015 have been identified for each key factor and subsequently the projections have been combined to consistent scenarios.

Consistency analysis

The consistency analysis is based on pair wise comparisons of the projections. The comparison result is presented on the scale from +2 to -2, where it has been agreed:

- +2, both projections are highly consistent,
- 0, neither consistent nor inconsistent
- -2, both projections are highly inconsistent.

The results of all pair wise comparisons generate the so called consistency matrix and the values of the consistency matrix are used to calculate consistency values for all different combinations of the projections. The aim of the consistency analysis is to identify all combinations whose projections are not inconsistent. During the IRRIIS scenario process two scenarios were selected, which are highly consistent and extremely different. The both scenarios have been named:

- Internet-driven open market and
- Concentration and private networks.

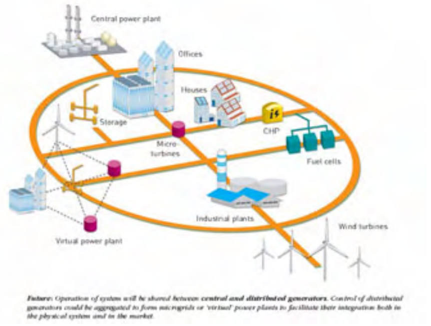
Two extreme scenarios of the IRRIIS project

Their projections differ in all projections and span a far-reaching range of potential risk factors. The “Internet-driven open market”-scenario is mainly characterised by increasing “liberalisation of the market” and by exploitation of an increasing number of “sophisticated and converging networks”. The “concentration and private networks”-scenario is characterised by a low rate of change of the both key factors.

Scenario 1 “Internet driven open market”

In the year 2015, liberalisation has led to an efficient EU market and CIs have grown together to international CIs. Free trade throughout Europe is facilitated by open markets, harmonised rules and transparent trading procedures. New services that need networked information and telecommunication systems are created. Energy supply and delivery are ensured in the EU area. Long-term contracts with energy suppliers, alternative transmission routes and the EU’s economic wealth ensure energy supply from outside the EU even if the prices increase. Increasing proportion of power generation will be based on conventional fuels and big power plants and on increasing proportion of renewable energy sources. Management of power transmission bottlenecks and power balance becomes more important. This increases the dependence on data communication. CI providers use increasingly self-tolerant, ICT-based services. Agent technology and different brokering service providers help users to manage the vast amount of data. Sophisticated networks are deployed increasingly. Telecommunication, Internet and TV will converge to a single trusted multi-technology network. Critical services will securely use the Internet as communication line and thus save costs. Increase of distributed generation (DG) and renewable energy sources (RES) require investments on reserve generation and power network strengthening. Suitable actions have been taken to avoid increasing costs and worsening reliability that DG and RES would otherwise cause. Liberalisation opens good chances to flexible and trans-national CI providers. Privatisation leads to lower prices due to keen competition and cost pressure, which enforces the operators to increase outsourcing and reduction of redundancies. Harmonisation of market rules and communication protocols has already achieved major advances. Regulation policies have succeeded in creating a competitive energy market. Many actors really compete in the market, which increases the volumes traded in real-time market. Automated trading is common. Communication infrastructure is important. ICT is able to give the necessary support.

Increasing distributed generation, use of renewable energy sources and energy saving services enabled the transfer to carbon neutrality and to diminish emissions. The balance between distributed and central generation is illustrated in following figure.


Central power plant
Offices
Houses
Storage
CHP
Micro-turbines
Fuel cells
Industrial plants
Wind turbines
Virtual power plant
Future: Operation of system will be shared between central and distributed generators. Control of distributed generators could be aggregated to form microgrids or 'virtual' power plants to facilitate their integration both in the physical system and in the market

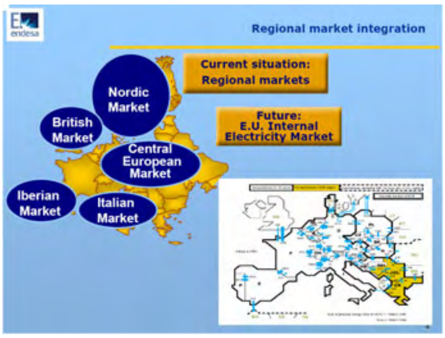
The suppliers have developed new energy saving services, which require two-way communication. Electricity distribution management is also improved by a secure telecommunication network. This is done by implementing of appropriate back-up channels.

Skilled and well-trained personnel are available. The increasing complexity of critical infrastructures with the necessity of integrated risk reduction enforces an integrated and multi-disciplinary educational approach which includes interdisciplinary knowledge, networked thinking, team spirit, co-operation, and efficiency in providing solutions. CI providers have to cover a wide range of clients and installations, local safeguarding of ICT is not enough. The importance of information security of networked systems is increasing. The security matters of the wireless communication information are understood well, security features are developed to be a natural part of fixed and wireless networks.

Scenario 2 “Concentration and private networks”

Scenario 2 is widely opposite to scenario 1. Liberalisation and globalisation have caused a concentration process with a few market dominating players. Official markets play only a marginal role and essential market information and prices are controlled by the dominant players during critical moments. Liberalisation has led to a strong dominance of a few big players with clearly regulated international connections. In reality, this means a diminished liberalisation of critical infrastructure markets.

The EU markets are integrated regionally: Central European Market, Nordic Market, British Market, Iberian Market and Italian Market (see figure below).


Regional market integration

Current situation: Regional markets

Future: E.U. Internal Electricity Market

Inside the regional markets, the bottlenecks of the transmission are mainly removed, but congestion in electricity transmission between different regions still exists.

The number of big dominating players is so small that they can trade bilaterally outside the public exchange. The marginal role of the public exchange makes it difficult for new players to enter into the market. Scarcity of primary energy sources and climate changes causing high market prices for emissions direct the investment decisions in favour of generation capacity. Reserve peak power generation is built outside the competitive market framework, which further shrinks both the role of the spot market and competitive investments. Also energy supply from outside EU suffers extremely from substantial reductions during high demand times. In addition some rich OPEC nations boycott the western world. Very high prices on electricity, oil and gas market are experienced. Rationing of electricity becomes necessary. Data communication is critical for enabling the most efficient use of scarce energy and in preventing the service of electricity infrastructure from collapsing. The real time performance of the Internet as communication means is insufficient for power balance control needed round the clock. The electric power sector uses SCADA systems only partly linked together via the Internet. The interoperability between networks is difficult with many technical and contractual problems. For business purposes, stakeholders use private networks and services because use of each one’s own physical or proprietary virtual communication lines increases the level of information security. The open standards have a weak position; the trend is toward strong proprietary standards. Also threats like terrorism, information security attacks, viruses and fear of disruption and instability have caused general mistrust towards Internet and integrated sophisticated networks. Hence, the common base for integration has been missing and different critical infrastructures developed in isolation. So far intelligent technologies are in place, but are not well integrated. This means that there are many different networks inside single multi-technology networks without efficient co-operation. The penetration of distributed generation and renewable energy sources has stopped increasing. Crucial reasons were:

- high prices of electricity produced by distributed generation and renewable energy sources,
- cost of reliable communication to distributed sites,
- complex protection systems,
- non-harmonised requirements for distributed generation, which leads to significant decrease of the security of the power supply.

Dominant shareholder value model is prevailing in business. Globalisation and liberalisation of trade have led to dominance of capital and survival of the fittest. The players in the network field are fighting against each others without fruitful co-operation and contracts. The concentration of the market has decreased the public real-time market trading. Trading can be done without a public communication infrastructure. Groups of businesses and critical services use only their own physical or proprietary virtual communication lines without connections to the Internet and to the LAN of the own company. The interoperability between networks is difficult with many technical and contractual problems. Complexity and traffic between net-works cause higher costs. Service providers will continue to develop their own “isolated” products as long as they can ensure their own existence in the business. Due to keen competition and cost pressure, investments into security without clear return of invest have been reduced to a minimum. Information security related actions including security-related data handling are largely outsourced because of cost optimisation. Different wireless networks are not well integrated and thus they have security features of their own, which are not compatible with other wireless networks. The overall feeling is that networked, especially wireless, communication is insecure.

Conclusions and prospects

Identification and control of the risk potential of future CIs require a consequent scenario management based on a systematic scenario management process. Cornerstones of such a scenario management are

- early detection of weak signals of new trends and threats,
- design and assessment of future scenarios,
- risk analysis based on these scenarios and
- identification, assessment and introduction of suitable protection measures.

The methods for the first two steps have been developed and successfully applied in the IRRIIS project. Up to now, the two basic scenarios “Internet driven open market” and “Concentration and private network” have been developed. Scenario 1 presents a situation with increasing “liberalisation of CI market” and increasing exploitation of “sophisticated and converging networks”. Liberalisation has led to an efficient EU market and CIs have grown together to international CIs. Free trade throughout Europe is facilitated by open markets, harmonised rules and transparent trading procedures. Services and applications are based on common standards that are available to everyone. The importance of information security is understood and holistic approaches to manage security issues are used. New systems often utilize built-in security standards.

Compared to scenario 1, scenario 2 assumes a low rate of change with respect to “liberalisation of CI market” and “sophisticated and converging net-works”. Markets are fractionalised due to insufficient standardisation and harmonisation, what limits competition and raises development costs and maintenance costs. Reliability and security of systems has remained technically poor and the data security is based on isolation of proprietary networks.

The both extremely different scenarios provide a basis for a subsequent risk analysis focused on (inter)dependencies of the considered CIs. In this context, a challenging task will be to analyse risk factors emerging from the different service providers with their varying service level agreements (SLAs) and behaviours.

NESSI and ESFORS: Paving the way towards secure software services

Together with the NESSI Technology Platform, ESFORS coordination action is bringing together different EU stakeholders from software engineering and IT security domains, with an objective to provide a unified view for European research in Secure Services Architectures and Software Infrastructures.

Aljosa Pasic

Head of Area at Atos Origin Research and Innovation.
Chairman of NESSI working group „Trust, Security and Dependability“
Aljosa.Pasic@atosorigin.com

ESFORS: www.esfors.org
NESSI: www.nessi-europe.com

The service centric ICT is changing the way infrastructure and applications will be managed and delivered, and, as such, is the main focus for security considerations of IST FP6 coordination action ESFORS, as well as for NESSI working group „Trust, Security and Dependability“. The recent workshop held in Paris in September 2006, shows that there is growing interest in this part of security and software engineering research. A number of conclusions, as well as the future road mapping are some of results of this workshop with over 70 participants.

> **Trust, dependability and security cannot be “bolted on”; it should be “woven in”.**

European Technology Platform NESSI and NESSI working groups

Promoted by thirteen major European ICT corporations, totalling almost a million jobs and about 300 B€ revenues, the NESSI (Networked European Software and Service Initiative) Technology Platform aims to develop a visionary strategy for software and services driven by a common European Research Agenda. The NESSI European Technology Platform has been officially launched on September 7th, 2005 in Brussels. During the last NESSI General Assembly, held 8 of June 2006 in Brussels, there has been an opportunity to present the Working Groups as well as NESSI contribution to the 7th Framework Programme. New Partners and new Community Members have also been announced during that event. One of the first NESSI Working Groups (NWG) to officially get approved and to start with its work is focusing on „Trust, Security and Dependability“ (TSD). NWGs are the privileged mechanism to participate in NESSI and provide input in its core activities. Other projects and initiatives, including relevant Specific Supporting Actions (SSA) and Coordination Actions (CA), are invited to provide input and coordinate their activities with NESSI through the participation of their members in appropriate NWGs.
NWG Members may develop or contribute documents as input to the preparation of the NWG deliverables. These documents will be published in future through the NWG section of the NESSI website (http://www.nessi-europe.com).

ESFORS, a Coordination Action that brings together the right stakeholders

ESFORS (http://www.esfors.org) is a coordination action that aims at bringing together the European stakeholders for security and dependability Information and Communication Technologies (ICTs) to address the security and dependability requirements of emerging software service platforms.

The project will complement already existing coordination actions, e.g. SecurIST, to help shape the security and dependability content within the European Strategic Research Agenda. It will co-operate with SecurIST to ensure that open service requirements are incorporated into the SecurIST security and dependability technology roadmap and that the roadmap is incorporated into the research agenda of the software and service research community. In matter of fact, ESFORS will act as a bridge between two communities: the software and services application community and the security and dependability community.

In order to take into account the views and experience of the experts and stakeholders in the field of security and dependability of software and services, the ESFORS project has gathered an elite expert group of researchers and experts from academia, industry and research institutes. The membership of this group is composed of well-known experts that are active in other European projects and in industry. Moreover, experts from nearly all states of the European Union are present in the ESFORS expert group.

Building secure software & services also means matching people's expectations and notions of trust

ESFORS conferences and workshops are the main vehicle used by the project to give a voice to the expert groups to present their ideas and discuss what the future research challenges in security and dependability ought to be in prospective European research programs. Such workshops are organized with particular topics that deal with security and service oriented software architectures and infrastructures.

Today responses to future challenges and future responses to today's challenges

Software applications will be broken into separately managed component services and will form so called service eco-systems. This has many security consequences: first, applications will need to utilise components out of different domains of control that require to obey separate security policies and ask for diverse security and dependability qualities; second, components may be owned and operated by different organisations so that informal company arrangements will have to be replaced by formal agreements resulting from partially mechanised negotiations; and third, the services will be shared between many consumers which implies advanced confidentiality and isolation requirements.

The ubiquity of mobile technology is likely to introduce more mobility characteristics into ICT-based business models. As a result, trust and security will become a far greater preoccupation for users of such services, and therefore it must be properly addressed at the service design and deployment stages.

Service ecosystems would operate in a specific (expected) context and one of the security research challenges is to cope with unexpected events, such as intrusion and misuse.

Trust relationships in multi-device environments may currently be established between two communicating devices, but the propagation of such relationships to other devices or network entities (such users, devices or applications) which are part of the communication is not trivial to do in a seamless way.

Comprehensive Risk and Security management framework should orchestrate and multiply the potential offered by diverse security technologies and this yields for beyond state-of-the-art research on methods to detect, assess and alert on malicious activity originating from different, ICT and non-ICT, sources and the real-time ability to apply results of this assessment on a systems responsible for the enforcement of security functions.

Other challenges include such as: secure access to service registry, service and identity federation, security related SLA (service level agreements) issues, secure (re) configuration and reallocation, security for service discovery mechanisms, security policy semantics, security and trust context identification (including computational trust), portable reputations, security self-monitoring, self-healing, resilience and stabilization.

Joint Workshop on Software Engineering, Trust, Security and Dependability

It is clear from the list above that the coordination effort and a broad discussion is needed in Europe in facing new challenges as well as measuring progress we make towards security and trust in the Internet. A 2-days workshop organised jointly by EC, NESSI and ESFORS in Paris on 6 and 7th of September was a clear step in this direction. During this workshop, each participant contributed in the best possible way, through the participation in one of these three streams: Secure applications and security services, secure service ecosystem and finally stakeholder expectations. An innovative brain writing methodology has been used in order to obtain the best possible balance between different opinions and point of views.

The result of this workshop has been summarised and has been prepared as the input for NESSI TSD working group meeting, held the day after, also in Paris. The idea of this meeting was to map workshop results to NESSI strategic research agenda (SRA) and to work towards the right level of abstraction. A number of future actions have been envisaged in order to expand SRA both in breadth and in width.

A broad approach to the dependability of IP networks

IP networking offers a tempting vision of a unified information infrastructure. However, dependability aspects of this infrastructure pose difficult problems that require broad, multidisciplinary attention.

Dr. Ilkka Norros

Research Professor
VTT Technical Research Centre of Finland
ilkka.norros@vtt.fi

The information infrastructure is changing towards IP

It is commonly believed that the three main sectors of electronic communication, voice, television and data transfer are converging to a largely unified infrastructure, where the key role is played by one generic service, the global delivery system of Internet Protocol (IP) packets. It is then more than natural to ask questions about the dependability of IP networks, i.e., about their availability, reliability, controllability, vulnerability, security, etc. Can one rely on an IP-based infrastructure as much as on the traditional technologies?

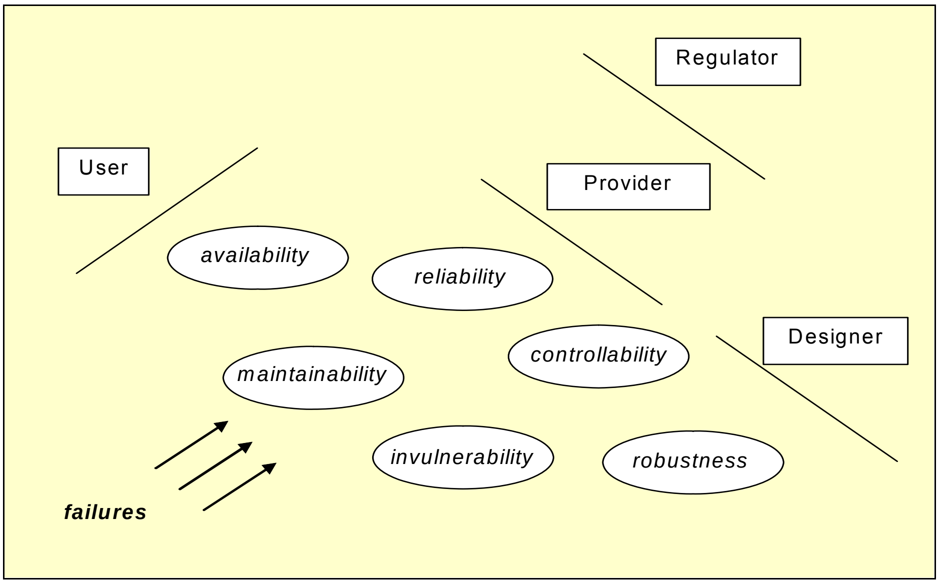
The IPLU project

The Finnish research project IPLU, "Dependability evaluation methods for IP networks" (http://iplu.vtt.fi), studies conceptual frameworks and methods for assessing this complex set of problems. The research is done by VTT (Technical Research Centre of Finland) and funded by several organisations, including Ministry of Traffic and Communications, National Emergency Supply Agency and four telecom operators. Since the project aims at a comprehensive view on the topic, it has a multidisciplinary character combining VTT's expertises in telecommunications technology, teletraffic and network modelling, and reliability analysis.

IPLU's baseline paper, available from its website, sets the scene for structured discussion of dependability problems in IP networking. The Internet is recognized as a new medium whose character is more generic than the traditional electronic communication media (in fact, it realizes Marshall McLuhan's vision which seemed so obscure to his readers in the 1960's). We propose a conceptualization of dependability, where a traditional set of dependability attributes is augmented by aspects that reflect the self-regulation features of many Internet protocols. The generic actors and aspects of the complex problem are depicted in the following picture. Let us briefly discuss each actor's point of view.

User point of view: IP medium

The generic User represents both individual and corporate users (their demands may vary up to global scale virtual private networks). When the IP convergence proceeds, the availability of IP connectivity becomes the central demand of the information infrastructure. No doubt the user does not consciously send individual IP



packets but communicates over particular applications. These often require various higher layer auxiliary services (e.g., home location register), of which failure would make the application unusable. However, it is important to note that we are entering an era of abundance of such IP-based services. If a particular service is lost, the user can try another to satisfy his communication need. If, however, the IP connectivity is lost, all "teleactivity" of a user will be paralyzed in the full All-IP vision.

Designer's point of view: problems in IP architecture

By the generic designer we denote all those instances which have created the IP architecture and protocols and develop them further: scientists, engineers, standardization organizations. At the same time as we note our indebtedness to their ingenuity and visions, we also note their "responsibility" for the weak points of the current architecture, and consider improvements in this area a necessary part of the improvement of the dependability of our information infrastructure.

If the IP connectivity is lost, all "teleactivity" of a user will be paralyzed in the full All-IP vision.

Indeed, IP was not originally designed to its now envisioned role but has grown to that. Like organic life, the IP architecture is deeply bound to designs made in its early history. At least the following features are now problematic:

- security is not inherent in the design; there is no separation of user plane and control plane,
- service rate guarantees are not inherent either; high quality usually requires light traffic load,
- the network operator's traffic control capabilities are rather restricted and
- higher level routing, provided by the Border Gateway Protocol (BGP), has stability problems and is seriously sensitive for configuration errors.

On the other hand, the Internet resembles organic life also in being under constant attack and load by malicious and detrimental elements, and surviving and getting stronger through learning in this fight. For example, it is noteworthy that the Domain Name System (DNS) has resisted serious denial of service attacks thanks to the introduction of mirroring and anycasting.

Network provider's point of view: imperative of profitability

The generic provider includes both network operators and the network equipment manufacturers. The division of labour between them has been shifting towards the manufacturer's side, and the operators' research activity has been shrinking.

Moreover, Internet service providers are often separated from the transmission providers, and both may outsource parts of their actual network operation to specialized companies. The whole picture of the network infrastructure has developed to a mosaic of independent but interdependent systems that do not respect the borders of countries.

Profitability is an imperative for most network providers, and they face fierce competition with each other. This may set difficult conditions for the improvement of dependability. For example, the highly resilient SDH transmission systems are being replaced by ten times cheaper Ethernet solutions of which the basic design was made for office networks and it is difficult to transform to a truly "carrier-grade" infrastructure. Another kind of problem is caused by the free IP telephony that will move a large part of voice transmission outside the dedicated telephone networks and thus threaten their profitability. This poses a serious problem in the total picture of electronic communication, since the criticality of the IP infrastructure becomes still higher than now.

Regulator's point of view: how to set dependability requirements?

The generic regulator contains both regulatory agencies and legislative bodies and represents the common will about the infrastructure. Most of the existing regulations concern literally only telephone networks: dimensioning rules to guarantee small call loss probability, requirements concerning emergency calls etc. IP-specific regulations are appearing - for example, the Finnish Communications Regulatory Authority, http://www.ficora.fi , has given regulations about BGP route advertisements and packet filtering. However, the task of creating an adequate body of regulations in the All-IP era is rather in its early phase.

"Dependability Case" Approaches

The IPLU project will be finished by the end of November 2006. Its proposals are still under work and cannot be reported here. One of the ideas that will be considered is to adopt the principle of the safety case methodology used to control the fulfilment of requirements for large safety-critical systems. (See http://iplu.vtt.fi/digitalo/up-conf.pdf .) This method transforms claims concerning the system into structured evidence for the fulfilment of these claims. We expect that a similar "dependability case" approach would be fruitful both as regards Service Level Agreements (user-provider relation) and as regards laws and regulations (provider-regulator relation).

Interdependencies & vulnerabilities of Energy, Transport and ICT

The third EAPC/PfP Workshop on CIP & CEP has attracted more than 110 participants from 33 countries. It has focused on three key sectors and assessed their interdepecncies and vulnerabilities as well as appropriate counter-measures.

Stefan Brem

Stefan Brem received his Dr.phil. in Political Science at the University of Zurich in 2003. He is International Security Policy Officer at the Centre for International Security Policy (CiSP) of the Swiss Federal Department of Foreign Affairs.

The CiSP has issued Workshop Proceedings that contains the Programme, the Speakers' list and selected written contributions. The Proceedings can be ordered at the following address: zisp[at]eda.admin.ch.

A set of the presentations and speeches of the Workshop can be found on the following Web site: http://pforum.isn.ethz.ch/events/index.cfm?action=detail&eventID=252

After two successful events in 2003 and 2004, the Centre for International Security Policy (CiSP) of the Swiss Federal Department of Foreign Affairs has organised a third Euro-Atlantic Partnership Council / Partnership for Peace (EAPC/PfP)[1] Workshop on Critical Infrastructure Protection (CIP) and Civil Emergency Planning (CEP) specifically focusing on interdependencies and vulnerabilities in the energy, transportation and communication sector.

More than 110 participants from 33 countries attended the Workshop that took place from 22 to 24 September 2005 in Zurich. For the first time, the event included representatives from the private sector (infrastructure owners and service providers) and the Mediterranean Dialogue[2].

From interdependencies to better understanding of risk factors and vulnerabilities

While the objectives of the two first workshops was basically to raise awareness and gain a better understanding of more general CIP concepts, the 2005 event specifically focused on interdependencies and vulnerabilities in the energy, transportation and communication sector.

Knowing the interdependencies is key to understand the vulnerabilities of CIs.

The particular goals were to get a better understanding of the risk factors and vulnerabilities as well as interdependencies of the different critical infrastructures in those sectors; exchange information and experience between individual countries, international organisations, academic experts and private sector as well as share lessons learnt from recent cases; and improve CIP by looking into issues of prevention, counter-measures and defence as well as consequence management.

Based on informative and insightful presentations the participants engaged in fruitful discussions. These presentations were given both in the plenary sessions and in the working group panels by governmental and academic experts as well as representatives from international organisations and the private sector.

This workshop has broadened its geographical reach and deepened the understanding of CIP

The participant's acknowledged that tremendous progress has been made since 2003. When the workshop series has started two years ago, participants were still reluctant to share information and experience. At its third edition,

[1] The Euro-Atlantic Partnership Council (EAPC) is the multilateral political framework that includes the 26 NATO allies and the 20 PfP partners.
[2] The Mediterranean Dialogue includes seven countries: Algeria, Egypt, Israel, Jordan, Mauritania, Morocco and Tunisia.

three parallel panels in all the working groups were specifically dedicated to the presentation of case studies and exchange of lessons learnt.

Recent events, ranging from the consequences of the 2002 Danube flood to the communication system to a comparison of several case studies of major blackouts in Europe and North America to a complete power failure of and severe flood damage to the Swiss Federal Railways in the summer of 2005 highlighted the interdependencies and vulnerabilities of the critical infrastructures.

Increased number of participants and more focused human network of experts

Also the increase in participants from around 60 to more than 110 in just two years is a clear indicator of the value of this Workshop series. The interest in CIP issues has also spread geographically – the number of represented countries has risen from 25 to 33. The event has also become more multi-disciplinary and provided a platform for inter-agency dialogue. The inclusion of the private sector offered the opportunity to deliver a series of useful examples of working public-private partnerships.

The private sector delivered a series of useful examples of working public-private partnerships.

However, there is still a need for further enhanced dialogue, pragmatic steps and coordination among all actors involved. This is the reason why Switzerland intends to remain active in this area and has offered to host a follow-up event in fall of 2006.

While the energy, transportation and communication sectors face different risk factors and vulnerabilities it is also evident that one serious interruption or failure in one sector can set off cascading effects in one or even several other sectors (for example banking and finance, public health, key industry infrastructure, etc.) at the same time.

The workshop stressed the need to further investigate the interconnections between various key infrastructure sectors and has identified energy, transportation and communication as the most important sectors in all the countries concerned. This is also the reason why they will remain on top of the agenda and will also be included in the 2006 edition of the EAPC/PfP Workshop series.

The workshop also showed that today’s liberalised and interconnected markets make it more difficult to control and protect critical infrastructures, especially those that cross borders (e.g. transmission power grids, information and communication technologies, oil and gas pipelines, international railtracks, etc.).

Assets very often belong to private companies. The way public-private cooperation is being addressed and preparatory and emergency measures are being taken differs from country to country.

It was stated during the workshop that clear structures are needed and the role and responsibility of each actor should be well defined before an incident takes place in order to facilitate a swift and efficient reaction in an emergency situation.

Given the impact that interruptions or failures in the energy, transportation or communication sector might have on neighbouring or even further away countries it is probably not enough to look at the national level only. International and particularly regional cooperation and coordination should be discussed and implemented.

The analysis of interdependencies and vulnerabilities as well as the resulting risk assessment are first steps that become more and more significant. Quite understandably nations as well as private companies are still reluctant to share specific information on their vulnerabilities – both for business as well as security considerations. Trust building and transparency are therefore key elements to an improved cooperation and to an effective early warning system. Discussions have shown that events like this workshop assist in the indispensable trust-building endeavour that provide a platform for the exchange of information and experience. It is a valuable tool to collect and disseminate practical information and lessons learned.

Importance of collection and dissemination of practical information and lessons learned

A volume of the CiSP Proceedings has been issued that contains the programme, the speakers' list as well as selected written contributions of the 2005 Workshop. The CiSP Proceedings can be ordered via e-mail: zisp[at]eda.admin.ch.

Further information on the workshop as well as a set of the presentations and speeches of the workshop can be found on the following web site: http://pforum.isn.ethz.ch/events/index.cfm?action=detail&eventID=252.

ILGOV-CERT: The creation process of a governmental CERT

In 2005, the Israeli government decided to create a governmental Computer Emergency Response Team (CERT), in order to fill an increasingly evident void in Israel's IT security sphere. There are many struggles accompanying the birth of a CERT project, but the original need overcomes them all.

Mr. Boaz Dolev
and the ILGOV-CERT members

Director of the Israeli E-GOV department and head of the TEHILA project, a part of the Israeli Ministry Of Finance.

Mr. Dolev is in charge of initiating planning and executing a wide range of projects in the field of Electronic Government.
E-mail: boaz@tehila.gov.il

The original ILGOV-CERT team was founded by iTcon-LTD, and all its current members were located and trained by it.
For more information regarding iTcon, please visit http://www.itcon-ltd.com

Over the past few years it is becoming clearer than ever that the Israeli IT security industry contains a void, which needs to be filled. Along side the drastic increase in computer based criminal activity; one can also see the increase in security awareness in all sectors of the population. IT managers, as well as system administrators and even the average man on the street, all are searching for a reliable and digested source of information, in order to maintain a proper and stable IT security policy.

Due to the extremely high rate of internet connectivity in Israel (approximately 65% of the Israeli households had broadband internet connectivity in early 2006); the problem is never finding a source answering these criteria. The problem is that there are so many of them.

Why create a governmental CERT?

The Israeli Governmental Computer Emergency Response Team (ILGOV-CERT) project was created in order to establish a unified governmental Israeli IT security front. Its goal is to make all relevant information public and accessible to governmental offices and agencies. In order to make better use of the information gathered, and in light of the current absence of an Israeli "civilian" CERT, The ILGOV-CERT project commits itself to always supply its clientele with the latest, most accurate and full information. Currently, this goal is achieved via a publicly available web site, constantly updating. Future plans contain more proactive methods, such as use of emails, fax, text messages and more.

The ILGOV-CERT project was created as a subsidiary project of TEHILA – The governmental ISP, and the branch in charge of all government related computers infrastructure. Among its other responsibilities, TEHILA provides secure web hosting for all government sites, secure payment portals for various governmental services and e-commerce infrastructures.

Due to this positioning, a large part of the ILGOV-CERT's clientele comprise of the various governmental offices and branches. However, all ILGOV-CERT publications are specifically written such that the technical population, the IT managers and the average guy, all can easily extract the knowledge relevant to them.

The ups and downs

During the relevantly brief time the ILGOV-CERT exists, it has been facing several difficulties. Nevertheless, each and every one of these difficulties was and is a chance to better the project.

One of the most unique problems the project has encountered was actually derived due to its positioning in the governmental hierarchy. The project's first responsibility lies in its governmental clients. All of these clients are represented by the same point of contact – TEHILA. This has created a unique and interesting situation. Not only the head of the TEHILA project is supposed to be the ILGOV-CERT's overseer, it is its main client.

On the one hand, this situation demands him constant attention, finding the thin line between the responsibilities for both sides. It is to be said, however, that in its core, the ILGOV-CERT project is a very independent one, and does not usually need to be approached by its clients in order to proceed with every day goals. On the other hand, it is because of this unique situation, the clients' representtative can be fully confident that the project is in good hands, and can monitor it in all its aspects.

A second difficulty the project has faced is one shared among all CERT projects world wide. As the project strives to present its client with one good source of information, that information needs to be gathered from the countless other sources available. After a period of great effort, the project has been able to define its main sources of information. It has been discovered that by covering a few carefully selected sources, the project is able to gather almost all the information it need. Among these sources are publicly available sites and mailing lists, as well as custom and paid for sources of information. On top of these sources, the ILGOV-CERT has been able to create fruitful relationships with major vendors, allowing it to receive crucial information in zero time.

Coordination Striving

As said before, the ILGOV-CERT project was created first and foremost as a unified portal of IT security knowledge. However, it is the project belief, as well as its creators, that by collecting and digesting only theoretical knowledge, one can only walk a certain length. To really hold all the cards, as they saying goes, the project has to "brand" itself as the place its clientele should turn to in signs of IT security trouble. Only by receiving and coordinating actual information regarding attacks, policies, infrastructures, and all things security related, from as many sources as possible, the Computers Emergency Response Team can really live up to its name.

Furthermore, due to recent events, it has become evident that the state of Israel itself needs the project to fulfil this role too. The virtual Israeli border is attacked on a constant and frequent level. Israeli governmental and commercial web sites and infrastructures are a target for every cyber-terrorist and "hacktivist" in the world. So far, the TEHILA project has been able to hold off almost every attack on governmental web sites to date. This aside, in the lack of a true computer emergency coordination centre, it has been difficult to spot comprehensive attacks on Israeli infrastructures, and all forensic work has been done retroactively. As this "branding" process continues, TEHILA and ILGOV-CERT has been able to quickly and accurately identify attacks on various Israeli sites, and respond to it accordingly. In this manner, many relevant position holders in the market were notified in time, and heavy damages were prevented.

Although ILGOV-CERT has faced some difficulties, as listed above, the project also found itself to be holding several advantages over other similar groups. One of these advantages is attached entirely to TEHILA's role in this virtual defence. Resulting from the threat level described earlier, over the last decade the TEHILA project has accumulated vast amounts of knowledge, experience and information regarding hackers' activity and general security matters. The full access to these assets advanced the CERT project beyond the greatest expectations.

Cooperation and Collaborations

A major part of the ILGOV-CERT's vision as a coordination centre, is to create collaborations with as many sources of information as possible.

One of the first orders of business for the ILGOV-CERT project was to become a full pledged member of the FIRST organization. FIRST is a global organization consolidating IT security projects from around the globe, in the emphasis of cooperation between them.

Another ongoing collaboration project is the establishment of a new research institute by the Inter Disciplinary Centre College. The IDC, one of Israel's leading academic institutes, is the first Israeli institute to develop and execute an academic program, resulting in a Computer Science BA degree, with a specialization in IT security. Along side this program, the IDC established a new research institute dedicated to the study of Internet Security, through various aspects. The ILGOV-CERT is a full partner and endorser of both programs, and is involved in their designing and architecture stages.

Furthermore, besides specific programs and projects, the ILGOV-CERT maintains close relationships with other CERT projects around the world. The project is always looking to expand its "social" network, sharing knowledge, experience and methodologies.

Young but determent

In comparison to equivalent projects in the world, the ILGOV-CERT is young and it still needs to grow. This said, the project was preceded by careful and thorough planning, a result of years of experience in the TEHILA project, allowing a quick and stable transition into operating status. Nevertheless, ILGOV-CERT is always looking for ways to better itself, whether by constant self tutoring, and ever growing relationships with many and various counterparts. We are looking forward to continue our mission as best we can, and do our part in the bettering of Israel's and the world's IT security.

Information security surveys as instrument of risk analysis

To evaluate the threats to information security, it is essential to know the frequency and quality of breaches in companies. Such information can be derived from surveys. This article discusses the strengths and weaknesses of surveys.

Manuel Suter

Center for Security Studies, ETH Zurich (Swiss Federal Institute of Technology)

suter@sipo.gess.ethz.ch

A fundamental concern of risk analysis is the identification and quantification of threats. The questions “What can go wrong?” and “What is the likelihood of it going wrong?” have to be considered carefully. Thus, in the domain of Critical Information Infrastructure it is important to know the quantity and quality of threats to information security. But the data for these threats are hard to come by. One possible option for completing this task is to conduct computer security surveys.

There are currently plenty of such surveys available, however, most of them are conducted by commercial IT-security companies and exist for marketing purposes rather than as a scientific endeavor to clarify facts. To gain more independent knowledge, several national organizations responsible for information security have undertaken their own studies. The best known among them is the annual CSI/FBI “Computer Crime and Security Survey,” as well as the survey “Hi-Tech Crime – the Impact on UK Business 2005” by the UK’s NHTCU (National Hi-Tech Crime Unit) and “The IT-Security Situation in Germany in 2005” by the German Federal Office for Information Security (BSI). The latest example is the survey “Information Security in Swiss Companies,” conducted by the Center of Security Studies (CSS) at ETH Zurich at the request of MELANI (*Melde- und Analysestelle Informationssicherheit*) the reporting and analysis center for information security of the Swiss government.

Drawing on the experiences gained in composing the Swiss survey, I’ll discuss the strengths and weaknesses of information security surveys as instruments of threat evaluation.

Often, expectations on information security surveys are exaggerated.

The challenges of information security surveys…

First, it is important to clarify that surveys aren’t able to accurately map the current-state analysis of threats to information security. There are simply too many methodological obstacles such surveys have to confront: first, the willingness of the companies to provide information about their problems with security (information that may be restricted for obvious reasons). This can make it difficult to build a sample big enough from which one can make generalizations. Another difficulty is the great diversity among companies. Threats to information security affect different companies to very different extents. Therefore, accurate statements about threats to information security of companies in general are extremely difficult to make.

I will discuss the methodological obstacles and requirements at length later in this article. But, it’s enough to emphasize that exaggerated expectations are often the biggest challenge to information security surveys and may entice researchers to present results that can only be weakly confirmed. For example, despite the difficulty, surveys often aim to precisely assess the average losses that companies suffer as a result of computer crimes.

…and their potential

But even though surveys aren't able to quantify threats precisely, investigations on information security in companies are still worthwhile. Actually, for the purpose of risk analysis, there is little need to tally the cost of threats, it is more relevant to discover or confirm trends and probabilities. It is also more important to investigate the type and frequency of incidents detected in a given type of company, instead of extrapolating the costs of threats. Findings on the frequency of incidents are essential for the setup of early-warning approaches. Furthermore, because many current threats originate in so-called botnets (infected computers linked in a network), threat estimations must also take into account the level of ICT-protection and risk management in companies. A common assumption is that companies tend to spend as little as possible on safeguarding information security, which could possibly result in insufficient protection, and would in turn increase the risk of attacks originating from infected computers. Again, one shouldn't expect surveys to accurately determine the overall quality of risk management in companies. Still, it is possible to examine some indicators, such as the diffusion of technical or organizational security measures, the financial and personal resources allocated to information security, or the outsourcing of risk.

Surveys deliver important insights into the threats facing companies, as well as into the use of security measures.

Such basic facts for threat estimation are only available through broad surveys among companies. In addition, conducting surveys may strengthen a company's awareness of security issues. By completing a survey, information security officers possibly gain new insights into the state of measures taken in their companies. The results of the survey may also help the officers to convince company management of the importance of additional measures. Thus, indirectly, surveys may play a role in risk management.

Finally, a survey is also a suitable instrument for testing the acceptance of innovative ways of solving the IT security problems. The survey participants could be asked, for example, which forms of joint action interest them. With questions of this type, it is possible to appraise (in advance) the chances of success of new solutions to the problem of information security.

In short, while surveys cannot quantify the threats to information security precisely, they can deliver important insights into problems facing the companies, preferred security measures, and new possible solutions.

Methodological requirements are rather demanding, however, they serve as guidelines for every survey.

Methodological requirements

The quality of survey results depends on the accurate application of methodological requirements. The biggest methodological challenge is the definition of the sample pool. Not only must the size of the sample pool be considered carefully, but its composition should be as well. There are many significant differences between firms that may potentially influence a firm's risk management approach. Common differentiating criteria included in information security surveys are company size and business sector. Depending on whether conclusions should be drawn from company size and individual business sectors, the size of the sample pool has to be converted, or a disproportionate sampling approach should be taken (e.g. quota random sampling, whereby individual strata are over- or under-represented – something that has to be rectified subsequently by weighting).

Of course, the response rate is also crucial for the quality of the results. To avoid the danger of too small a representation of categories, it is helpful to set a numerical target for each category in advance. In addition, the mere fact that a company responds to the survey may be a sign that it takes the subject of IT security more seriously than others do. Thus, if the respond rate is low, it may be necessary to properly compare the respondents with the non-respondents.

A further methodological challenge is the creation of the questionnaire. As mentioned, it is disadvantageous to ask questions of great complexity. Respondents will abandon the survey if they don't understand many questions, or worse, they will give false answers. Also, the questions shouldn't be too sensitive as some companies won't give an answer for security reasons. In short, the simpler the questions are, the better the interpretation of the results will be.

The methodological requirements for such a survey are rather substantial and it is almost impossible to fulfill all of them completely. However, to assure the quality of the results, these requirements should serve as guidelines for every survey.

The results of recent surveys

The most recent surveys strive for somewhat different goals, but they have important commonalities. In particular, the similarities among the results are interesting for risk analysis, as they indicate global trends in information security threats. Therefore, it is interesting to compare the most important results of the US, British, German and Swiss surveys.

As expected, all the surveys show that viruses, spyware, trojans and other malware are by far the most frequent breaches noted. Because the sample pools of the surveys are different, it is rather difficult to compare the percentages of companies affected. However, it can be clearly stated that malware is the most widespread threat. Another interesting finding is that in all the country surveys (except for the German survey, in which the question wasn't included), the conventional equipment theft is one of the most frequently cited incidents. In addition, the comparison also shows that the most sophisticated attacks in technical terms (that also have a more serious impact) are less frequently encountered in all countries surveyed.

International and chronological comparisons of surveys could help to identify trends.

The findings about the technical security measures are analogical. All of the surveys analyzed indicate a nearly uniform use of firewalls and antivirus software across companies. Meanwhile, more complex technologies such as intrusion detection and biometric systems are rarely used.

These examples show that most of the results in the surveys aren't astonishing. Nevertheless, they are valuable because they serve to confirm trends. But above all, the results constitute the basis for further investigations and provide a global perspective on IT-security threats.

Suggestions for future surveys

Some of the cited surveys are already a tradition. For example, the FBI/CSI "Annual Computer Crime and Security Survey" is in its 11th year. This is remarkable since continuity is a precondition for all research into developments. Surveys don't have to be repeated annually and the questionnaires don't have to always include the same questions. Though, it would be interesting if future surveys could highlight trends by formulating questions in the same manner as current surveys. Therefore, the first suggestion for future information security surveys is that they should include some similar standard questions. This would ease the comparison of survey results, whether international or chronological. In my opinion, standard questions should be rather basic, such as questions about the frequency of incidents. Detailed questions about the amount of losses sustained and losses by type of attack, for example, are hardly comparable, as respondents' answers may change over time and may vary between the different countries. Unfortunately most current surveys concentrate too much on these kinds of questions.

The second suggestion concerns the composition of samples. The Swiss survey showed significant differences between the various companies. It is important to note that the size of the company has a great impact both on the frequency of incidents, as well as on the use of security measures. It would be beneficial to design future surveys to take this into account and differentiate between categories of size. Furthermore, surveys should distinguish between the business sectors of companies surveyed, since in all likelihood, companies of some sectors (e.g. the financial sector or IT services) are much more affected by incidents than firms in other sectors, such as the hospitality (hotels and restaurants) or the manufacturing sectors.

Finally, as a third suggestion, I would propose to include more questions referring to the needs of companies. Granted, such questions go beyond the scope of risk analysis, but they are indispensable to evaluate new solutions to the problems of information security.

Conclusion: The prospects of information security surveys

We can conclude that information security surveys are not a panacea for risk analysis. However, they are an applicable instrument for gathering information on the nature of threats. In order to be effective, the surveys must be conducted in a methodological manner and the interpretation of the results must be consistent and reliable.

Finally, it should also be mentioned that information security surveys do not yet tap their full potential as instrument for risk analyses. Comparing the results of different international surveys could provide a better overview, and with chronological comparisons it could be possible to identify new developments with regard to threats.

See www.crn.ethz.ch for an online version of the Swiss survey.

1st International Workshop on Critical Information Infrastructures Security

The CRITIS 2006 workshop attracted the interest of both academia and industrial experts with high-quality papers and a remarkable invited talk, creating an appropriate environment where all attendees shared their experiences and discussed about CIIP.

Javier Lopez

CRITIS'06 Program Chair

University of Malaga
Computer Science Department
Tel: +34-952131327
jlm@lcc.uma.es

Slides available: http://critis06.lcc.uma.es

The First International Workshop on Critical Information Infrastructure Security (CRITIS 2006) was born as an event that wanted to bring together researchers and professionals from universities, private companies and public administrations interested or involved in all security-related heterogeneous aspects of Critical Information Infrastructures.

The workshop was held on August 31st and September 1st 2006 in Samos Island, Greece. It was hosted by the Laboratory of Information and Communication Systems Security (Info-Sec-Lab), University of the Aegean. It was held in conjunction with the 2006 International Information Security Conference (ISC'06).

An organizational success

The program committee of CRITIS was composed by an international group of recognized experts in both information security and critical information infrastructure protection. The committee worked efficiently in order to obtain a high-quality program that could be important and relevant to the actual CIIP context.

In response to the CRITIS 2006 call for contributions, 57 papers were submitted. At the end of the reviewing process, only 22 papers were selected for presentation, resulting in an acceptance rate of 38%. The workshop received contributions from all over the world, and the final papers were authored or co-authored by researchers coming from the public and the private sector of 16 different countries from Europe, America and Asia.

In total, the workshop had around 50 attendees. The quality of the contents of the workshop was corroborated by the good level of participation in the discussions that took place during and after the sessions, discussions that became more interesting due to the heterogeneous nature of all the attendees.

The workshop received submissions from all over the world, resulting on a high-quality and attractive program.

Invited Talk

CRITIS 2006 was fortunate to have Mr. Andrea Servida, Deputy Head of Unit of the European Commission (Information and Society and Media Directorate General) as invited speaker, giving the talk “Security and Resilience in Information Society: The European Approach”.

In his talk, Mr. Servida stated that in order to achieve a trustworthy, secure, and reliable ICT, it was necessary to deal with problems that can be classified into four dimensions: technical, economical, social, and legal. In addition, he commented that it was important to assure an open and inclusive multi-stakeholder debate in order to create a secure Information Society, where all actors could dialogue and participate in the global decisions.

The concept of Critical Infrastructures arose when the dependences of our civilization in such Information Society became clear. Then, Mr. Servida presented the plans on CIIP of the European Union, pointing out the challenges of the CIIP dialogue, such as organizational issues, policy issues, and information sharing and continuity issues, amongst others. Finally, Mr. Servida presented the plans of the European Union for the FP7, where CIIP play a crucial role.

After the talk, the attendees translated their interest into some questions. They ranged from the social point of view, like the responsibility of the normal user in the maintenance of security in today's context, to the emergent problems that our society was helping to create, such as the need of collaboration policies or the issue of identity theft.

Research Talks: Day One

The scientific program of the workshop was organized into 8 sessions. In the first session, P. Veríssimo, from University of Lisboa (Portugal) proposed a distributed systems architecture that allows the secure integration of the different realms in a CII system, maintaining essential properties such as reliability, fault tolerance, and attack prevention. Also, P. Mellstrand, from Bleking Institute of Technology (Sweden) described a combined experimental approach that could be used to build targeted resilient software required for critical infrastructures.

The second session focused on risk assessment and security modelling. In this sense, S. Naqvi, from the Centre of Excellence in Information and Communication Technologies (Belgium) presented a methodology for modelling security requirements of grid data management systems (GDMS), which was also able to derive the security policies directly from those requirements. Then, F. Baiardi, from University of Pisa (Italy) presented a framework to define risk mitigation plans based upon a ranking of set of countermeasures that considers alternative attack strategies of a threat. Y. Asnar, from University of Trento (Italy) introduced a goal model to analyse risk at organization level, illustrating a number of different techniques to help the analyst in identifying and enumerating relevant countermeasures for risk mitigation. Finally, R. Rieke, from Fraunhofer Institute for Secure Information Technology SIT (Germany), presented a framework for model-based symbolic interpretation, simulation and analysis, which was able to automatically compute a graph of all possible attack paths from that model of an ICT network.

In the third session, Jose J. Gonzalez, from Agder University College (Norway), described a new method for helping in the detection and prevention of social engineering attacks, recognizing dynamic patterns rather than heaps of symptoms. On the other side, the work by S. Bologna et al., from ENEA (Italy) was presented, reporting an overview of R&D activities in Europe on Critical Information Infrastructure Protection, and emphasizing the major areas of research and also identifying the most relevant lacks.

Andrea Servida presented the plans of the EU for FP7, where CIIP play a crucial role.

The fourth session focused on early warning systems. The work by K. Bsufka et al., from Technische Universität Berlin (Germany), presented an approach for an agent-based early warning system (A-EWS) for critical infrastructures, combining existing security infrastructures with new detection approaches. Urs E. Gattiker, from CyTRAP Labs (Switzerland), outlined how early alert systems can help home users and SMEs in improving their culture of security, using a security website as a case study.

Research Talks: Day Two

The second day of the workshop began with the fifth session, where J. García-Alfaro, from Autonomous University of Barcelona (Spain), presented a mechanism for avoiding remote attackers to escalate privileges on a compromised system by ensuring the administrator's identity through the use of Smart Cards. Besides, Y. Desmedt, from University College London (UK), analyzed the use of censorship as a secure tool and provided information for deciding whether one can censor a network using limited resources.

The main focus of the sixth session was about trust and its effects on Critical Infrastructures. While E. Aivaloglou, from University of the Aegean (Greece) reviewed the state-of-the-art of trust establishment frameworks for ad hoc and sensor networks, J. Zhou, from Institute for Infocomm Research (Singapore), proposed a trust enforced pervasive computing environment. On the other side, J. Forné, from Universitat Politécnica de Catalunya (Spain), proposed a protocol to build a virtual hierarchical PKI from a peer-to-peer PKI, and R. Román, from University of Málaga (Spain) introduced guidelines for choosing the right key management system in CIP/CIIP scenarios based on sensor networks.

The seventh session focused on intrusion detection and intrusion prevention systems. P. García-Teodoro, from University of Granada (Spain) proposed a method to automatically prepare the database to accurately train, test and evaluate hybrid (signature and anomaly-based) NIDS. S. D'Antonio, from Consorzio Interuniversitario Nazionale per l'Informatica (Italy), presented a distributed architecture aiming to secure the communication network upon which the critical infrastructure relies, while also proposing an innovative method to extrapolate real-time information about user behaviour from network traffic.

The workshop concluded with the eighth and final session, and focussed on both attacks against critical infrastructures and measures for detection and defence. J. Willemson, from Cybernetica (Estonia), presented a simple risk-analysis based method that, using elementary game theory, studied the security of institutions against rational (gain-oriented) attacks. D. Martínez-Manzano, from University of Murcia (Spain), analyzed the usage of the standard Session Initiation Protocol (SIP) for performing a multi domain virtual negotiation, in order to protect the exchange of critical data from the security risks of the public networks.

The work by C. Xenakis et al., from University of Athens (Greece), presented the security weaknesses and the possible attacks that threaten the GPRS backbone network and the data that either reside at the network or are transferred through it. Finally, the work by V. Stathopoulos et al., from the Authority for the Assurance of Communications Security and Privacy (Greece), presented a framework for secure logging in public communication networks, where an independent Regulatory Authority is responsible to verify the integrity of the log files.

Workshop summary

The workshop was very successful in many aspects. On a technical side, the workshop hosted high-quality peer-reviewed papers and a remarkable invited talk that attracted the interest of all the attendees, resulting on a lively debate in every session, debate that continued also after the sessions.

Besides, the organization committee achieved their goal of bringing both academia and industrial experts to the conference. As a result, all attendees shared their different points of view about the problems and solutions that we must face for protecting the critical infrastructures, creating the foundations for an open and collaborative environment faithful to the spirit of critical information infrastructure protection.

Further Information

The full program of the workshop, along with all the slide sets, is archived on the workshop web site at http://critis06.lcc.uma.es . Additionally, post-proceedings will be published by Springer in the Lecture Notes in Computer Science series before the end of the year. Also, extended versions of CRITIS'06 selected papers will be published in the International Journal of Critical Infrastructures (IJCIS).

IFIP CIP Conference will bring together international experts to tackle security challenges

The First Annual IFIP WG 11.10 International Conference on Critical Infrastructure Protection will be held at Dartmouth College in Hanover, New Hampshire, USA, March 19-21, 2007

Eric Goetz

Eric Goetz is the Assistant Director for Research and Analysis at the Institute for Information Infrastructure Protection (I3P) at Dartmouth College, USA. He coordinates and oversees I3P's research portfolio, focused on the security of cyber systems and US information infrastructures. For more information about the I3P see: www.thei3p.org

E-mail: egoetz@thei3p.org

The *IFIP Working Group 11.10 on Critical Infrastructure Protection* is an active international community of researchers, infrastructure operators and policy-makers dedicated to applying scientific principles, engineering techniques and public policy to address current and future problems in information infrastructure protection.

The *First Annual IFIP WG 11.10 International Conference on Critical Infrastructure Protection* will provide a forum for presenting original, unpublished research results and innovative ideas related to all aspects of critical infrastructure protection.

Attendees will address current and future CIP challenges by applying scientific principles, engineering techniques and public policy.

Papers and panel proposals are solicited. Submissions will be refereed by members of Working Group 11.10 and other internationally-recognized experts in critical infrastructure protection. Papers and panel submissions will be selected based on their technical merit and relevance to IFIP WG 11.10. The conference will be limited to sixty participants to facilitate interactions between researchers and intense discussions of research and implementation issues. A selection of papers from the conference will be published in an edited volume – the first in a new series entitled *Critical Infrastructure Protection: Issues and Solutions* (Springer) in the fall of 2007. Revised and/or extended versions of outstanding papers from the conference will be published in a special issue of an international journal. The event is supported by the Institute for Information Infrastructure Protection (I3P), based at Dartmouth College.

Papers are solicited in all areas of critical infrastructure protection. Areas of special interest include, but are not limited to: Infrastructure vulnerabilities, threats and risks; Security challenges, solutions and implementation issues; Infrastructure sector interdependencies and security implications; Infrastructure protection case studies;legal, ethical, economic and policy issues related to critical infrastructure protection; distributed control systems/SCADA security; telecommunications network security

Instructions for Authors – Technical Papers / Panels:

Contributions and panel proposals (in pdf format) should be emailed to the program co-chair (sujeet[at]utulsa.edu). For details and updated submissions deadlines please see the WG 11.10 website at: www.cis.utulsa.edu/ifip1110

Conference Deadlines:

- Paper/Panel Submission: December 31, 2006
- Notification of Acceptance: January 31, 2007

Conference announcement: DIMVA 2007 in Lucerne, Switzerland July 12-13, 2007

DIMVA provides an academic forum for presentation and discussion of novel research in three crucial areas of IT security: intrusion detection, malware, and vulnerability assessment. Following a very successful 2006 conference in Berlin, security researches and practitioners are now invited to submit contributions for DIMVA 2007 in Lucerne, Switzerland.

Pavel Laskov Ph.D.

Pavel Laskov is a senior scientist at the department „Intelligent Data Analysis“ in the Fraunhofer Institute FIRST. He was the General Chair of DIMVA 2006.

pavel.laskov@first.fraunhofer.de

Dr. Robin Sommer

Robin Sommer is a staff scientist at the Lawrence Berkeley National Laboratory and at the International Computer Science Institute, Berkeley, USA. He is the Program Chair of DIMVA 2007.

robin@icsi.berkeley.edu

The *Fourth International Conference on Detection of Intrusions and Malware & Vulnerability Assessment* (DIMVA) will be held in Lucerne, Switzerland on July 12-13, 2007. Following highly successful conferences in Dortmund (2004), Vienna (2005) and Berlin (2006), DIMVA 2007 will again serve as an international forum for IT security experts from academia, industry and government.

An academic forum in IT security. Since its inception in 2004, DIMVA provides an academic forum for presentation and discussion of novel, mature research in three crucial areas of IT security: intrusion detection, malware detection, and vulnerability assessment. Focusing on these three areas, DIMVA covers the reactive components of network security; in contrast to proactive mechanisms such as firewalls and secure communication. These three fields are a significant part of a good security concept, due to the fundamental lag between the times when a new vulnerability is discovered until a preventive mechanism gets in place. Despite much prior work, both in academia and industry, new attacks are developed at a brisk pace and constantly challenge existing technology.

The main objectives of DIMVA are to foster scientific exchange in the international security community and to facilitate the dialogue between academics and practitioners. DIMVA has been conceived, and is supported by, the German Informatics Society (GI). It is organized by GI's special interest group *Security - Intrusion Detection and Response* (SIDAR). Each year the conference features a dynamic two-day scientific program; exciting invited talks; active participation of academic, commercial and governmental institutions; and, last but not the least, an informal, productive atmosphere.

DIMVA 2006. DIMVA 2006 was held in Berlin, Germany on July 13-14, 2006, at the beautiful conference centre of the Berlin-Brandenburg Academy of Sciences. The conference gathered over 90 participants from 15 countries. The two-day program featured two invited talks, eleven presentations of peer-reviewed papers, two best-practice presentations, and a "rump-session" with eight informal short talks presenting work in progress. DIMVA 2006 was accompanied by two satellite events: the SPRING student workshop and the CIPHER capture-the-flag contest.

DIMVA features a two-day scientific program, exciting invited talks, and extensive interaction between researchers and practitioners.

Invited talks. In the first invited talk of DIMVA 2006, called *Reaction: the Internet security paradox*, John McHugh, Director of the Privacy and Security Lab at Dalhousie University, Canada, presented an overview of a long quest to make security reactive. Starting from the early major Internet security incidents, such as the Morris Worm, reaction has become a major issue in the agenda of security administrators. The conceived countermeasures comprised administrative actions, such as the creation of the US-CERT, as well as technical advances in protection mechanisms. Yet the underlying problem is an inherent arms-race between attack and defense. As the complexity of the systems to be protected grows, so does the chance that security holes remain open due to careless software engineering, misconfiguration or human error. To make the matters worse, the increasing degree of automation reduces the technical hurdles for intruders, thus making attacks even more likely. To raise the level of security in current and future systems, advances in both reactive and proactive security mechanisms are needed. Reaction should be based upon comprehensive network monitoring, unbiased data analysis and insightful visualization. Proactive countermeasures should span the wide range of technical and organizational actions, including improving the engineering of software, better coordination in the field of incident analysis, and raising the end-users' awareness of security issues.

In the second invited talk—*Security management - 5000 events/sec, half an engineer and automation discouraged*—Michael Behringer, Distinguished Engineer at Cisco Systems, described the main challenges for intrusion detection systems (IDS). The current state-of-the-art IDS have proven to be a vital part of security administration, yet significant effort is required to make them work in practice. Main challenges for IDS improvement are manageability, intelligence and performance. The manageability challenge amounts to automating the processing of heterogeneous security information gathered from various components: IDS, IPS, firewalls, routers, etc. Intelligence is needed to decrease false positives and false negatives, as well as to carry out decision support functionality such as correlation of multiple alarms and evaluation of potential alarm threats. Performance issues require re-thinking of intrusion detection methodology, as hardware performance is capped by physical size limitations, power consumption and heat dissipation. Future IDS have to operate in a more distributed fashion, combine a variety of intrusion detection techniques, and provide intelligent management interfaces. All this requires further advances in intrusion detection research.

M. Behringer: With sufficient thrust, pigs fly just fine; with sufficient effort, you can make your IDS work.

Technical program.
The main technical program of DIMVA 2006 consisted of five sessions on code analysis, intrusion detection, threat detection & response, malware & forensics, and deployment scenarios.

Code analysis. In the code analysis session, Ebrima Ceesay presented an approach for automatic detection of potential integer misuse in C programs. The approach extends CQual, a static analysis tool using type theory, with "trusted/untrusted" qualifiers. Certain operations, for example for memory access, are not allowed anymore for untrusted integers, and an alarm is raised if they are detected. The approach was tested on several widely used open-source programs and detected various integer-related vulnerabilities, some of them formerly unknown.

Manuel Egele presented a method for providing additional information on application-parameters to an intrusion detection system. The method performs detection of parameter names accepted by a PHP application, inference of parameter types and determination of possible value sets. The proposed method was able to detect all parameter names in six real-world PHP applications and to infer additional information (type and/or value sets) for about 35% of these parameters.

Intrusion detection. Masayoshi Aritsugi presented a technique for masquerade detection in host-based IDS using command co-occurrence matrices and Support Vector Machines. The method yields similar detection and false positive rates as the previous Extended Co-occurrence Matrix method of Oka et. al., yet is orders of magnitude faster and allows for incremental processing of large datasets.

Michalis Polychronakis addressed the problem of detecting highly polymorphic and self-modifying code, which cannot be tackled by previously used pattern matching and static analysis methods. The proposed approach based on network-level emulation and the "payload read" detection heuristic (detection of read operations from distinct areas in the input buffer) is able to reliably detect self-contained decryptors in polymorphic shell code at rates of 10-100 Mbps.

Konrad Rieck introduced an anomaly-based technique for detection of unknown network attacks using language models. The technique uses simple n-gram- and word-models for embedding network connection byte-streams into a high-dimensional feature space in which geometric similarity measures can be efficiently computed. The method was tested on a real dataset created by penetration simulation and was able to detect 80-95% of attacks with no false positives without any prior knowledge about attacks.

Threat protection and response. Colin Mulliner presented cross-service attacks, a new type of attacks against smart phones. A cross-service attack exploits vulnerability in a smart phone's OS, e.g., an insecure configuration or a buffer overflow, in order to access an unauthorized service. As a countermeasure against cross-service attacks, a resource labelling technique was proposed in which labels are assigned to various OS resources and checked against access control and exception policies. A prototypical implementation of the labelling method for a Linux OS verified its effectiveness against cross-service attacks at a cost of 10-25% performance overhead.

Yohann Thomas proposed a novel threat response approach using contextual security policies. Unlike conventional Organization-Based Access Control, the new approach explicitly accounts for prohibitions and augments policies with contexts. A threat response architecture was discussed in which contexts can be inferred from alerts in IDMEF format, incorporated into the policies and instantiated in an enforcement unit. An implementation of the policy instantiation and decision units in Prolog confirmed feasibility of a new approach.

Malware and forensic. Lorenzo Martignoni discussed a technique for the detection of self-mutating malware based on control-flow graph matching. Unveiling of malicious code involves normalization built on top of the Boomerang, an open-source decompiler, and identification of malicious code, formulated as a graph isomorphism problem, using the graph matching library VFLib. The proposed approach shows that normalization can bring self-mutating code into an archetypal form in which it can be reliably identified using graph isomorphism detectors.

André Åarnes presented an approach to digital forensic reconstruction based on the virtual security testbed ViSe. It is based on the replay of attack actions in a virtual machine setting, whereby the sequence of system transformations is recorded using the VMware snapshot function. Forensic evidence is collected by tracking the state of modified files and can be used to verify or refute legal hypotheses brought to court.

Deployment scenarios. Sascha Lettgen opened the last session of the conference with a presentation of an SNMP-based infrastructure for intrusion detection and response in tactical MANETs. Current IDS infrastructure protocols do not meet the requirements of tactical MANETs. The proposed approach implements the functionality of the IDMEF protocol using SNMPv3.

Finally Arno Wagner presented a method for worm-scan detection for VPN congestion avoidance. The method is based on counting failed connection attempts on a per-host basis. Simple rules can be devised for detection of TCP, UDP and ICMP scans typically used for worm propagation. The proposed rules allow reliable worm detection within several minutes with no false positives.

DIMVA 2007 on July 12-13 in Lucerne, Switzerland. Submission deadline is February 9, 2007.

http://www.dimva2007.org

Satellite events. Co-located with DIMVA 2006 were two satellite events, the SPRING student workshop and the CIPHER capture-the-flag hacking contest.

SPRING. The first SIDAR student workshop SPRING was held on the same premises a day before the conference. The workshop provided undergraduate and graduate students with an opportunity to present and discuss their security-related work in an informal setting. Extended abstracts of the talks were published as a technical report. Being attended by over 40 participants, the workshop was a great success and will now be held on a regular basis.

CIPHER. CIPHER is a capture-the-flag contest on security penetration and system hardening for teams of students. It is organized by the Security and Privacy Research Group of RWTH Aachen. The teams' task is to secure a server running multiple vulnerable services, while simultaneously trying to get unauthorized access to the other teams' systems. Each successful penetration gains points, as well as keeping the own services functional during the course of the game does. This year's CIPHER contest was co-organized by SIDAR, and the contest took place on the second day of the DIMVA conference. While participating teams were located across the world, a local team from the Technical University of Berlin played on the DIMVA premises, providing the conference attendees with an inside view of the contest. The contest's scoreboard presented live to the DIMVA audience followed by a wrap-up presentation by the contest's organisers.

DIMVA 2007. Building on the success of previous conferences, DIMVA 2007 will take place in Lucerne, Switzerland, on July 12-13. The submission deadline for papers is February 9, 2007. For the first time DIMVA 2007 will also accept the submission of *short papers*.

Such papers should present original, still ongoing work that has not yet reached the maturity required for a full paper. Short papers will be published in the conference proceedings and will be clearly marked as Extended Abstract to allow subsequent publication as a full paper. By submitting short papers to DIMVA 2007 the authors will benefit from presenting their preliminary results and obtaining early input from the audience.

Now in its fourth incarnation, DIMVA has become an established venue for publishing high-quality research on intrusions, malware, and vulnerability assessment. Started as a regional workshop, it has become a well-known conference for a large international audience. To match this development, the 2007 program committee has a wider international scope than ever. It includes security experts from renowned institutions from eleven different countries. DIMVA is committed to having a strong technical program, and the expertise of the program committee will enable us to select the very best among the submissions for presentation at the conference.

We very much encourage security researchers as well as practitioners to submit a paper to DIMVA 2007, and to attend the conference in the lovely Lucerne area. Besides the technical program, the conference will again feature a wide variety of related events, including invited talks, a work-in-progress session, business presentations, and a fun social event well-suited to informal sharing of knowledge and experience. Further information on DIMVA can be found at http://www.dimva2007.org. We are looking forward to having a great conference in Lucerne, Switzerland.

Selected links and events

Actual upcoming CIIP conferences in Europe

- ITCIP 2007 (Information Technology for Critical Infrastructure Protection), 4+5 September 2007, Petersberg (near Bonn, Germany), information at: www.itcip.eu
- Fourth International Conference on Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA) in Lucerne, Switzerland on July 12-13, 2007

European projects with articles in this issue

IRRIIS:	www.irriis.org/
ESFORS:	www.esfors.org
NESSI:	www.nessi-europe.com

Links related to articles in this issue

Dependability evaluation methods for IP networks	http://iplu.vtt.fi
Finnish Communications Regulatory Authority:	www.ficora.fi
3rd EAPC/PfP Workshop on CIP and CEP 2005:	pforum.isn.ethz.ch/events/index.cfm?action=detail&eventID=252
4th EAPC/PfP Workshop on CIP and CEP 2006:	pforum.isn.ethz.ch/events/index.cfm?action=detail&eventid=265
Cert project in Israel:	www.tehila.gov.il/Tehila1/english_site
Crisis and Risk Network	www.crn.ethz.ch
Information Security Survey in Swiss Companies:	www.crn.ethz.ch/publications/crn_team/detail.cfm?id=25402
Swiss ISAC “MELANI” Status Reports:	www.melani.admin.ch/berichte/lageberichte/index.html?lang=de
Slides of CRITIS 20006 Conference:	http://critis06.lcc.uma.es
Institute for Information Infrastructure Protection	www.thei3p.org/
International Federation for Information Processing:	www.ifip.org
IFIP WG Critical Infrastructure Protection	www.cis.utulsa.edu/ifip1110/
DIMVA Conference 2007	www.dimva2007.org
FG Intrusion Detection and Response SIDAR	www.gi-ev.de/fachbereiche/sicherheit/fg/sidar/

Various resources for IT risk, security and disaster management

The following reports issued by the Italian Communication Ministry are available by now and are part of a number of activities carried out by the Communication Ministry (http://www.iscom.gov.it/):

- Report on NETWORK SECURITY IN CRITICAL INFRASTRUCTURES: Report in English: http://www.iscom.gov.it/documenti/files/news/pub_003_eng.pdf
- Report on the QUALITY OF SERVICE IN ICT NETWORKS: http://www.iscom.gov.it/documenti/files/news/pub_001_eng.pdf
- NETWORK SECURITY - From risk analysis to protection strategies: http://www.iscom.gov.it/documenti/files/news/pub_002_eng.pdf
- A security paper by the ITU: http://www.itu.int/osg/spu/visions/papers/securitypaper.pdf