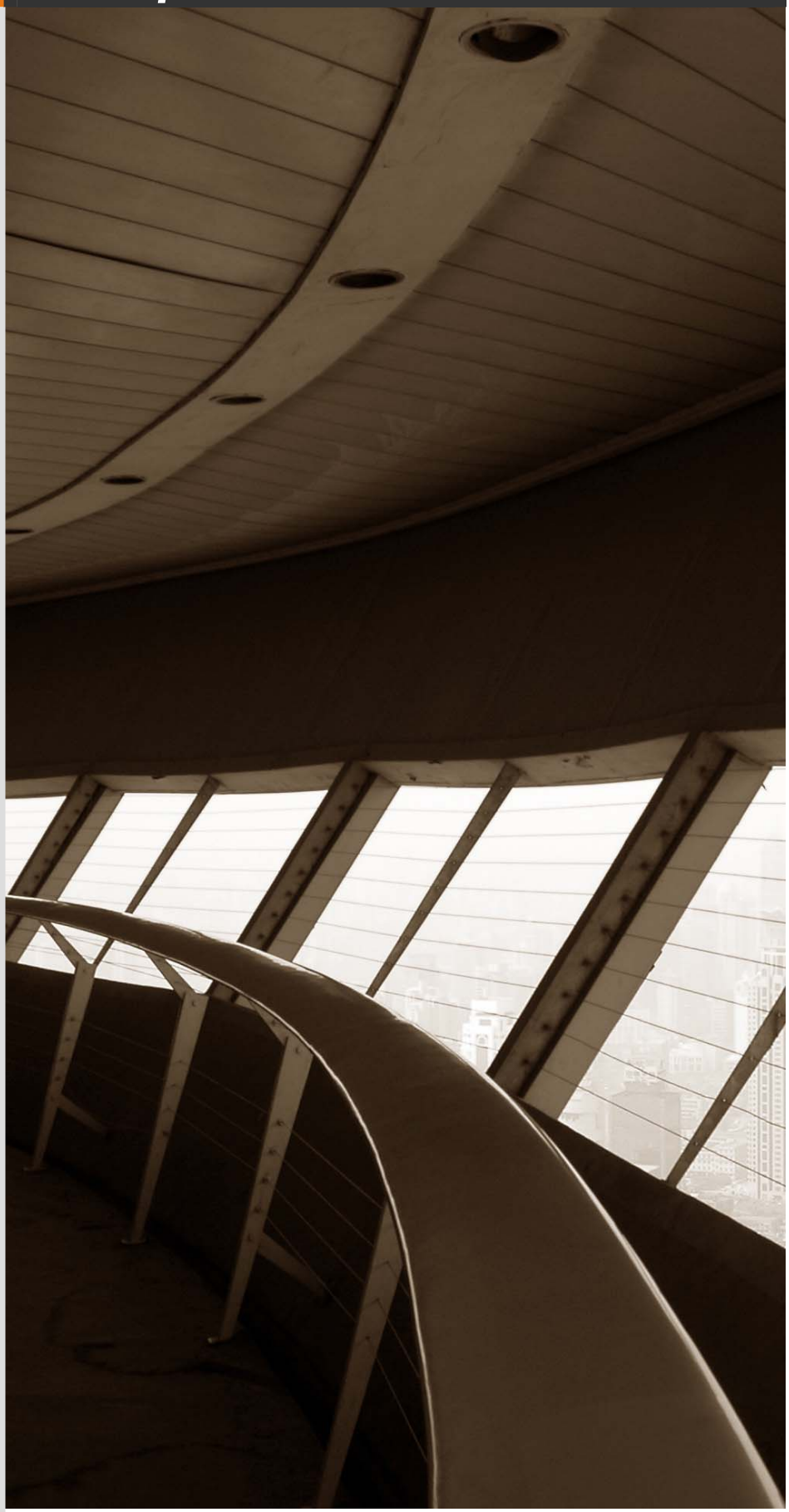
May /June 2006, Volume 2, Number 2

ECN

European CIIP Newsletter

CI²RCO



> 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 CI²RCO project
The CI²RCO 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 side for specific issues:
http://www.ci2rco.org

Table of Contents

Introduction

European Activities

Country Specific Issues

Methods and Models

News and Miscellaneous

Selected Links and Events

Building an European Network of Country Specific ECN Editors

The activity started in the last ECN to gain an associated country editor in each EU member state is continuing successfully. We are very pleased to introduce two new members: Javier Lopez from Spain and Hannu Kari from Finland.

Dr. Bernhard M. Hämmerli

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

The European CIIP Newsletter will be founded for three more years within the project IRRIIS. We are happy to continue the effort for providing relevant information from EU member states with the concept of country specific Editors. Therefore we introduce two new country specific Editors:

New Country Specific Editors

Javier Lopez, Spain, received his M.S. and Ph.D. degrees in Computer Science in 1992 and 2000, respectively, from the University of Malaga. After four years as System Analyst in the industrial sector, he joined in 1994 the Computer Science Department at the University of Malaga, where he actually is engaged as an Associate Professor. Prof. Lopez is Co-Editor in Chief of the *International Journal of Information Security*, member of the Editorial Boards of *Information Management and Computer Security Journal* and *International Journal of Internet Technology and Secured Transactions*, Spanish representative of the *IFIP TC-11* (*Security and Protection in Information Systems*), and member of the board of ERCIM's Working Group on Security and Trust Management. Recently he has become Chair of the IFIP TC-11 WG on *Trust Management* and Member of the Editorial Board of IOS Press series on Cryptology and Information Security.

Hannu Kari, Finland, currently works at the Helsinki University of Technology (HUT), in the Laboratory for Theoretical Computer Science (TCS) of Computer Science and Engineering (CSE) department as a professor on mobility and wireless communication. From 1998 to 2002 he worked at HUT as a director of TOTI-research institute and from 1.9.1999 onwards also as a professor. His primary interest is focused on securing communication in wireless networks, especially in ad hoc based wireless networks in military-grade hostile environments. The research work is done in close co-operation with Finnish Military research organizations. The results gained can also be applied on commercial networks.

Professor Kari has also a long track-record as an industry-manager, e.g. he worked more than 10 years for Nokia.

Another research topic of him is to build a novel mechanism, called Packet Level Authentication, PLA, to add strong authentication information into every packet sent in the IP based networks.

About the Link Collection

We updated our link collection. Due to the high quality of existing security portals we decided to list only very relevant links,. You still find links to the most important security portals.

The link collection can be found on www.ci2rco.org ("downloads", weblink.rtf)

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.

Enjoy reading the ECN!

Vital Infrastructure Threats and Assurance (VITA) project

A novel threat taxonomy, a proof-of-principle of synchronised tools for multi-national and cross-sector CIP exercises, recording of human behaviour in-the-loop, and shaping the Critical Infrastructure Protection research area.

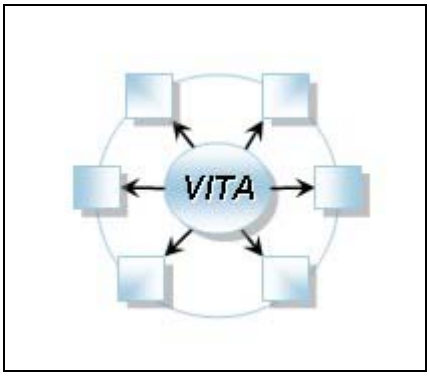
Eric Luiijf MSc.

Eric Luiijf graduated in 1975 at the Technical University of Delft. Eric is Principal Consultant Information Operation and Critical Infrastructure Protection at TNO Defence, Security and Safety, The Hague, The Netherlands. He is connected to the Clingendael Centre for Strategic Studies.
Tel. +31 70 374 0312
E-mail: eric.luiijf@tno.nl

On the 18 May 2006, the European Vital Infrastructure Threats and Assurance (VITA) project conducted an experiment that demonstrated the synchronised use of two different scenario simulation tools and the registration of physiological aspects of decision-taking processes. Using a scenario where heavy snowfall, a terror threat, a train collision and a slow collapsing of the power grid across two nations, the experiment was able to demonstrate the cascading effects on Critical Infrastructures (CIs). The VITA demonstration successfully showed that the concept can be used effectively by private and public parties from multiple nations. They can prepare themselves for dealing with cascading effects in CIs. The project results give an impetus for joint exercises by governments, agencies and diverse control centres of various CIs. The VITA results will be used to shape part of the CI Protection (CIP) European Research Area (ERA) on Security.

European Security Research Programme from 2007 on

Since 2004, research in increasing the security of nations and the safety of the citizens ranks high on the research agenda of the European Union. Commencing in 2007, significant funding will be allocated to the European Security Research Programme (ESRP). The EU Preparatory Action for Security Research or PASR prepares the European Research Area (ERA) on Security research by up to fifteen projects each year between 2004 and 2006 dealing with a large variety of security topics. One such topic is CIP.



The PASR projects are designed to indicate in a short time-frame and with a limited budget the direction of security research that should be explored and exploited in the ESRP.

The Vital Infrastructure Threats and Assurance (VITA) project was contracted by the EU as one of the projects answering the first PASR call. VITA aims to improve the under-standing of threats and risk factors to CIs. As well as raising awareness among European Partners on the need for CIP, one of the main objectives was, through the demonstrator experiment, to show how an innovative combination of existing scenarios and modelling and analysis tools can help to understand dependencies between CIs at the community level. This is vital in funding future research to develop CIP co-operation within the EU at the most appropriate level.

VITA is managed by IABG (Germany). Others partners in the VITA consortium are IBBE, the Institute for Biocybernetics and Biomedical Engineering (Poland), the Swedish Defence Research Organisation FOI (Sweden), QinetiQ (United Kingdom), Red Eléctrica de España (Spain), PM Projektmanagement (Germany), and the Netherlands Organisation

for Applied Scientific Research TNO (Netherlands).

VITA work packages

TNO was responsible for the VITA first work package which aimed to list possible threats to CIs. We identified that most threat lists contain malicious human actions instead of threats, e.g. sabotage, terrorism, or catch-all categories like 'Acts-of-God'. VITA developed a novel extendible threat taxonomy which contains some 300 threats to CIs. Potential exploitation of such threats by humans for activism or terror is identified at another axis of the taxonomy.

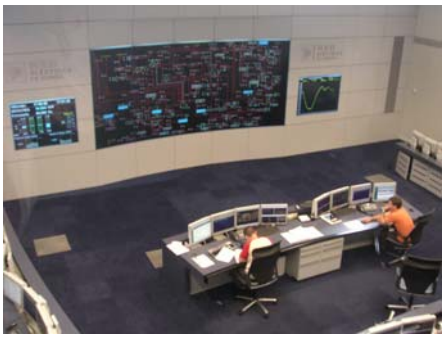
Synchronised scenarios for cross-border critical infrastructure protection challenges. VITA showed the validity this approach while measuring the human decision-taking processes in-the-loop.

QinetiQ investigated tools and methodologies that could potentially be used by VITA for building and supporting scenarios. A database was developed to information about all identified tools that incorporated a unique method for scoring tools and methodologies against CI assessment criteria identified during the project. In parallel, FOI used the threat taxonomy in the development of two scenarios affecting multiple CIs. One of the base scenarios was selected for the later demonstration exercise. The VITA project partners contributed scenario ingredients based on their knowledge of the behaviour of various CIs, (inter)national crisis management as well as public and private parties (telecommunication and power).

The next challenge to the VITA project was to show that the combined and synchronised use of multiple scenario and training tools can support analysis of dependencies between CIs at different levels to support the development of 'good practices' for incident management and for the protection of CIs across the community.

Demonstration preparation

IABG provided the DEMOCRIT scenario tool that comprises a network of PCs and scenario driver program. Players are connected and communicate via the PCs to enact individual roles (e.g. Crisis Management, Civil Protection, the Media, Tele-communication provider or Transmission System Operator. Using a prepared scenario, pre-scripted email messages prompt players to react at the most appropriate time in the scenario. Key management players decide about courses of action whilst providers and end users interact with key information and responses. Their response is based on the defined roles and player expertise. All messages are logged for later analysis. Underlying mathematical models generate delay, disruption, and chain effect factors (weather, road condition, congested or disrupted GSM and fixed telecommunication, disrupted power). The course of the scenario play is monitored by a control function which may inject additional challenges where appropriate.



REE operators / dispatchers

Red Eléctrica de España (REE) provided the OTS, the Operator Training Simulator. This is an existing tool designed to provide hands-on training for system dispatchers/ operators. During the exercise, OTS has presented the events in real time and has been used in a novel way due to the interaction with external agents during the operation (such as Civil Protection). Even, due to cascading effects provoked for unexpected situations, the operators have met new scenarios that have been solved.

IBBE was responsible for a complimentary work package (known as Jazz-Novo) that examined the physiological aspects of human decision -taking by in the protection of CIs). As part of the OTS element of the experiment, the IBBE work package used REE control centre operators. A small measurement device is attached to the operator's forehead to collect physiological data. The collected data includes head and ocular movements, heart beat and systolic rate. An integrated webcam and microphone are used to record the visual and audible environment. During phases one and two one of the OTS operators was wired and monitored with de Jazz-Novo headset and recordings of his "attention state" in the decision-making process will allow analysis of physiological aspects of the operator actions during the crisis.

The Jazz-novo recording the human behaviour during decision-taking processes by one of the OTS-operators.

Proof-of-principle

The VITA proof-of-principle demonstration took place near Madrid, Spain in the training centre of Red Eléctrica. Three scenario sessions were played, each taking one and a half to two hours. The first session set the scene under the title "crisis arising": some days before Christmas, busy roads and an expected snow storm for both scenario nations VITALAND and ATIVIA. Ten real operators behind the

OTS, fifteen DEMOCRIT-players including experts from the German Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (Civil protection and emergency management), and four observers were engrossed in the experiment. Despite heavy snow, high winds, traffic congestion and power outages, players made executive decisions, tasked resources, and fended off the inquisitive media in a scenario temperature of -5 °C whilst, in reality, outside the rest of Madrid baked in a balmy 32 °C.

The second session "escalating phase" increased the pressure on the players due to the increasing power and communication outages and cascading effects on other infrastructure. A full shift of operators used OTS synchronously with DEMOCRIT to keep up the power grid of both VITALAND and ATIVIA. Despite their efforts, more lines were damaged and lost due to heavy snow, high winds and high demand. Unusually, a phenomenon known as "islanding" occurred, where a part of the network becomes isolated from the rest of the power grid.
Problems were exacerbated by disruptions to supporting tele-communication systems Black-outs could not be avoided, which hampered both national crisis management organisations in handling multiple disaster situations and were amplified by serious traffic congestion and industrial accidents.

In the third session (the 'restoration phase') crisis management centres tried to obtain international coordination support and resources and demonstrated the difficulty in providing international assistance whilst dealing with a major internal crisis.

Initial Impressions

Whilst the exercise will be subject to considerable in depth analysis our initial impressions are that the experiment was a resounding success in raising awareness for co-operation in CIP. In addition a set of tools has been identified that can be used to conduct experiments in CIP at the community level.

Whilst the number of people involved in dealing with an international crisis on this level would be considerably more than the thirty souls available for the VITA demonstration.

However, five different functional levels were enacted in the experiment ranging from international co-ordination to deployment of local resources. What the experiment did highlight was the need for formal international agreement about cross border co-operation with particular attention to roles and responsibilities and the need for a common taxonomy for CIP. At the national level, as has been recognised by many European Partners the need for tried and tested initial response, recovery and reconstitution procedures where all participants are clear on their roles and responsibilities are essential.

VITA, the next steps

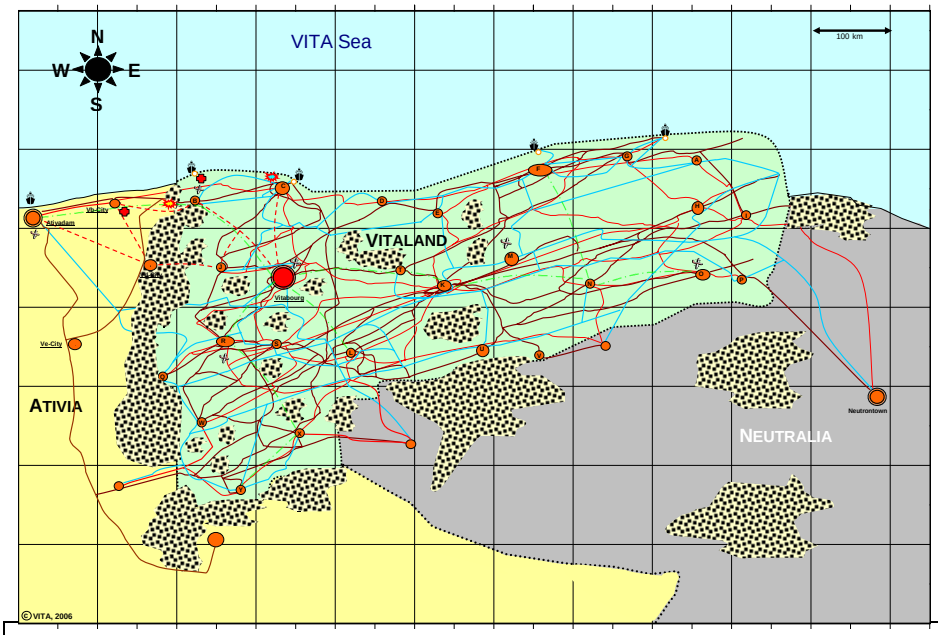
The next two months will be spent by the VITA team to complete the analysis of the results. Input will be given to the ESRP. On July 4, 2006, a final conference will take place in Brussels.

The full crew which partipated in the VITA demonstration exercise.

More information on VITA

Rudi Schaefer, IABG mbH
phone: +49 89 6088 3061
mobile.: +49 172 8375 420
email: SchaeferRu@iabg.de

The VITA project is sponsored by the EU under the PASR-2004-004400 grant.



(at left) The geographic scenario layout of Ativia, Vitaland and Neutralia. Some of their critical infrastructures is visible: power lines, road, rail, harbours, and hospitals.

IRRIIS – A new European Project to Increase CII Dependability

IRRIIS enhances the understanding of large complex critical infrastructure (inter)dependencies by creating a synthetic simulation environment and developing novel Middleware Improved Technology.

Dr. Felix Flentge

Dr. Flentge is responsible for all IRRIIS activities inside the Fraunhofer Institute for Autonomous Intelligent Systems and assists the IRRIIS Project Manager Uwe Beyer in co-ordinating the project.

Timo Steffens

Timo Steffens is responsible for the simulation framework at the Fraunhofer Institute for Autonomous Intelligent Systems and for the scientific assessment of the results.

The new EU Integrated Project "Integrated Risk Reduction of Information-based Infrastructure Systems" (IRRIIS) started in February 2006. Within the next three years, IRRIIS will be carried out under the motto: Substantially enhance the dependability of Large Complex Critical Infrastructures (LCCIs) by introducing appropriate Middleware Improved Technology (MIT) components.. IRRIIS aims at increasing the dependability, survivability and resilience of EU Critical Information Infrastructures based on Information and Communication Technology (ICT). IRRIIS has the objectives to:

• determine a sound set of public and private sector requirements based upon scenario and related data analysis;

• design, develop, integrate and test Middleware Improved Technology components suitable for preventing and limiting cascading effects as well as for supporting automated recovery and service continuity in critical situations;

• develop, integrate, and validate novel and advanced modelling and simulation tools integrated into a synthetic environment (SYNTEX) for experiments and exercises;

• validate the functions of the MIT components using the SYNTEX environment and the results of a detailed scenario and data analysis;

• disseminate novel and innovative concepts, results, and products to other ICT-based critical sectors.

IRRIIS will address the challenges of Critical Information Infrastructure Protection (CIIP) by a "diagnosis - therapy strategy" and "therapy implementation and validation approach".. The first CII sectors addressed will be the electrical power and the telecommunication infrastructures. After thoroughly analysing these infrastructures and their dependencies and interdependencies, the synthetic simulation environment (SYNTEX) will be build. MIT components will be developed, tested and validated inside SYNTEX to demonstrate their capabilities before dissemination to potential stakeholders. The IRRIIS approach is open for successively including additional critical infrastructures.

The interdisciplinary research will be performed in the coming three years by a European consortium of fifteen partners. Among these partners are key stakeholders, like Telcom Italia and Red Electrica de España, technology providers, e.g., Alcatel, Siemens and AIS (Malta), and consultants and service providers, like IABG from Germany and AIA from Spain. Additionally, various research organisations and universities from the Netherlands (TNO), Finland (VTT), the UK (City University), Italia (ENEA), France (ENST) and Germany (Fraunhofer SIT, Fraunhofer AIS, TU Dresden) take part in the project.

The project is supported by the European Union Sixth Framework Programme within the area of

"Information Society Technologies" with seven million Euro funding. The integrated project is co-ordinated by the Fraunhofer Institute for Autonomous Intelligent Systems (Fraunhofer AIS).

LCCI Analysis and Requirements

Up till now there is a lack of advanced understanding of the dependability, dependency and interdependency of Large Complex Critical Infrastructures (LCCIs), in particular with regard to the use of Information and Communication Technology (ICT). Although some models and tools dealing with these issues exist, LCCI complexity and criticality can not yet be tackled properly. Basic research is necessary to understand the phenomena of (inter)dependency, dynamic behaviour and cascading effects in order to support the development of solutions for protecting and managing existing LCCIs in case of incidents. IRRIIS will perform in-depth research regarding the topological structure of LCCIs and the dependencies and interdependencies between different LCCIs. Appropriate analytical approaches will be applied such as simulation models or analytical models suitable to investigate (inter)dependency, network dynamics and cascading effects.

Basic research is necessary to understand interdependencies, dynamics and cascading effects

Starting from a thorough analysis of LCCIs, incorporating the stakeholder's views regarding ICT tools and models, a sound set of public and private sector requirements can be determined. These requirements will build the basis for the development of the SYNTEX simulation environment and the Middleware Improved Technology (MIT) components.

In order to enhance the understanding of LCCIs and to gain a sound foundation for the development of the SYNTEX simulation environment and the MIT components, IRRIIS will:

- Survey LCCI stakeholder requirements on technology and tools needed for understanding and mitigating cascading effects;
- Survey and analyse existing CIIP tools and models for LCCIs;
- Analyse current research gaps to identify relevant research and development efforts;
- Provide detailed scenario and risk analysis;
- Perform in-depth topological analysis of LCCIs;
- Analyse the dependencies and interdependencies between different LCCIs;
- Analyse the upcoming Next Generation Networks (NGN), i.e. networks based on IP-connectivity or wireless connections with mainly software-based services.

This work will not only help to ensure the adequacy of the SYNTEX environment and the MIT components to the stakeholders' needs but also contributes to the ongoing world-wide research efforts concerning LCCIs.

Middleware Improved Technology

Starting with the knowledge gained from the LCCI analysis and the survey of stakeholder's requirements and existing tools, MIT components will be developed. These MIT components will facilitate the communication between different LCCIs and will allow identifying and evaluating incidents and malicious attacks and responding accordingly.

Currently, a big problem for the dependability, security and resilience of LCCIs is the high level of inter-dependence of different LCCIs, both within the same sector and between different sectors. The consequence is that problems within one LCCI may lead to severe problems in dependent LCCIs. The resulting cascading effects are not limited to one kind of infrastructure and do not stop at national borders. To make things worse, there is often a lack of appropriate communication structures between the dependent LCCIs. This results in a lack of awareness of problems occurring in other infrastructures and appropriate mitigating actions can not be performed in time.

To facilitate the communication between different infrastructures, IRRIIS will develop appropriate middleware communication components. All communication between different LCCIs should be handled by this middleware layer in a standard way. The advantage is that each LCCI only needs one communication link towards the middleware and does not have to interface several other LCCIs and to implement different protocols.

The middleware will also be used by the optional MIT add-on components which have some kind of build-in "intelligence". These add-on components will monitor data flowing within and between the infrastructures and raise alarm in case of intrusions or emergencies and take measures to avoid negative effects. They will be able to detect anomalies, filter alarms according to their relevance and support recovery actions. In this way, they contribute to the security and dependability of LCCIs. MIT components will interface existing systems and will not require major replacement of existing hardware or software. The flexibility of the middleware shall allow the easy integration of new LCCIs or new kind of information to be exchanged.

SYNTEX Simulation Environment

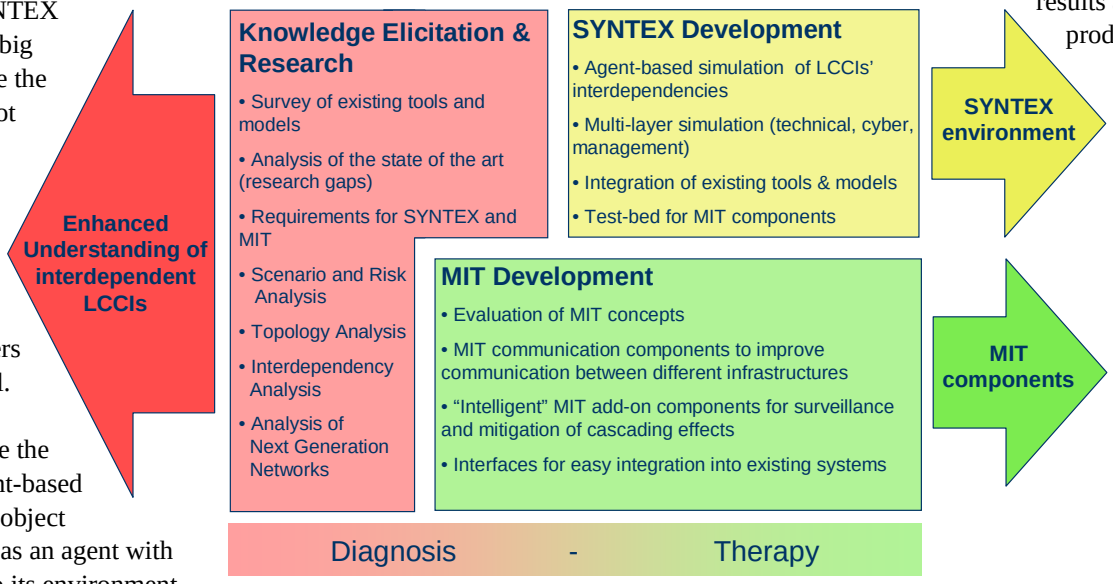
The purpose of the SYNTEX simulation environment is twofold: First, simulation can be used to improve the understanding of dependent and interdependent LCCIs. Secondly, the MIT components will be tested and validated in experiments using SYNTEX. Their applicability and usefulness will be demonstrated within the SYNTEX environment to critical infrastructure stakeholders before deployment to "real world" systems.

A generic simulation environment is necessary to account for specific stakeholders' needs

Building the SYNTEX environment is a big challenge because the simulation will not only have to include physical simulations but also has to simulate the cyber and the management layers of a LCCI as well. For this purpose SYNTEX will use the principles of agent-based simulation. Each object will be modelled as an agent with clear interfaces to its environment and other agents. A language for agent-based modelling of scenarios and processes (LAMPS) will be developed in order to precisely define scenarios and the dependencies between objects. LAMPS will be able to cope with the high degree of parallelism in LCCIs and will offer graphical representations for intuitive display of the dependencies.

The SYNTEX environment will include and interface existing tools to keep the simulation meaningful with respect to existing technologies and to allow the use of the results gained in current systems. This also means that the SYNTEX environment does not have to start from scratch but can rely on already existing and proven technology. To decide which tools and models should be included in SYNTEX, an in-depth survey of existing tools and models will be performed.

However, the main strength of SYNTEX will be the simulation of dependencies and interdependencies between different LCCIs. To that end it will be necessary to have the possibility to model some objects of the individual LCCIs on more abstract levels. This will ensure a high scalability and flexibility of the SYNTEX environment. SYNTEX should be as generic as possible to allow its application to various kinds of LCCIs and its adaptation to the specific needs of individual stakeholders.



Summary

The major parts and the main outcomes of the IRRIIS project are summarised in the figure on this page. Knowledge Elicitation and Research will lead to a "diagnosis" of the current and the future status of (inter)dependent LCCIs. The "therapy" will be implemented through the MIT components which can be tested and validated in the SYNTEX environment. The main contributions of IRRIIS are an enhanced understanding of LCCIs, the SYNTEX simulation environment and MIT components able to facilitate communication between different LCCIs and to mitigate negative effects. To disseminate the results broadly to stakeholders, technology and service providers and the research community, these groups will be addressed within the IRRIIS project right from the start. IRRIIS also relies on international co-operation and is open for joint efforts of all kinds to achieve its goals. To foster co-operation, IRRIIS will establish an international conference and form a special IRRIIS Interest Group of people, institutions and companies interested in IRRIIS results and products.

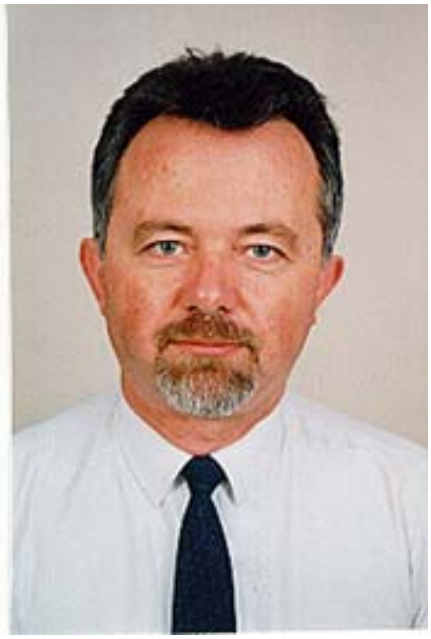
Contact & Information:
Felix Flentge
Fraunhofer Institut AIS
felix.flentge@ais.fraunhofer.de
www.irriis.org

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 European Community is not liable for any use that may be made of the information contained therein.

Achievements and Problems in the Security of Bulgaria's Critical Information Infrastructure

A European taskforce to co-ordinate research and development on critical information infrastructure protection and support of co-operation and CIIP awareness was initiated, and the first CI2RCO work package was completed.



Eugene Nickolov, Prof. DSc. PhD Eng. Mag.

eugene@nlcv.bas.bg

Director of the National Laboratory of Computer Virology in the Bulgarian Academy of Sciences since 1991. His main scientific interests are: algorithms, effectiveness, protections of operating systems; abstract models of computer systems, theory of programs; simulation and modelling of computer and communication technologies; theory of information and cryptographics; data security, computer sSecurity.

1. Definitions and concepts

A country's critical infrastructure consists of facilities, services and information systems whose suspension improper functioning or destruction would have a negative impact on the health and security of the population, the economy or the efficient functioning of the government. This notion of critical infrastructure includes key Bulgarian economic areas such as national security, agriculture, food services industry, civilian aviation, naval transportation, highways, bridges, tunnels, dams, water supply, healthcare, emergency services, government, military production, telecommunication systems and networks, energy supply, the Kozlodui nuclear plant, transportation, banking and financial systems, chemical industry, post services, skyscrapers, national and historical monuments. All of these key sectors of our society, including the national security system and the economy as a whole are heavily dependent on the interrelated national and international regulation and control systems. They compose the country's critical information infrastructure and have to conform to reliability, stability and longevity requirements. The protection of the critical infrastructure and its normal functioning is directly reflected in people's lifestyle and safety which depends on a large number of factors.

2. Geographic and demographic factors

According to National Statistical Institute data on December 31, 2004 Bulgaria's population was 7.761.049. The average population density is 70 people per square kilometre with 52.2% of the population living in the South and Southwest. The urban population is over 5.43 million (70%), and according to the 2001 census over 2 120 000 people (over 27%) live in the four largest cities Sofia, Plovdiv, Varna and Bourgas. The highly developed communication and entertainment systems of the cities create the potential for large gatherings of people and objects with critical importance for society, which is a cause of concern with regard to critical infrastructure security. The European security strategy and the European neighbouring policy outline other dangers related to technology development and globalisation – transnational criminal and terrorist networks, the danger of a symbiosis between them, as well as the danger of weak or failed states to generate instability and crime or to harbour terrorist networks.

3. Economic and political factors.

The challenges in Bulgaria's neighbouring regions are multiple: criminal networks in unstable Kosovo, extremist Islamic foundations in Bosnia, frozen conflicts in the Black Sea region, etc. The separatist republic of Pridnestov in Moldova, for example, is an international post for arms traffic

according to some sources. Bulgaria as a part of NATO and soon of the EU can serve as a pillar for the policies of both organisations towards the new neighbours in the region. Last but not least, Bulgaria has its role in the so-called larger Middle East – from Central Asia and Afghanistan to the southern Mediterranean – by protecting its national interests and those of its citizens. Serious problems related to critical infrastructure security are the intense passenger and cargo flows that cross the country in all directions. In 2004 the country has been visited by almost seven million foreigners and 3.900.000 Bulgarians have been abroad. Bulgaria is crossed by the European transportation corridors 4, 7, 9 and 10. The cargo transported by trucks (both domestic and international) amounts to 165.3 million tons and the railway traffic to 20.4 million tons. With such volumes of passenger and cargo flows, strict border control is a necessary but not sufficient measure to protect the critical infrastructure.

4. Crisis planning and management

A survey on crisis planning and management information coverage was carried out in the beginning of 2005 in accordance with the National Program for Statistical Research. It encompasses all crises that occurred in 2003 on the territory of each district, their parameters, the condition and characteristics of potentially dangerous buildings and critical infrastructure objects, and the losses incurred. The data was entered in an integrated statistical geo-referential information system for crisis management which is connected to the national and regional centres for crisis management. According to the data received from 259 districts and 24 regional administration centres in Sofia, in 2003 there were 11.905 crises in Bulgaria and about a third of them impacted the country's critical infrastructure. Districts affected by natural disasters are 192 (74.1%) and by fires 139 (53.7%). The largest fraction is industrial incidents and car accidents (52.9%): from them 0.5% are industrial incidents, 3% - theft of cables, 94.7% - car accidents. Fires (excluding forest fires) are 33.6% from all crises: 7.3% - arsons, 31.6% - accidents, 22.8% - from technical malfunctioning. Arsons have affected 12.7% of the districts, accidents - 29.7%, technical malfunctioning - 18.5%, natural disasters - 3.9%, unknown causes - 32%. Natural disasters accounted for 8.1% from all crises in 2003: 24.8% are landslides, 29.6% - floods, 10.3% - whiteouts, 11.5% - storms, tornados, wind sprouts, whirlwinds, 1.5% - earthquakes, 1.3% - droughts, 1.8% - hail, 1.7% - ice and frost, 17.6% - other. Over 80% of these natural disasters have interrupted the functioning of the country's critical infrastructure. Although the 2004 crisis events statistics has not been made official yet, partial results show an increase in the number of natural disasters and other significant crises that affect the functioning of critical infrastructure objects. The 2005 floods hit Bulgaria really hard. 82% of the country has flooded with a population of 3.200.000 from which 2.000.000 were directly affected. 185 regions in 27 districts were impacted. Emergency state was declared in 19 districts and 47 regions. During the rainfall 14.000 were evacuated. The technical infrastructure – roads, railways, electricity and water supply as well as the cable network suffered losses of over 622.349.694 leva. 2.470 km of roads has been affected, 219 bridges have been completely destroyed and 273 have suffered severe damages. 1.126.974 acres of arable land have been flooded and the harvest losses total 74 million leva. Critical infrastructure damages including damages to critical information infrastructures amount to tens of millions of leva.

5. Ministry of national policy in emergencies

The current crisis situation undoubtedly points to the need of purposeful national policy in this area. The Bulgarian government has realised the need of effective management that guarantees the rights and interests of Bulgarian citizens in case of accidents and emergencies. In connection with these engagements, Bulgaria has taken in the process of adhesion to the European Union, the decision to create a governance platform. Therefore, the new government that came into power in 2005, includes a new Ministry of national policy in emergencies that encompasses the current agencies charged with the prevention, reaction, management and rehabilitation in crises – State Agency of Civil Protection, National Bureau of Fire and Accident Safety and State Agency of State Reserve and War-time Supplies. The job of the new ministry is to guarantee the adherence to the principle of undivided authority in the case of critical infrastructure emergencies. Its main goals are to prevent uncoordinated and slow institutional action, to create an effective and efficient, technically well-prepared and materially integrated system for the prevention, preparation, reaction and rehabilitation in case of emergencies. This system shall protect the critical infrastructure and address the real needs of Bulgarian citizens in those situations. The policy of the ministry is aimed at the creation of a unified action model in crises, the achievement of efficient communication for crisis management, and increase in the transparency of the administration's actions in crisis management. In 2006, the ministry is expected to propose changes to the Crisis Management Law and a project for a Population and National Resources Protection in Cases of Emergencies Law, as well as build systems for early warning and space monitoring.

6. National Training Centre

The Population Protection Convention in Civil Crises developed by the new ministry and approved by the Council of Ministers, includes the creation of a National Training Centre for rescuers and citizens. It also previews the creation of a central organ for civil crisis management under the Minister of National Policy in Case of Disasters and Accidents.

7. National Emergency Calls System

The government has started building a national emergency calls system with a common European number according to EU Directive 2002/22. This number will be introduced without interrupting the use of other police, fire department and first aid emergency lines. The introduction of telephone number 112 will improve citizens' access to emergency services and the co-ordination between different agencies in case of emergencies and civil crises. The common number will accept phone calls not only in Bulgarian, but also in the EU's official languages English and French, so that foreigners in the country can also receive assistance.

8. Crisis management law

The ministry of state policy in emergencies and accidents will also be governed by the March 2005 crisis management law that creates the national system for crisis reaction. This system will include governance centres, communication systems and crisis reaction forces. Its main objectives are observation opportunities, analysis and evaluation of risk factors, actions and objects; on-time crisis reaction possibilities; development of a reliable communication structure.

9. Critical information infrastructure protection

The fast-paced development of information technology and internet's globalization have created new dangers for the elements of the national critical information infrastructure – multitudes of criminal and terrorist organizations now have the opportunity to use the global network for their criminal goals. This is why critical information infrastructure security becomes one of the main aspects of the security and economic stability of the country. The main tasks in the area of critical infrastructure protection with regard to the whole government strategy consist of black-out prevention due to natural disasters or purposeful attacks, decrease in the nation's vulnerability to such attacks and minimisation of the losses and rehabilitation time. In practice, the national critical infrastructure protection strategy follows the principles of the classical civil protection scheme: training, warning, notifying and eliminating of the consequences. In the case of critical information infrastructure, however it is critically important to create reliable structures for nation-wide communication. Therefore, all interested agencies should co-operate in keeping communication structures on high alert in case of an emergency. This includes elements storms or natural upheavals (magnetic storms, floods, hurricanes, earthquakes), as well as technological and ecological catastrophes (power plant and chemical plant accidents), anthropogenic catastrophes (air, railway and car accidents), epidemics, as well as civil unrest, sabotages, diversions and terrorist acts. One should not forget that every developed country today uses Internet's resources along with the special (government, diplomatic, reconnaissance, military, etc) and general (phone, mobile, cable, satellite, wireless, etc.) networks. Even such a strong communication system can be put out of order in a second through a natural disaster, malfunctioning, terrorist act, or hacker attack. The sad proof comes from the 9/11 attacks on New York and Washington, DC when the phone connection for general use (cable and wireless) was paralysed due to the hundreds of thousands simultaneous calls that blocked the overloaded phone stations. According to American expert evaluations the phone calls in New York on 9/11 were 14 times more than the limit and the largest national service provider AT&T had 100 million calls more than usual that day.

10. National Communication System

One necessary measure for the creation of a reliable communication structure is the creation of a national communication system. Through a telecommunication modernisation and development program, the system will supply the technical back-up of the guaranteed connection between the most important government structures in case of an emergency, when the respective communication centres could be out of order, blocked, or overloaded. The technical abilities of such a system can be provided on the basis of a flexible and operative distribution of resources and traffic configuration while taking into account the priorities of cable and mobile networks for general use based on digital technologies and the Internet. Such a national communication system would allow each subscriber within the territory of Bulgaria to gain access to the resources of that network according to the established procedure for emergency official message delivery related to national security and for extreme population notification. High alertness of this system in case of emergencies can be achieved through automatic survey and projection of the condition of the conductive layers of the ionosphere, tri-monthly training, weekly

connection checks, unification of the connection standards and equipment, incorporation of package connection technologies and the IP suite of protocols. The basic requirements for wireless communication systems are priority service, and compatible and safe access in case of emergencies based on the existing and future standards of wireless phone connection. The intended users of those systems are the president, the prime minister, the chair of the National Assembly and his aids, the ministers of the defence and the interior and their staff, the special service director and his aids, the director of the national coordination council, district governors, city mayors, emergency reaction headquarters, the directors of rescue, transportation and medical services, diplomats and law-protection officers. In modernising communication technologies, one should take into account that their key role in the contemporary society determines the high degree of dependence of the national infrastructure security on the information security of all of its elements both in the public and private sectors. That means that the information security of a separate company can become a factor in the national and internal security of the country as a whole. If, for example, a company X works in the financial services industry, the efficiency of its operations on the stock market will depend not only on the reliability and protection of the used equipment and software, on the qualifications and moral qualities of the employees, but also on the robustness of the cryptographic means used to protect data-transmission channels it borrows from other companies. Furthermore, company X can cause not only financial loss for its clients in case of transactions through unsecured communication channels, but it could cause a crisis in the entire industry, or even the whole economy, to cease shipments of arms and military technology, for example, and infringe on national security.

11. Public or private infrastructure.

One should not forget that the resources of the national information infrastructure, both public and private, are physically and logically interrelated. Therefore, there is a sharp need to unite the different security mechanisms that guarantee access to corporate resources, to constantly monitor their condition, and to act on suspicious or unacceptable activity. Although the market provides a fairly wide variety of such means, the security problem requires even more options. According to foreign and local experts, private companies providing Internet services are not currently taking sufficient measures to guarantee the security of the critical information infrastructure. A large percentage of the critical information infrastructure (80% of all on-line communications with the rest of the world) is not under state control. Therefore, the efforts of all organisations (state, public and private) should concentrate on the clear determination of corporate policy and security management, on the main goals, the current limitations and the status of corporate security.

12. Interaction between national organisations and corporations

It should include: problem analysis and awareness regarding the threats to the critical information infrastructure; focusing the attention of special services and that of hardware and software producers on the security and protection of their products; simultaneous and quick reaction in case of accidents related to a malfunctioning in information systems; creation of channels for official and unofficial exchange of information regarding the danger of computer crimes and cyber terrorism. The co-operation and partnership between different organisations, the attraction of expert groups and private contractors for certain tasks related to the use of information technologies, not only broaden the borders of information resources but also change the notion of internal threats to information security. One insulted or unhappy employee in a company who has legal access to its network and information resources and sufficient knowledge of its corporate network structure can cause much more harm than a hacker attacking the same network through the Internet. Different estimates claim that 50-80% of all attacks aimed at sensitive information come from the Internet. The problem with internal security threats is especially present with the development and widespread of mobile storage USB devices (flash-disks, USB-memories, etc.).

13. New security rules for critical relations.

All basic elements in cyberspace (people, organisations, software, hardware) constantly have the need to develop dynamic relations without authorisation or guarantees from a pre-approved mediator which goes against the principles of critical information infrastructure security. New organisational and technical solutions are needed for this acute problem that concerns the autonomy of separate elements, the size, the complicity and dynamics of the critical information infrastructure in Bulgaria as a whole. The experts need to carry out further studies to find new models for the creation of critical information infrastructure security guarantees. Its autonomous elements are geographically distributed and belong to different agencies, so that the requirements for dynamic security management in direct connections between users, equipment, programs and data can be satisfied.

14. New regulations against information leaks

Further expert investigation of the additional capabilities and the critical features of the information infrastructure components (equipment, software, connection devices, storage devices, information) needs to be performed especially with respect to information leaks and unauthorised use. The security degree of an information system as a whole can not be determined based only on the security of its components. The critical functions of especially large systems can not be predicted at all. Therefore, additional studies of the vulnerability of critical information infrastructure systems in all life cycle stages (design, construction, assembly, modernisation, exploitation, part substitution) with regard to when and how new security threats could be imported, are much needed. Thus, new methods for adaptability determination, software and hardware analysis in the case of especially large systems need to be developed.

15. New regulations for wireless system security

Special attention needs to be paid to the wireless system security which is gaining increasing importance. The networks using such technology include not only telecommunication devices, but a variety of end-user devices, such as controllers and others than can also provide wireless connection. Although the problems related are similar to those in wired networks, the technical solutions borrowed from them are not always applicable in wireless situations. It is necessary to explore the security of the current wireless access and connection protocols, to unite the connection mechanisms on all protocol levels and to create analysis methods for the security of wireless networks. A strategy against attacks and security breaches can prevent denial of service or interruption of the connection.

16. Conclusion.

The further additions and changes to the legislation, the structure of the national budget, the development of the national communication system, the physical protection of the most important objects from the critical information infrastructure, the creation and incorporation of new secure and efficient information technologies, the training of the population, and the creation of survival skills in the case of technical or natural disasters and terrorists acts – all these and other pending measures for national security that will be undertaken in Bulgaria, need to be co-ordinated with similar measures taken in other countries – the members of NATO and the EU, because the risk and the vulnerability of the critical information infrastructure are becoming more and more international. For a prompt and effective reaction to the related incidents, the respective scientific sections and the special and technical forces of many countries need to co-operate, both officially and unofficially, to create a common strategy and tactics against the greatest danger so far in the history of our civilization. This is the inevitable logic of globalisation.n.

Critical Energy Infrastructure Assurance. A case for international Collaboration

The Euro-Atlantic Symposium on Critical Information Infrastructure Assurance

Dr. Saifur Rahman

Dr. Saifur Rahman is the Joseph R. Loring professor of electrical and computer engineering and the director of the Advanced Research Institute at Virginia Tech. He is also the Division Director of Northern Virginia Engineering Program of the university. He is a Fellow of the IEEE, and a director of the IEEE board. He is serving as the Vice President of the IEEE Publications Board in 2006. Dr. Rahman is a member of the Editorial Board of the Proceedings of the IEEE. He has served on the IEEE Power Engineering Society (PES) Governing Board for five years as the Vice President for Technical Information Services and the VP for Education/Industry Relations. He is also a member-at-large of the IEEE-USA Energy Policy Committee. His research interests include alternate energy systems, infrastructure studies, electric load forecasting and power system planning. He has authored over 300 technical papers in these areas.

srahman@vt.edu

The Euro-Atlantic Symposium on Critical Information Infrastructure Assurance was organized by Professors Saifur Rahman and Mohamed Eltoweissy of the Advanced Research Institute of Virginia Tech, USA, in collaboration with Professor Bernhard Hämmerli, HTA, Luzern, Switzerland. The symposium was held at the Riva San Vitale site of Virginia Tech in Switzerland on 23-24 March 2006.

The goal of this symposium was to set the stage for an Euro-Atlantic partnership to better identify, prioritize and address key workforce development and research issues in the core area of critical information infrastructure assurance (CIIA). The symposium provides a forum for the exchange of ideas, interests, expertise and work plans focusing on CIIA workforce development and research issues.

A total of 25 experts and thought leaders from Europe and United States participated in this two-day event representing the following institutions:

US institutions:

Applied Physics Laboratory, Johns Hopkins University
Georgia Tech Information Security Center
NASA Goddard Space Flight Center
Naval Research Laboratory
US Department of Commerce
Virginia Tech

EU institutions:

Ecole Nationale Supérieure des Télécommunications, FRANCE
Fraunhofer Institute for Autonomous Intelligent Systems, GERMANY
Fraunhofer Institute for Secure Information Technology, GERMANY
SAP AG, GERMANY
Waterford Institute of Technology, IRELAND
Joint Research Center, ITALY
TNO Defence, Security and Safety, NETHERLANDS
Computer Associates AG, SWITZERLAND
HTA Applied University, SWITZERLAND
IBM Zurich Research Laboratory, SWITZERLAND

A total of 19 papers were presented focusing on four areas that are considered crucial for a better understanding of the CIIA web of technological, organizational, societal and human factor issues in building a global trustworthy information infrastructure. These four areas are:

- business, management and organizational issues of CIIA,
- law, policy and privacy issues of CIIA,
- assurance aspects in CII design and evolution,
- assurance aspects in CII operation and maintenance.

A website (www.cimap.vt.edu/CIIA) has been created in order to host the information presented at the symposium, as well as to provide an interactive discussion forum to facilitate joint research opportunities, and collaboration between US and EU experts for the Virginia Tech Executive Masters of Information Assurance (EMIA) program.

CIIP – Reached its Peak?

USA and German Experiences regarding the Decreasing Political Importance of a Key Element of National Security

Tillmann Schulze

Dr. Tillmann Schulze is consultant at Ernst Basler + Partner Ltd in Zollikon, Switzerland. He studied political science at the University of Münster and Dartmouth College. He received his PhD degree in 2005. From 2002 to 2005 he worked with the German Federal Agency for Information Security (BSI) in the CIIP unit.

Tillmann.Schulze@ebp.ch

10 years ago, the US administration launched the discussion about the implications of information technology (IT) to critical infrastructures. Executive Order 13010 can be regarded as the first official steps to highlight the importance of dealing both with physical threats and dangers stemming from the dark side of the triumphal development of IT. In 1997 the President's Commission on critical Infrastructure Protection (PCCIP) published its final report "Critical Foundations: Protecting America's Infrastructures". Without doubt, this document should be considered as the starting-point of a cascade of political initiatives, R&D programmes and other activities dealing with the effects of IT on critical infrastructures.

For some years afterwards, the United States have had a pioneer role in CIIP activities. Only one year after the PCCIP's report, Bill Clinton's administration released the Presidential Decision Directive 63 (PDD-63). The directive, titled "Counterterrorism and the Protection of the Homeland", already contained core-elements of a subsequent CIIP-strategy. The aims of the directive were just as ambitious as naïve. On the one hand it called that „any disruptions or manipulations of these critical functions must be brief, infrequent, manageable, geographically isolated and have minimal impact on the United States." PDD-63 postulated that no later than in 2003, critical infrastructures in the US were to be protected against every intentional act that would significantly diminish the abilities of the Federal Government, state and local governments and the private sector.

The protection of critical infrastructures against IT-related threats was the prime focus of the Clinton Administration. In year 2000 the National Plan 1.0 superseded PDD-63. There was however no lead agency within the Administration which held total responsibility for all required tasks. This of course proved to be a great problem.

The situation dramatically changed after the 9/11 attacks in 2001. Homeland Security became of major concern to the US Administration and as a result the Department of Homeland Security (DHS) was founded. Its aim was to help protect the US against all possible attacks. The importance of critical infrastructure protection became crucial for the wellbeing of the US. As a result all CIP and CIIP-activities were to be co-ordinated by the Under-Secretary for Information Analysis & Infrastructures Protection within the DHS.

Within days of the DHS being founded two major documents dealing with infrastructure protection were published:

- "National Strategy for the Physical Protection of Critical Infrastructures and Key Assets" and
- "National Strategy to Secure Cyberspace".

The latter was of paramount importance to CIIP and stated the USA should be protected against all threats regarding the use of IT, which included CIIP. The National Cyber Security Division (NCSD) was to hold responsibility for this task and as such was founded in June 2003.

Unfortunately, the founding of the NCSD was the last act in the US policy regarding CIIP. The meaning of CIIP within the US Administration continues to be on the decrease. This can be explained by the following:

1. The majority of personnel in charge of CIIP within the DHS left the department within eighteen months: Frank Libutti, Under-Secretary for Information Analysis & Infrastructures Protection, Robert Liscouski, head of the Infrastructure Protection directorate, and Amid Yoran, head of NCSD.
2. The "Protected Critical Infrastructure Information Program" which was to help obtain information regarding the needs and IT-related security problems in critical infrastructures failed. In line with the USA PATRIOT Act, the private sector did not trust the DHS and was reluctant to provide confidential information to a governmental institution.
3. The attempt to promote the meaning of CIIP failed. In autumn 2004 delegates of the Democrats within the House of Representatives started several initiatives to increase the influence of NCSD. They failed. News regarding the division henceforth became scarce.

The situation has not changed. A visit to the DHS' CIIP-website displays the same strategies as those in early 2003. Limited information about the table top exercise "Cyber Storm" performed in early February 2006 exists. In short one cannot help but get the impression that the current CIIP-policy in the US is weak with little or even no results.

CIIP became of great interest to most western industrial countries after the release of the PCCIP's report. Germany was of no exception. A cross-ministry working group (AG KRITIS) was founded immediately with the aim to determine the threats to Germany's critical infrastructures by information technology. The working group's results were disturbing to the German government (it showed the shortfalls in CIIP) and hence it was decided to treat the document as highly confidential.

In despite of this, the document was and still is available on the Internet, which was of great embarrassment to the German Home Office. At the time the Germans elected another administration and all rumours that resulted of publishing the working group's report faded.

From 1998 to 2001 CIP and CIIP were of little or no importance within the German administration. Moreover, the German Home Secretary Otto Schily paid no attention to it. Only a small unit within the Federal Office of Information Security (BSI) worked on CIIP and on CIP. For more than two years as few as three people were dealing with these crucial tasks within the entire German administration!

The situation changed after 9/11. The CI(I)P unit within BSI grew and obtained funds for in-depth studies to answer important questions relating to CIIP. The importance of CIIP was elevated: the German Home Secretary paid attention to CIIP; the people in charge of the Federal Office for Criminal Investigation (BKA); as well as the new founded Federal Office for the Protection of the Population and Disaster Relief (BBK). But there was still one thing missing that the US already had: a national strategy for CIIP. This strategy was announced for the first time in autumn 2003 by the Federal Ministry of the Interior's (BMI) Under-Secretary Ute Voigt – nothing happened. A year later the same strategy was again announced with again the same result.

It is however worth noting that within this period a CIP-task force was founded within the BMI, table top exercises took place and Germany tried to deal with CIIP on an EU- as well as an international level. In late summer 2005, the first German CIIP-strategy was then published: the "Nation Plan to Protect Information-Infrastructures" (NPSI).

This took place five years after the US' PDD-63 and more than two years after the National Strategy to Secure Cyberspace. Compared to the progress in information technology, progress is slow. Germany now however does have a national strategy which is enforced. In spite of NPSI however, the future of the German administration's efforts in CIIP is unclear. Within the BSI there are still only a handful of CIIP-experts and the new Home Secretary Wolfgang Schäuble has not as yet discussed CIIP.

In reviewing the current CIIP-situation in both the USA and Germany, the question remains, why progress in promoting this crucial task was stopped. Critical infrastructures remain dependent on IT and potential threats continue to grow, not diminish. Of course, there are many projects in several countries touching different aspect of CIIP. But it is clearly apparent the relevant administrations are not particularly interested in CIIP. Why could this be so?

1. There is no pressure by supranational organisations. Firstly, there is no international regime dealing with CIIP. International agreements are weak in results. The European Union's Network and Information Security Agency (ENISA) does not currently deal with CIIP. Hence, there is no clear guideline for member-states like Germany.
2. Physical threats to critical infrastructures are considered far more in detail than IT-related threats. Since there is no evidence of cyber-terror, people in charge are more concerned about real bombs than about logic ones.
3. There has been neither an "Electronic Pearl Harbor", or a "Digital Armageddon" nor were scientists, politicians and journalists surprised by the year 2000 bug. Articles about IT-system disruptions of critical infrastructures are published on a regular basis. But these disruptions are not far-reaching enough to fulfil the definition of damages that really threaten national security. As a result there is no need for the administrations to act.

Currently, there are some promising CIIP R&D projects like the CI2RCO project[1] as well as projects at

[1] www.ci2rco.org

Dartmouth College's Information Infrastructure Protection Centre (I3P).[2] A few Ph.D. theses have been published the last years.[3] But one important aspect regarding CIIP should not be overlooked: not only is CIIP a scientific subject but also a political task. Communication is vital.

The examples of the USA and Germany clearly illustrate that the respective governments currently show little interest in CIIP, although there are many gaps where efforts are definitely needed. CIIP R&D results to fill the gaps are certainly needed in the following areas:

- Policy: Policy and conceptual papers for different aspect of CIIP to support current CIIP policies;
- Co-ordination of activities: A central, responsible unit for CIIP has to be created in all countries;
- Public-Private Partnerships: models for trusting partnerships;
- International activities: The current working-groups are still weak in results;
- Crisis Management: There is a need for scenarios and basic materials to conduct (tabletop) exercises;
- Public Relations: There are hardly any governmental efforts for public relations in the field of CIIP. But information and sensitisation is necessary;
- Terms and Definitions: The terminology for CIIP is still rather fuzzy both in the international and the national context.

The current behaviour of the administrations could indeed jeopardise results achieved so far. The IT dependence of critical infrastructures increases day by day. CIIP solutions require the co-operation between the private sector and the research community and the necessary resources (financial, experts). Without doubt: CIIP has several great challenges to overcome within the coming years.

[2] www.i3p.org

[3] Schulze, Tillmann: Bedingt abwehrbereit. Schutz kritischer Informations-Infrastrukturen in Deutschland und den USA. Wiesbaden 2006. Also: Sonntag, Matthias: IT-Sicherheit kritischer Infrastrukturen. Von der Staatsaufgabe zur rechtlichen Ausgestaltung. München 2005.

Complex Network and Infrastructure Protection - CNIP 06 in Rome

Executive Round Table "HOW TO BUILD R&D COLLABORATIONS ACROSS THE CONTINENTS WITH REGARDS TO CRITICAL INFRASTRUCTURE PROTECTION"

Sandro Bologna

CNIP06 International Program Committee Chairman
Phone: +39-06-30483708
E-mail: bologna@casaccia.enea.it

Claudio Balducelli

CNIP06 General Chairman
Phone: +39-06-30483334
E-mail: claudio.balducelli@casaccia.enea.it

Multidisciplinary was the main characteristic of the CNIP 06 International Conference held in Rome, 28-29 March, 2006. The level of participation was very high: 8 key note speakers, 44 papers presented in two parallel tracks, each one made of several scientific sessions, 10 papers in poster sessions, about 200 scientists and engineers coming from every part of the world.
In the scientific sessions debates and discussions addressed the following themes:

- how to understand vulnerabilities and scenarios, and propose protection methods and tools for different types of infrastructures;
- how to apply risk analysis methodologies for Critical Infrastructure protection;
- how to understand the topological and structural vulnerability of single and (inter)dependent networks;
- how to understand the societal/managerial issues of Critical Infrastructure Protection.

The Conference was ended with a Round Table. In the following is the summary of the executive round table at the end of the CNIP 06.

Roberto Vacca, an independent Consultant was moderating the discussion, where the following personalities participated:

- Claudia Eckert – Managing Director Fraunhofer Institute for Secure Telecooperation, Germany
- Paul K. Kearns – President and Managing Director Battelle Italia, USA
- Paul D. Domich - CIP Portfolio Director, DHS, USA
- Paolo Donzelli – Prime Minister Office, Innovation and Technology Department, Italy
- Jacques Bus – Head of Unit ICT for Trust and Security, DG INFSO, EU
- Harald Drager – President TIEMS, Norway
- George Apostolakis – Professor, MIT, USA
- Alberto Sarti – Vice President Defence Products Function, Finmeccanica, Italy

Roberto Vacca opened the Round Table with the following statement:
"I contend that this Round Table should reassess the results reached in different contexts and also discuss general issues like:

- Design integration and co-operation among designers of different systems providing cross risk assessment and determining how to create inter-systemic event trees;
- Training of end users and operators with special consideration given to override procedures, in low probability occurrences not foreseen by system designers;
- Optimising communication standards and practices for timely monitoring and control of adjacent systems;
- Solve the problem of lack of transparency of control software. Man-machine communication standards are needed to discriminate between hardware, communication and software faults.

I suggest that the Roundtable might appropriately blueprint the outline of an

international network of experts to co-operate integrating their expertise and approaches to accelerate progress on the path of security and resilience of complex systems and infrastructures. [This could possibly have an informal character, in the vein of so called *invisible colleges*]."

After that a first round among the panellists has started in the following order.

Claudia Eckert made the following statements:

- We have to learn from each other. People from power grid and networks in general have to learn from computer sciences, and vice-versa.
- We need to bring together different stakeholders. Unfortunately we are treating sensible data. We should establish a Trust Platform to exchange information in a reliable way.
- We have to improve education on the topic of Complex Networks and Infrastructure Protection.

Paul Kearns made the following statements:

- Complex Networks and Infrastructure Protection is a new field, still very nebulous; we need continuous collaboration with stakeholders and industry.
- We need to use best practice in modelling development.

Paul Domich made the following statements:

- US Department of Homeland Security has already collaborations with Canada, Australia, UK and EU on the subject of Critical Infrastructure Protection.
- There will be a workshop organised by DHS in the Autumn 2006.
- More research is needed in the field of Complex Networks and Infrastructure Protection.

Jacques Bus made the following statements:

- I agree with the different needs mentioned from the previous panellists, but I would also like to mention what is already in place funded from EU: e.g., CI^{2}RCO, IRRIIS, ENISA, European CIP Newsletter, etc.
- There is already in place a collaboration between the EU and NSF. We have just had a successful Workshop in Washington D.C., March 16 and 17. At the workshop we agreed on exchanging experiences among EU and NSF projects, and in programming we try to be as complementary as possible.
- There is still a lot of work to be done, but we have started and we are on the way.

George Apostolakis made the following statements:

- We need a lot of work to validate the proposed models, as was started many years ago (and continues) with the risk analysis for nuclear power plants and other hazardous facilities. Workshops like this are welcome.
- If we want to support decision makers, we should have valid models in our hands otherwise we will fail.
- More than just EU-US collaboration, we need international peer review and scrutiny of existing models.

Alberto Sarti made the following statements:

- Co-operation is welcome but unfortunately we have to collaborate inside a competitive system and that is not easy.
- To collaborate means many actors around a table for pursuing the same goal. That is not easy in Europe because Europe is not a "nation" but a "set of nations".
- Just an example, in the Airbus 50% of the technology is coming from the US, while in the Boeing, only 10% of the technology is coming from the EU.

Paolo Donzelli made the following statements:

- Complex Networks and Infrastructure Protection is an "emerging field" that needs much more research.
- We need to establish a "common language" to deal with these new systems of systems.
- There was a considerable shortness of projects on security in the last Italian National Research Programme (PNR) call for ideas, less than 7%.
- We need to work about what kind of measures we should put in place to support international collaboration.

Harald Drager made the following statements:

- TIEMS as a scientific association is an opportunity for establishing international co-operation among different people working on Critical Infrastructure Protection.
- A Special Interest Group on Critical Infrastructure Protection has been already started, with about 30 members, from different countries.

At the end of the first round among the panellists, **Roberto Vacca** said that we should concentrate more on prevention of disasters (caused by hackers, vandals and terrorist attacks as well as due to mistakes and shortcomings in design and in management and maintenance). Emergency management is certainly a relevant and vital sector of research and optimisation activity, but it should be considered a last line of defence. Security and protection should also be considered as resources to be relied on to prevent the most deadly threat, i.e. nuclear war unleashed by terrorists or by rogue states or by mistaken retaliation after misinterpreted false alarms. Total nuclear disarmament should be on all agendas concerning security and protection.

A second round among the panellist was started in the following order.

Claudia Eckert: Modelling is not the only tool we should look for, we have to look also to simulation, human factors, test beds and above all how to share test beds among EU and US, because they are very costly.

Paul Kearns: We are talking about Systems of Systems, in which there are a lot of legacy aspects. Legacy problem should be investigated.

Jacques Bus: The area of Complex Networks and Infrastructure Protection is an interdisciplinary area that would benefit from developing common semantics.

George Apostolakis: The decision makers must prioritise the allocation of resources, but this is a function of what kind of attacks we can foresee and what their likelihood is. Unfortunately, on this topic, we do not have any data or models to support the decision makers in a meaningful way.

Alberto Sarti: Critical Infrastructure Protection is not only a technological problem, but also a human and political problem. People want to know where they are in the chain of responsibilities.

Paolo Donzelli: We should agree on what kind of outputs we would expect from a network of experts.

Harald Drager: Dialogue is very important. TIEMS is a very good means to support and facilitate dialogue.

At the end of the second round were collected a few statements from the floor.

Flaherty (Univ. of Melbourne, Australia) – In Australia, we have established the Research Network for a Secure Australia (the RNSA www.SecureAustralia.org) which is focused on CIP, seeking to mobilise Australian research in the various research areas of CIP connecting industry, government and academic researchers together, to achieve common research outcomes. We have, as well, developed significant international collaborative research exchanges in the US, UK, Asia and European Union. In fact, in the UK, Imperial College is a contact point for RNSA in the UK, and we are keen to further develop these types of research linkages within the European Union.

Gadomski (ENEA, Italy) – I agree with all the needs mentioned, especially related to the critical role of human and organisational socio-cognitive factors. For the co-operation reinforcement, three items I consider essential.
The primary is a motivation building of political decision-makers – it requires clear and convinced expertises transfer from international research communities to the EU and US stakeholders and policy makers. Here, the demonstration of the *business – safety* relation is crucial for all parts. For this task, independent experts representing international professional organisations, such as TIEMS may play important role.
The second factor is a technical consensus building to cross the barrier of the comprehension between researchers and technologists engaged in the development of CIIP systems, i.e., the necessity of the development of "trans-oceanic" common ontology/ terminology standards. The last but not least, is a priority planning, it requires an EU-US *business co-operation committee* involving and supported by big owners of LCCIs which will be decided to provide funds for long-term Euro-American R&D CIIP programs.

Roberto Vacca closed the round table with the following recommendations:
In order to establish an operational and concrete co-operation between panellists, their organisations and other experts and outfits, it would be desirable that we all produce program statements to be centralised at ENEA as a first step to implement synergies and cross-fertilization through a forum / interdisciplinary exchange. ENEA should take the lead in this endeavour.

According to the organisers of CNIP 06, that are also the authors of this report, one important question not addressed at the Conference and that should be addressed in a next editions of the Conference is relative to the organisational model that may be more adequate to improve emergency prevention and management for Critical Infrastructure.
It is better a "central" or a "federate" organisational model? What is the more effective and realistic model?
To address interdependency problem of critical infrastructures, there is the necessity to share sensible data between different stakeholders: but, due to their competition, it is actually a not solved problem.

After the conference, a comment from Mr. Giuliano Basso, Energy Solution Europe, about this topic was: *there is a gap, or better, a divergent interest in the different stakeholders and energy market players between the need of 'competition' and the need of a 'collaborative' behaviour to achieve the necessary common goals to improve security and operate the gas logistic chain in the best way.*

The auspice is to continue to discuss about these themes, increasing in the government institutions, private networks operators, and scientific communities the awareness about the criticality and the importance of these issues.

For more information about the CNIP 06 conference and presentations see:
http://ciip.casaccia.enea.it/cnip06

CRITIS 2006

1st International Workshop on
Critical Information Infrastructures Security
Samos Island, Greece, August 30 – September 2, 2006

Javier Lopez

CRITIS'06 Program Chair

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

Key sectors of modern economies depend highly on ICT. The information flowing through the resulting technological super-infrastructure as well as the information being processed by the complex computing systems that underpin it becomes crucial because its disruption, disturbance or loss can lead to high economical, material and, sometimes, human loss. As a consequence, the security and dependability of this infrastructure becomes critical and its protection a major objective for governments, companies and the research community.

CRITIS'06 has been born as an event that wants to bring together researchers and professionals from universities, private companies and Public Administrations interested or involved in all security-related aspects of Critical Information Infrastructures.

The focus of CRITIS is to bring together researchers and professionals interested in all security-related aspects of Critical Information Infrastructures

Our main goals is that attendees with different expertise can meet and learn about the new advancements in the security of Critical Information Infrastructures while, at the same time, discuss about the heterogeneous issues and problems in the area, identifying common research interests and establishing co-operation networks.

Conference Scope

The following is a non-exclusive list of areas covered in CRITIS'06: Continuity of Service, Dependable Infrastructure. Communications, Early Warning Systems, Embedded Technologies Security, Incident Response, Infrastructure Interdependencies, Information Assurance, Internet-based remote control, Forensic Techniques, National and Cross Border Activities, Network Survivability, Trust Models in Critical Scenarios, Policy Management, Resilient Software, Secure Information Sharing, Security Logistics, Security Modelling and Simulation, Security Risk, Threats Analysis, and Vulnerability Assessment.

Paper Submission

We invite research papers, work-in-progress reports, R&D projects results, surveying works and industrial experiences describing advances in the aforementioned or related areas. Submissions will be evaluated by the reviewers of our international committee of experts from academia and industry. Accepted papers will be presented at the workshop and post-proceedings will be published by Springer in the Lecture Notes in Computer Science series. The deadline for paper submission is June 16th, 2006.

For specific submission instructions and general information of the event, see: http://critis06.lcc.uma.es/

The IMF 2006 Conference Connects IT Security Teams and IT-Forensic Experts

The international conference on IT Incident Management and IT Forensics (IMF) provides a common platform for the still separated communities of the security teams, aka CERTs or CSIRTs, and the IT forensic experts. The conference will take place in Stuttgart on October 18 – 19.

Oliver Goebel

Is the Program Chair of the International Conference on IT Incident Management and IT Forensics IMF 2006 , he is the CISO of Stuttgart University and Head of RUS-CERT

Information technology has become crucial to almost every part of society. IT infrastructures have become critical in the world-wide economy, the financial sector, the health sector, the government's administration, the military, and the educational sector. Due to its importance the disruption or loss of IT capabilities results in a massive reduction of operability. Hence, IT security is continouslygaining importance.

Operational Security is still a wallflower

Although security usually gets integrated into the design process of IT systems nowadays, the process of maintaining security in the operation of IT infrastructures still lacks the appropriate attendance in most cases.

Especially the capability to manage and respond to IT security incidents and their forensic analysis is established in the rarest cases. The quickly rising number of security incidents worldwide makes the implementation of incident management capabilities essential.

IMF – a Common Forum for CERTs and IT Forensic Experts and Operators

In order to advance the fields of IT Incident Management and Forensics the special interest-group Security - Intrusion Detection and Response (SIDAR) of the German Informatics Society (GI) organises an annual conference, bringing together experts from throughout the world, to discuss state of the art in the areas of Incident Management and IT Forensics (IMF). IMF promotes collaboration and exchange of ideas between industry, academia, law-enforcement and other government bodies.

IMF 2006
October 18 – 19, 2006
Stuttgart, Germany
http://www.imf-conference.org/

IMF has a Broad Scope

The conference covers the following topics in its two main areas:

IT-Incident Management

- Purposes of IT Incident Management
- Trends, Processes and Methods in Incident Management
- Formats and Standardisation in Incident Management
- Tools for Incident Management
- Education and Training in the field of Incident Management Awareness
- Determination, Detection and Evaluation of Incidents
- Procedures for Handling Incidents

- Problems and Challenges while establishing CERTs/ CSIRTs
- Sources of Information/ Information Exchange/ Communities
- Dealing with Vulnerabilities (vulnerability response)
- Current Threats
- Early Warning Systems
- Organisations (Nat. CERT-Associations, FIRST, TERENA/ TI, TF-CSIRT)

IT-Forensics

- Trends and Challenges within IT-Forensics
- Methods, Processes and Applications for IT Forensics (Networks, Operating Systems, Storage Media, ICT-Systems etc.)
- Evidence Protection in IT Environments
- Standardisation of Evidence Protection Processes
- Data Protection- and other legal implications for IT Forensics
- Investigation Methods and Processes
- Juristic Relevance of IT Forensic Investigations
- Tools for IT Forensics
- Forensic readiness

High-Level Program Committee

The program committee reviewing submissions and assuring the quality of the presentations selected is formed by high-ranking experts from both communities. It includes members from the industry, law-enforcement organisations, lawyers specialising in IT forensics, as well as universities and other academic institutions.

- Henrik Becker, Kanzlei Becker, Germany
- Vlasti Broucek, University of Tasmania, Australia
- Ian Bryant, NISCC, UK
- Brian Carrier, CERIAS, USA
- Andrew Cormack, UKERNA, UK
- Herve Debar, France Telecom, France
- Ralf Doerrie, Telekom-CERT, Germany
- Maximilian Dornseif, University of Mannheim, Germany
- Ulrich Emmert, esb Rechtsanwaelte Stuttgart, Germany
- Guenther Ennen, BSI/CERT-Bund, Germany
- Christoph Fischer, BFK-Consulting, Germany
- Sandra Frings, Fraunhofer IAO, Germany
- Oliver Goebel, RUS-CERT, Stuttgart University, Germany
- Dieter Gollmann, TU Hamburg-Harburg, Germany
- Detlef Guenther, CERT-VW, Volkswagen AG, Germany
- Bernhard Haemmerli, ACRIS GmbH, Switzerland
- Hardo G. Hase, IT-Consulting Hardo G. Hase, Germany
- Mark Hoestra, IT Forensic BV, Nethlerlands
- Klaus Peter Kossakowski, DFN-CERT, Germany
- Thorsten Lieb, Avocado Rechtsanwaelte Frankfurt, Germany
- Jim Lyle, NIST CFTT, USA
- Neil Mitchison, Joint Reseach Centre, EU
- Jens Nedon, Consecur, Germany
- Jason Rafail, CERT/CC, USA
- Damir Rajnovic, CISCO-PSIRT, USA
- Gavin Reid, CISCO-INFOSEC, USA
- Dirk Schadt, CA, Germany
- Christian Schaller, SIEMENS-CERT, Germany
- Rolf Schulz, gnsec, Germany
- Marco Thorbruegge, ENISA, Greece
- Helmut Ujen, Bundeskriminalamt, Germany
- Andreas Wagner, Frontrunner FZ LLC, Dubai
- Stephen Wolthusen, Gjovik University College, Norway

Sponsorship Opportunities

We solicit interested organizations to serve as sponsors for IMF 2006; please contact the Sponsor Chair, Dirk Schadt, for information regarding corporate sponsorship (mailto: dirk.schadt @ gmail.com).

Registration

Registration is not open yet.

Details on the registration will be published on IMF's website at

http://www.imf-conference.org/

The conference will take place in Stuttgart on October 18 – 19 in Stuttgart.

Selected Links and Events

Actual Upcoming CIIP Conferences in Europe

- INFSO D4 events, http://cordis.europa.eu/ist/trust-security/events.htm
- IST events, http://europa.eu.int/information_society/newsroom/cf/newsbytheme.cfm?displayType=calendar&tpa_id=7
- DIMVA 2006 - Third GI SIG SIDAR Conference on Detection of Intrusions & Malware, and Vulnerability Assessment July 13-14, 2006 – Berlin, Germany: http://www.dimva.org/dimva2006
- Applied Security Congress and Exhibition September 20&21 2006, Zurich: www.security-zone.info
- NATO/EAPC/PfP Workshop in Zürich, August 24-26: The Swiss Federal Department of Foreign Affairs organizes a fourth Workshop on Critical Infrastructure Protection and Civil Emergency Planning in the framework of its Partnership for Peace activities. The event will take place on August 24-26, 2006, near Zurich and is entitled "Building Bridges between Stakeholders to Mitigate Disasters." The Workshop's main objectives is to examine how critical infrastructures of the energy, communication and transportation sectors and key industrial plants are exposed to various risks and threats and how they can be protected. Further information can be obtained directly from the Workshop Organizer (Stefan Brem: stefan.brem@eda.admin.ch) or on the PfP-Partnership Forum website http://pforum.isn.ethz.ch.
- EU Joint Software and Service Development/ Security and Dependability Workshop, Sept 6-7, 2006 ENST Paris, organized form ESFORS and NESSI. Goal: Defining input for FP7. Contact: zdooly@tssf.org
- 6th European Dependable Computing Conference, Coimbra, Portugal, October 18-20, 2006; http://edcc.dependability.org The sixth European Dependable Computing Conference aims to provide a European venue for researchers and practitioners from all over the world to present and discuss their latest research results and developments. Papers are solicited on theory, techniques and tools for the design, validation, operation and evaluation of dependable computing systems. Besides traditional hardware and software faults, concerns include human interaction faults, be they accidental or malicious.

Conference Papers and Periodic E-Reports

- EAPC / PfP International Workshop on CIP: http://www.dfae.admin.ch/eda/e/home/foreign/secpe/intsec/wrkshp/cybsec.html
- CIP Report USA, is published once a month, accessible with a email note or from the home page: http://cipp.gmu.edu/report
- International Journal of Emergency Management (IJEM): http://www.inderscience.com/browse/callpaper.php?callID=257
- International Journal of Critical Infrastructures (IJCIS): http://www.inderscience.com/browse/index.php?journalID=58#board
- International Journal of Information and Computer Security (IJICS): http://www.inderscience.com/browse/index.php?journalID=151#objectives

Various Resources for IT Risk, Security and Disaster Management

- European Homeland Security Agency: www.e-hsa.org
- http://www.nsarchive.org
- The International Emergency Management Society (TIEMS) http://www.tiems.org/index.php
- http://www.listible.com/list/best-pc-security-sources (various links)
- http://CASEScontact.org (alerts, guides about IT security, worms, rootkits, spyware, identity theft, cyber crime and risk management - weekly news, podcasts/audio files - delivered via e-mail or RSS feeds)
- http://blog.CASEScontact.org (better security with Windows - hands-on solutions with the tools - delivered via e-mail or RSS feeds)
- http://blog.CyTRAP.eu (EU - IST News - the daily news and weekly summary about security trends, critical infrastructure protection, risk management and the latest tools to fight off attacks - delivered via e-mail or RSS feeds)
- http://cyTRAP.org/RiskIT/course/view.php?id=4 (glossaries in English and German about IT security and critical infrastructure protection -- login as a guest, free access) http://cytrap.eu/RiskIT/course/view.php?id=3 (intelligence reports about vulnerabilities, threats, malware, infrastructure protection, offshoring and cybercrime - login as a guest, free access)