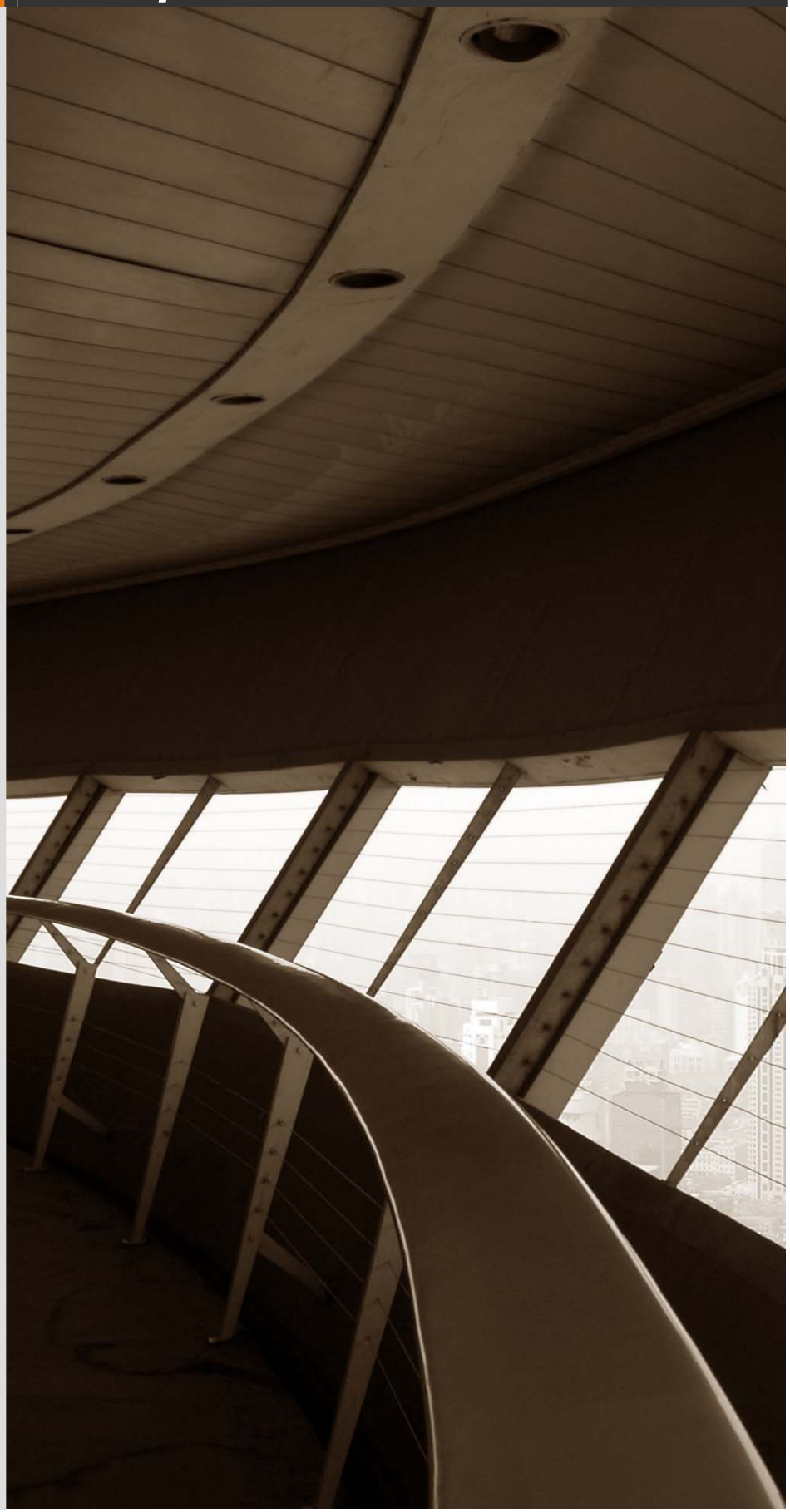
April/Mai 2005, Volume 1, Number 1

ECN

European CIIP Newsletter



Building a secure EU Information Infrastructure

Focus on Critical Information Infra-structure Research Co-ordination

Success and Risk Factors for Multinational CIIP Co-operation

International Cooperation for Critical Infrastructure Protection

Secure Electronic Communication Infrastructure

CI²RCO

> About ECN
ECN is co-ordinated with
The European Commission, Dr. Andrea Servida
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
and reply the received registration request.

>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/

>Founding Editors
Eyal Adar CEO iTcon, eyal@itcon-ltd.is
Bernhard M. Hämmerli, HTA, Initiator and Main Editor
bmhaemmerli@acris.ch
Eric Luiijf, TNO, Eric.Luiijf@tno.nl
Willi Stein, BSI, willi.stein@bsi.bund.de

> Graphics and Layout
Florian Widmer florian_widmer@gmx.net

> Spelling:
British English is used except for US contribution

Table of Content

Introduction

European Activities

Country Specific Issues

Methods and Models

News and Miscellaneous

Selected Links and Events

CIIP: Why should we have a European CIIP Newsletter?

Tasks like CIIP are trans-national and trans-disciplinary. Therefore the exchange of information should be fostered. ECN is a platform to communicate CIIP related activities to provide networking possibilities for CIIP experts and stakeholders. We hope it serves its purpose.

Dr. Bernhard M. Hämmerli

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

The idea of a European CIIP Newsletter was borne at the first CIIP conference in Frankfurt in 2003. As we were discussing topics and activities during the planning phase, we realized that the Frankfurt conference is a valuable start, but more sustainable actions should follow (see under **Actual: Upcoming CIIP Conferences in Europe,** Page 29 and following).

A Long Development Time for ECN First Issue

There are different ways to promote new ideas. As we were discussing the focus of a new CIIP newsletter we decided to issue a trial issue for funding purposes.

Europe is aware with a lot activity in CIIP.

With the newsletter we can improve co-ordination and generate synergies.

The development of a trial issue took some time. During this development phase the following changes occurred:

- The EU-sponsored CI^{2}RCO project (see article before) is willing to support ECN financially,
- ECN can directly start with the first volume,
- ECN has been adjusted regarding its structures and its content.

Goals of the CIIP Newsletter

Numerous CIIP efforts have been launched or are still on-going in Europe, in NATO as well as within the European research community have been launched or are still on-going. The exchange of information on these projects or on the findings of the numerous past and planned CIIP conferences is neither very well organised nor easily available. A common platform to share information is still lacking. Therefore the ECN has the following focus:

- Articles on current CIIP topics
- Reports about actual political decisions
- New CIIP-related research programmes
- A CIIP "Who is who"
- Other CIIP related issues
- Announcements of planned CIIP conferences
- Web links
- Reference to CIIP-related publications

In general the ECN aims at supporting and evolving the European CIIP process across the 25 nations and its decision makers.

About ECN Policies

Discussing in the CI²RCO kick off meeting about ECN, the board supported the definition of the policies to have guidelines about the wanted articles. All policies will be applied in a tentative but not absolute manner.

About ECN Content

- Publish articles on CIIP topics concerning the aspects of politics, science / research, problem owners (operators and agencies), CIIP producers of hard-/ software and other relevant stake holders of critical infrastructure CIIP topic.
- Generally sophisticated technological articles are published if its content represents a major step in security development.
- The article must have aspects of CIIP, e.g. have viewpoints to high availability or continuity of service for essential widely used infrastructure.
- Each number should have:
  - an **Introduction**
  - a report about **European Activities** in security and / or its projects
  - **Country Specific Issues** such as:
    -national reports
    -new country report
    -American / Canadian report
  - Reports about **Methods and Models**
  - In **News and Miscellaneous** further articles which do not fir in one of the category above will be published
  - links (un)commented to conferences
  - links to CIIP sites

About ECN Publication

- Email registration can be done with an email (also content free) to:
  subscribe@ciip-newsletter.org
- Each new ECN issue will be announced by email to the registered email list automatically generated by
  submit@ciip-newsletter.org
- 3 issues per year will be provided at the start:
  April/ May,
  August/September,
  December/January
- The CIIP Newsletter is published on the following web site:
  http://www.ci2rco.org/
  and will be replicated soon on the following web sites:
  - EU commission
  - Telecom Paris
  - IABG
  - DLR
  - CityPlan spol sro

  Publishment on the web pages of further interested members of the CIIP community is very welcome and wanted.

General Policies

- ECN publishes articles provided by experts at no costs
- Advertisement of CIIP conferences is free of cost until a need for regulation arises. The advertised conferences must adhere the following properties:
  - Multiparty, CIIP related and of a high quality
  - Scientifically or politically of a relevant quality
- British English spelling dictionary is applied except for US contributions (English USA)

Who are the Initiators?

Alphabetic order:
Eyal Adar, CEO of iTcon Ltd, Israel;
Bernhard Hämmerli, Prof. FHZ and Acris, Switzerland;
Eric Luiijf, Consultant CIIP at TNO, The Netherlands;
Dr. Willi Stein, BSI, Germany.

The editors thank Andrea Servida (EU/ DG Information Society) for his warm support and encouragement to launch the European CIIP Newsletter.

Paul Friessem (Fraunhofer, SIT) and Daniel Bircher (Ernst Basler + Partner Ltd) have been supporting the development from a trial issue to the fully newsletter. We thank them especially for their coaching and support.

Building a secure EU Information Infrastructure: the role of R&D

The research and development programmes have significantly contributed to raise awareness and stimulate the debate on how to meet the future security challenges of the information infrastructure. This is particularly true for the European R&D whose role would possibly become even more important because of the activities planned under the Information Society Technologies (IST) Programme and the Preparatory Action on Security Research (PASR).

Andrea Servida[1]

Andrea Servida is Deputy Head of the Unit ICT for Trust and Security in the Directorate General Information and Media of the European Commission. Among other duties, from 1997 to 2002 he has been in charge of the dependability initiative in Information Society under the IST Programme. Before joining the Commission he worked in industry for nearly eight years as R&D project manager. He graduated with Laude in Nuclear Engineering at Politecnico di Milano and carried PhD studies on Artificial Intelligence at Queen Mary and Westfield College, University of London.
E-mail: andrea.servida@cec.eu.int

It is my believe that research, in particular when it is carried out at the European level, has a unique role to play in fostering a better understanding of the societal challenges associated to the advent of highly sophisticated technologies. The experience of the "European dependability Initiative" under the Information Society Technologies (IST) Programme of the 5th Framework Programme (FP5) has showed how European R&D could be beneficial in anticipating and meeting the needs of our Society.

Supporting R&D on CIIP at the European level would be beneficial for everybody

This paper briefly presents this experience and introduces the future plans on CIIP research in the second part of Information Society Technologies (IST) priority under the 6th Framework Programme (FP6) and in the Preparatory Action on Security Research (PASR).

The dependability initiative in Information Society

In 1997, the European Commission launched, as part of the R&D Information Technology (IT) Programme, an activity to identify the future research and technological challenges on security and dependability in Information Society. This activity led to the European initiative on dependability (also called DEPPY) which took the form of Cross Programme Actions on dependability under the Information Society Technologies (IST) Programme. This initiative pulls together a number of European scientists from different communities (such as fault tolerance, security, reliability, system correctness, etc.) to work on how to provide solid and robust technical foundations to Information Society. In this context, the following two areas were identified as of highest priority: i) large scale networks and information infrastructures, and ii) extensively deployed and networked embedded systems.

The projects funded under DEPPY were instrumental to characterise the urgency to push research in looking more holistically at the systemic issues affecting the dependability of the information infrastructure and its interdependencies to other societal and economic infrastructures. In this respect, DEPPY has also highly valued the international cooperation, in particular with the USA, on R&D as a means to further leverage the European know how, researchers and capabilities.

The research on security and dependability in the Information Society Technologies thematic priority of FP6

Under FP6, the research on security and dependability has received a lot of

attention in the Information Society Technologies thematic priority. The allocated budget to this domain was significantly increased (to nearly 150 M€ in four years) and one of the key priority was set on promoting the development and use of advanced technologies to master and manage CIIP and interdependencies.

Achieving the dependable behaviour of the information infrastructure would mean

1. ensuring the flexible and co-operative management of the large-scale computing and networking resources,
2. establishing distributed early warning capability and
3. providing resources for effective prevention detection, confinement and response to disruptions. And, in so doing, we would contribute to protecting our industry wealth and investments in ICT as well as in other intangible assets.

On the other hand, we should not forget that the dependable behaviour of the infrastructure depends on the behaviour of a growing number of players, systems and networks (including the users and the user systems). The interdependency among critical infrastructures (like the electric grid, e-commerce and e-business systems, the financial/banking systems, telecommunication, etc.) that are enabled and supported by the information infrastructure can not be easily mastered by currently available technologies. They are global and geographically distributed beyond any jurisdictional or governmental boundary.

The overall goal of pursuing dependability and interdependencies in the Information Society will be to support innovative and multidisciplinary research and development to cope with and support scale issues of dependability connected with new business and everyday life application scenarios.

Important aspects of the scale issues would be those associated with:

- the increasing volatility and growing heterogeneity of products, applications, services, systems and processes in the digital environment;
- the tighter interconnection and interdependency between information and communication systems and infrastructures and with other vital services and systems for our society and our economy.

The detailed articulation of the research priorities in IST benefited a lot from the targeted road mapping exercise that had been launched by the Commission at the end of FP5.

In the fourth Call of the IST that closed on 22 March 2005, CIIP and interdependencies are included as a priority of the Strategic Objective 2.4.3 ‘towards a global dependability and security framework’.

The Preparatory Action on Security Research

Further to the requests from the Parliament and the Council, the Commission started in 2004 a Preparatory Action in Security Research entitled "Enhancement of the European industrial potential in the field of Security research 2004-2006". The goal of this activity is to contribute to the improvement of the European citizens’ security, to reinforce European technological and industrial potential in this area and to prepare for a future European Security Research Programme (ESRP). This Preparatory Action covers the period 2004-2006 and addresses five main areas, including the protection against terrorism of networked systems. In parallel to the preparation to this activity, a Group of Personalities (GoP) was established in 2003 and tasked to propose key orientations, principles and priorities for a future ESRP. The GoP report describes the essential elements of an ESRP and its contribution to address the new security challenges of a changing world. Its main recommendations include:

- the establishment of an ESRP, from 2007 onwards, with funding of at least 1 billion Euros per year, additional to currently existing resources,
- the creation of a “European Security Research Advisory Board” to define strategic lines of action, user involvement, implementation mechanisms and a strategic agenda for the ESRP.

As a follow-up, the Commission adopted on September 7, 2004 a Communication entitled “Security Research: The Next Steps”, to initiate a debate with the Council and the Parliament. It subscribes to the main thrust of the report and indicates steps to be taken to progress the activity, that is:

- consultation and cooperation with stakeholders, in particular via the being established “European Security Research Advisory Board”;
- development of an ESRP as part of FP7.
- ensuring an effective institutional setting, taking into account Common Foreign and Security Policy and European Security and Defense Policy and other relevant Community policies, as well as developing cooperation and synergies with the European Defense Agency.
- establishing a governance structure responding to the needs of security research work in terms of contract, participation and funding.

The way ahead on security and dependability research

In the course of the consultation for the preparation of the Work Programme 2005-2006 we have solicited a broader reflection on what would be the future challenges for EU research in this domain. Such a process has already identified as a critical priority the need to make the digital environments and systems able both to dynamically and autonomously adapt and evolve securing the seamless control and use of data, information and knowledge (plasticity) as well as to autonomously and gracefully tackle, tolerate and recover from accidents and/or attacks. Of course, such preliminary results would be investiga-

ted further in collaboration with researchers and stakeholders in order to finally identify the key priorities for future R&D in FP7.

Concluding remarks

The need for a strategic approach to CIP, CIIP and interdependencies is getting higher and higher on the agenda of policy makers. In June 2004, the European Council asked the Commission and the High Representative to prepare an overall strategy to protect critical infrastructure. A lot of work has been done at the European level to both provide an overview of ongoing Commission activities related to the protection of critical infrastructure as well as propose measures to meet the mandates given by the European Council. This resulted in four Commission communications in October 2004 among which is the COM (2004) 702 on 'Critical Information Infrastructure Protection in the fight against terrorism'. In December 2004, the European Council conclusions welcomed the revised Commission Action Plan that would lead, among others, to the establishment of a European Programme for Critical Infrastructure protection with potential trans-boundary effects before the end of 2005. It is, therefore, a great pleasure for me to witness the publication of the first issue of this European newsletter on critical information infrastructure protection, which could not be timelier to help the European exchanging information and fostering awareness, which are two fundamental steps in shaping up a coordinated European strategy for CIP. I wish the editors of this important endeavour all the bests because their success would be the success for the entire EU.

Focus on Critical Information Infrastructure Research Co-ordination

The CI²RCO Project placed within the 3. IST-Call of the 6th Framework Programme by the European Commission addresses the creation and co-ordination of a European Taskforce to encourage a co-ordinated Europe-wide approach for research and development on Critical Information Infrastructure Protection (CIIP).

Paul Frießem

Head of Department Secure Processes and Infrastructures of the Fraunhofer Institute for Secure Information-Technology (FhG-SIT)
Phone: +49 (0) 22 41 / 14 – 31 94
E-Mail: paul.friessem@sit.fraunhofer.de
Internet: http://www.sit.fraunhofer.de

Modern society depends nowadays heavily on Information and Communication Technology (ICT). ICT has pervaded in all traditional infrastructures, rendering them more intelligent but more vulnerable at the same time. Our new economy is highly dependent on such safe and reliable information infrastructure services – they are to be considered as critical information infrastructures. A disruption or destruction of those infrastructures would have serious impact on the health, safety, security or economic well-being of citizens or the effective functioning of governments. Survivability and dependability of Critical Information Infrastructures have therefore to be considered on a level which goes beyond the level of the local and national stakeholders to guarantee an acceptable level for economy, society, and politics.

Europe's critical infrastructures have become more dependent on common information technologies.

Challenges

Europe has recognised the challenges of CIIP later than the US, Canada and Australia. Long-term shared visions for research and exploitation among Member States as identified by Member States in the European Research Area (ERA) working group of the IST Committee (ISTC) and by various nations themselves are strongly needed.

Project objectives

Thus, the main objective of the *Critical Information Infrastructure Research Co-ordination* action (CI²RCO) project co-ordination action within the Information Society Technology (IST) Call 3 of the 6th European Framework Programme – is to create and co-ordinate a European Taskforce to

- encourage a co-ordinated Europe-wide approach for research and development on Critical Information Infrastructure Protection (CIIP), and to
- establish a European Research Area (ERA) on CIIP as part of the larger IST Strategic Objective to integrate and strengthen the ERA on Dependability and Security.

In line with the EU-IST strategic objective "Dependability and Security", the CI²RCO consortium further on aims to support CIIP awareness and actions in the EU-25 and Associate Candidate Countries[2] (ACC) countries in order to:

- provide a forum and a platform to bring together the different key players to exchange experiences, share interests and define areas for joint activities,
- identify the key dependability and security CIIP challenges,
- foster truly multidisciplinary and innovative approaches to research that would build on the contribu-

[2] Associated Candidate Countries are Bulgaria, Romania and Turkey

tions provided by diverse scientific communities,

- encourage and support the national and international co-operation on key global CIIP research issues,
- develop recommendations and a roadmap for current and future CIIP research activities,
- support policy-makers in charge of financing or managing R&D programmes.

In implementing an extended network of experts, expertise, and knowledge for CIIP, CI^{2}RCO starts from the hypothesis that national, regional and international research programmes with a wide variety of objectives do exist which have direct or indirect relation to CIIP. Relevant players of research, research funding actors, policy makers and critical infrastructure stakeholders are mostly unaware of such CIIP related R&D programme similarities in various fields due to lack of knowledge, fragmentation, and limited networking capability, national need to know, restrictive policies and legal obstacles, as well as varying political structures across Europe. These factors lead to isolation and thus hinder an effectively netted and efficient research infrastructure in Europe.

CI^{2}RCO's focus is on CIIP related R&D programmes and initiatives within the EU-25 and ACC.

Project Approach

In order to achieve the objectives stated above, CI^{2}RCO will focus on activities and actions across the EU-25 and ACC that are essential to be carried out at European level and that require collaborative efforts involving research and research funding actors as well as other stakeholders across the European Research Area. This will be accomplished by the set of activities allocated to the following six work packages:

1. Creation of a network of CIIP related research organisations, agencies, promoting initiatives and policy makers
2. Identification of completed, on-going and planned CIIP R&D programmes and projects on national and EU-level
3. Analysis of the European CIIP Research Area according to appropriate evaluation and assessment criteria
4. Feedback loop with CII stakeholders to identify gaps in the current and planned CIIP actions and activities
5. Elaboration of a European CIIP research agenda to determine R&D priorities
6. Provision of a common information platform to supply sustainable support for information and co-operation

In order to facilitate the networking as well as to establish opportunities for collaboration and information exchange, at least four workshops and two international conferences are foreseen within the project's lifetime of two years.

Advisory Board

As the co-ordination action requires a broad EU-25 and ACC support, a major instrument within the project is the so-called Advisory Board representing the participating EU Member States and ACC by delegates mandated by the appropriate European, national, regional or local bodies responsible for financing and managing research programmes and initiatives aiming at the developing European Research Area "Critical Information Infrastructure Protection". The Advisory Board is the central consultation, harmonisation and consensus-building platform for the activities of the participating countries in this area and thus might influence the EU-25 and ACC decisions on CIIP-relevant topics.

Project Consortium

The project consortium has been built around various organisations representing large European communities on the CIIP topic, namely:

- Fraunhofer-Gesellschaft zur Förderung der angewandten Forschung e.V.; Fraunhofer Institute Sichere Informationstechnologie (FhG SIT) as project coordinator, Germany;
- Ernst Basler + Partner AG, Switzerland;
- Ente per le Nuove tecnologie, l'Energia e l'Ambiente (ENEA), Italy;
- Groupe des Écoles des Télécommunications - École Nationale Supérieure des Télécommunications (GET-ENST), France;
- Industrieanlagen-Betriebsgesellschaft mbH (IABG), Germany;
- Nederlandse Organisatie voor toegepast-natuurwetenschappelijk onderzoek (TNO), Netherlands
- Deutsches Zentrum für Luft- und Raumfahrt e.V., Projektträger des BMBF für Informationstechnik (PT-DLR), Germany.

The consortium partners have been recognised, both in their nations and internationally, for their state-of-the-art approaches to C(I)IP issues and their internationally renowned CIIP awareness and outreach activities. The partners have complementary expertise and strong national and international links. The project's programme of work will draw upon that expertise and the broad spectrum of contacts and networks with various CI-stakeholders in EU-25 and ACC stemming from those state-of-the-art activities.

Secure Electronic Communication Infrastructure

The newly established European Network and Information Security Agency, ENISA, has an important role to play in the securing of our electronic communication and information systems.

Mr. Andrea Pirotti

Executive Director, European Network and Information Security Agency.
E-mail: andrea.pirotti@cec.eu.int

While today's society and economy depend heavily on networks and information systems; new wireless applications will enable us to access the Internet from anywhere, at any time; more and more products are connected to the Internet; the potential risks for security breaches and security breakdowns grow as fast as people invent new ways to use the Internet.

We see clear evidence that both businesses and citizens suffer from various kinds of network and information system failure or problems. Such problems can be caused by accident or malicious intent; there is everything from non-compatible software to viruses or other attacks that cause interruption of services and damage to companies, administrations and private users. The electronic communication networks are becoming a critical infrastructure in itself and together with the information technology it has also become vital for the other critical infrastructures such as water and electricity supply.

In order to manage the transformation into a secure information society we all have to contribute; we need to achieve a culture of security.

It has become clear that network and information security is a concern for everybody, from infrastructure and service providers to product and service consumers, that is, citizens, businesses and public administrations regardless of sector or nationality. The worrying part is that we see that with increased complexity of systems and increased use and dependability the problems seem also to grow more common and more expensive and damaging to the information society.

In order to manage this transformation into a secure information society we all have to contribute; we need to achieve a culture of security. ..

What is the role of ENISA?

Network and information security is certainly not a new issue. In fact most Member States have done considerable efforts during a long period of time to strengthen information security. We have seen policies on cryptography, privacy, electronic signatures and on awareness rising, just to mention a few areas. Now we have added the word "network" to the old notion of information security as the interconnected networks create a new set of issues that needs to be solved. The interconnection has also increased the need to co-operate both across sectors and across national borders.

This is what forms the basis for the ENISA. The Agency shall be a forum where all stakeholders can meet in order to be able to increase information

exchange and co-operation on network and information security.

Secondly ENISA will become a centre of expertise to be able to provide guidance and advice to the Commission and to Member State governments and other organizations in Member States.

The main purpose of ENISA is therefore to increase security in order to support industry, end users and consumers. As the Agency will have fairly limited resources, and there are organizations in all Member States already doing work in this area, the idea is not to replace any existing functions. Enterprises, administrations and citizens shall still turn to their national organizations or authorities for help, but now ENISA will be able to quickly provide these with input on how to handle the relevant issues.

The strengths of a European Agency

Although small in size, ENISA will through its structure bring all the stakeholders in network and information security together, both from public and private sector, consumers and researchers, small and big Member States. The Management Board has representatives from all Member States but also from stakeholders, which means academic, business and consumer communities. It has also been decided that EEA EFTA countries (Iceland, Lichtenstein and Norway) shall be able to participate as observers in the Management Board.

ENISA has a Permanent Stakeholder Group consisting of highly qualified representatives from various sectors in society and we have the possibility to establish ad hoc working groups consisting of experts in network and information security

We have already seen a strong interest and support for ENISA from Member States, from the EU institutions and from industry. By increasing cooperation and information exchange ENISA will be able to draw on the experience all over Europe in this area and it will become a centre of expertise.

We must act in concert to get our choice of technical security options and organizational arrangements right. Applying these options in a non-harmonized fashion might lead to inefficient solutions and in practice create obstacles to the single market? For example; if security requirements for goods and services differ from one Member State to another, they could lead to obstacles to free trade across the EU.

ENISA shall avoid conducting overlapping tasks that are already conducted elsewhere, e.g. by CERTs and similar organizations, by software and network industry and by Member States.

With this variety of issues and stakeholders it is very clear that we need to address different user groups in different ways

Promotion of awareness raising activities and of best practices

Acting in concert and making all stakeholders take their own responsibility requires awareness on how to take this responsibility. ENISA will be able to gather best practices on how to raise awareness from what has already been done in Member States. Good examples shall be published so others can follow suit and ENISA shall help put together “awareness raising packages” that can be used for such actions in specific sectors or areas.

ENISA will also gather information on best practices in the area of risk management and risk analysis and assist in the development of risk assessment methods for both public and private sectors. This will also have an impact on how to handle the dependability and interdependencies between the various networks and systems and what this means for the critical communication infrastructure.

With this variety of issues and stakeholders it is very clear that we need to address different user groups in different ways; children and home users need other information than system managers and public authorities. We also believe that the message from ENISA on security should be positive; it is important not to frighten people, but to give some positive tips so that users feel that they know what to do. Users don’t need to be scared, but they need to know what the risks are and how to handle them.

The information on security best practices will be published on the ENISA web site which is currently being built up. Another useful feature of this site will be the “country pages” where each Member State can present its own work and contact points in this area. This will also help users all over Europe to know whom to turn to in

Member States if problems arise and to make ENISA known.

Becoming a centre of expertise

ENISA will not manage to take on all its tasks in the first year, but it will have to develop gradually. In the ICT area the development is quick and I also foresee further tasks for ENISA in the coming years, the objective is that ENISA shall also develop into a centre of expertise for network and information security issues.

As a centre of expertise ENISA will also be able to advice and assist the Commission and Member States in the area of network and information security and it shall provide its own opinions on security related matters, which could e.g. be input to the Commission on how the legislative framework works in practice..

Conclusions

In conclusion, the ENISA's contribution to more secure electronic communications networks and information systems are:

Firstly, by acknowledging that network and information security affects everybody and all stakeholders have a responsibility in using our information and communication systems in a secure manner. I'm very happy about the great willingness to co-operate that has been shown already by Member States and industry and I hope that the trust ENISA will build up can be used to improve the security all over Europe.

Secondly, risk preparedness and compliance with risk management standards will increasingly become an economic factor in the global supply chain. Ensuring business continuity will become an increasing challenge for corporate governance. This is what ENISA will aim at doing by helping Member States and Member State's organizations to support European users and European industry to handle security risks and vulnerabilities.

Finally, I want to stress again that the messages from ENISA shall have to be positive, we are not there to frighten people or to make people stop using the Internet – on the contrary. We want help making the Europeans into advanced and security aware Internet users in order to be able to make full use of the advantages of the information society.

International Cooperation for Critical Infrastructure Protection

US Searching for Deeper and Closer Cooperation in the CIP S&T Domain. New forms of Cooperation Proposed.

Dr. Stan Riveles

Senior Counsellor,
Office of the Science and Technology Adviser to the Secretary,
U.S, Department of State

RivelesSA@state.gov

Growing Awareness of S&T Role in CIP Challenge

The tragic events of 9/11, Bali and the Madrid bombings, have forced many nations to recognize that the protection of critical infrastructures is a new security imperative in safeguarding civil society. While critical infrastructure protection (CIP) remains primarily a domestic responsibility, protecting such infrastructures has an important international dimension.

We all recognize that the threats posed by trans-national terrorism require international action. But the paradox is that traditional diplomacy and military alliances do little to mitigate these threats to infrastructures or respond to attacks on infrastructures, especially when the source of the attack is uncertain.

Accordingly, international activity to protect infrastructures requires new and creative forms of cooperation. It requires new cross-border contacts between experts and managers who have rarely viewed themselves as international representatives. Computer security experts, food safety specialists, infectious disease researchers and first responders—all these specialists face unaccustomed international challenges. They need to be prepared to create international networks to discuss their needs and to share their experiences. They need to share approaches based on their own experiences and best practices. Wherever feasible, they need to form international teams to address specific research problems and come up with solutions that have application beyond the domestic environment. The knowledge and experience gained by fostering such international collaboration can help to prevent attacks and to mitigate their consequences, should they occur. Such cooperation will also help first responders fulfill their more customary roles— by improving domestic capabilities to respond to the traditional challenges posed by natural disasters and other domestic threats.

There is a growing awareness that S&T make essential contributions to meeting the CIP challenge. Scientists and researchers are increasingly being called upon to help industry and governments to better understand infrastructure vulnerabilities and aid in resolving them. Diplomats can play an important facilitating role—using their traditional skills to work together with the S&T community to carve out a new area of constructive international relationships that will help promote secure and safe societies.

Security Challenge

The overarching purposes of U.S. foreign policy are to support the strategic goals of security, stability, and development. These goals have taken on a very different aspect in the aftermath of the tragic events of 9/11. Since 9/11, one of the principal priorities of U.S. S&T policy has been to serve the mission of Homeland Security. In the U.S., the creation of the Department of Homeland Security (DHS) has been the principal institutional response to the new security challenge, and one of the key instruments of the new department

has been to exploit S&T to protect the critical infrastructure. The Science and Technology Directorate, one of four DHS directorates, reflects the important place S&T occupies in the government's strategy.

From the outset, DHS has been keenly aware of the need for international cooperation to strengthen critical infrastructures. 9/11 lent urgency to the problem in the U.S. and heightened the awareness of interdependency across national borders. Indeed, it made us acutely aware of the inadequacy of our border protection and underscored the need to work with other countries. Thus, DHS has deemed international cooperation essential to assessing and resolving security vulnerabilities. We would be remiss if we did not enlist the best scientific thinking and adopt best practices to accomplish these goals. Just as terrorism represents an asymmetrical and non-conventional threat to our security, S&T can be exploited as an asymmetrical "force-multiplying" response to that threat.

Incentives for Cooperation

There are many reasons why international cooperation on CIP serves the mutual interest. The foremost reason is that new types of transnational threats can affect domestic security and safety, and it behooves us to work together. As far as S&T is concerned, there are a number of incentives:

- No nation has a monopoly over the relevant technologies – multiple potential solutions.
- R&D is fully international enterprise
- Technologies relevant to infrastructure protection are largely unclassified.
- Cooperation provides a way to leverage our R&D investment and make resources go further.
- Cooperation brings a larger number of minds to bear on technical problems.

Role of S&T Adviser to Secretary of State

The Department of State—the U.S. foreign office—devotes an entire bureau to foreign policy issues involving Oceans and International Environmental and Scientific Affairs (OES). The Office of the Science and Technology Adviser to the Secretary (STAS), where I work, has a more specialized mandate that includes identifying science and technology (S&T) issues on the "cutting edge" and promoting international S&T cooperation in areas of national importance. Protecting critical infrastructures by mobilizing the best international S&T is such an issue.

The S&T Adviser to the Secretary (STAS) was created in 2000 pursuant to a study by our National Academy of Sciences that recommended strengthening the role of science in foreign policy. In response to this recommendation, the STAS position was written into law by the U.S. Congress. The role of STAS is intended to complement the functions of existing offices, such as those contained in OES, by making best use of S&T to serve broad foreign policy interests. STAS is a small planning and policy unit and has a set of specialized objectives.

- Building S&T capacity and literacy within the Department of State
- Build partnerships with the S&T community, including the international community
- Identifying and communicating "over the horizon" S&T problems to enable policy makers to be proactive
- Providing advice to the Secretary and other policy officials about S&T issues likely to affect foreign policy over the longer term

Current Initiatives

Working closely with DHS and other U.S. agencies, STAS has been involved in several initiatives that are relevant to the topic of S&T for CIP. The first involves Canada, with whom we share a common border. Safeguarding our borders with Canada and Mexico is among the highest international priorities for DHS.

When DHS was formed in mid-2003, STAS was already engaged in an effort to negotiate an agreement with Canada to promote cooperation on S&T for CIP. When first conceived in early 2002, the agreement was to focus on cooperation for the information infrastructure. However, DHS made clear that it desired an agreement of considerably greater scope and depth. The Canadian government agreed. Accordingly, the agreement was adjusted to reflect these new priorities. Signed in June 2004, the agreement is intended to encourage wide-ranging S&T cooperation for the protection of critical infrastructures on both sides of the border, along with the promotion of more effective border security. Science and Technology are defined to include all phases of research and development, including testing and evaluation. The agreement provides for the movement of equipment and materiel across the border for the purposes of cooperation and for the exchange of information, including classified information. The agreement also contains protection for intellectual property (IP) and for equitable sharing, if IP is created in the course of cooperation activities. It represents a government-to-government agreement and is legally binding. It is the first of its kind between the U.S. and another state, and it has become precedential for other such agreements.

Along those lines, a second agreement was recently concluded with the United Kingdom that was coordinated with all USG technical agencies by the OES Office of Science and Technology Cooperation (STC), which aided DHS in negotiation and legal clearance of this agreement. The cooperative activities undertaken pursuant to this agreement build on a long history of cooperation

between the U.S. and UK. By sharing lessons learned and best practices both countries will assemble valuable information on Homeland/Civil Security as well as Critical Information Protection.

The other initiative I would like to mention involves a bilateral framework for greater cooperation with Japan and has a very different character. Known as the "U.S.-Japan Workshop for S&T for a Secure and Safe Society", this series of conferences and meetings began in early 2004 in Japan with a one-day meeting of science policy makers from a number of different government agencies on both sides. The agenda covered areas of interest for both countries, such as infectious diseases, food safety, counter crime, and counterterrorism, inter alia. The U.S. team was led by Dr. Atkinson, the S&T Adviser to the Secretary of State; the Japanese side was headed by a representative of MEXT, the Ministry of Education, Culture, Sport, Science, & Technology. The purpose of this first meeting was to increase understanding about national S&T priorities in the areas of interest and to plan a series of technical exchanges among experts. Several follow-on meeting have been held in the U.S. since then. We have arranged bilateral expert workshops in cyber-security and interdependency analysis. Further experts meetings are in the works on the topics of food safety and chemical and biological agent detection.

Features of a Cooperative Agenda

There is considerably more opportunity for international cooperation than is currently underway. Indeed, the relative lack of cooperation in the transatlantic context is particularly glaring. With the exception of the DHS-UK S&T Agreement for Home land/Civil Security and Critical Infrastructure Protection, no agreements exist with European states to address this issue. This is all the more surprising when one notes how much domestic effort is being made to protect infrastructures in the European states. One of the ways in which we can advance the goal of international cooperation is by working through government to facilitate contacts. U.S. agencies are very interested in such cooperation. Many agencies have their own international outreach efforts. But there is an appetite and interest for more.

The State Department can help in the following ways:

- By identifying U.S. representatives responsible for CIP R&D
- By promoting opportunities for international discussion of respective research agendas and priorities
- If necessary, by developing legal arrangements for cooperative research and development.

In our view, the elements of a cooperative agenda extend beyond promoting bilateral contacts. The U.S. is particularly interested in exploring ways in which we can develop a joint U.S.–EU research agenda and forum.

In the past, differences in outlook and structure have been hard to overcome. However, this situation may be changing. The "Group of Personalities" Report on "Research for a Secure Europe" recognized that "New threats have emerged that ignore state border and target European interests outside and within EU territory. … These threats call for European responses and a comprehensive security approach that addresses internal as well as external security and can combine civil and military elements." In its September 2004 decision creating the European Security Research Agenda, the Commission stated that, "To address the growing and diversifying security challenge, Europe needs to harness the combined and relatively untapped strengths of relevant industry and coordinate the research community in order effectively and innovatively to address existing and future security challenges. . . ". These decisions appear to represent a new direction for research and certainly suggest a convergence of views across the Atlantic Community.

We should not expect immediate results, but we can persistently and patiently seek to expand our joint efforts to serve the common goal of creating secure and safe societies.

Germans effort in C(I)IP and its actual state

Germany was early recognising the value of Critical Information Protection. Public Private Partnerships, bi- and multilateral agreements do support other efforts to enhance protection level of the critical infrastructure.

Marit Blattner

Responsible for Critical Infrastructure
Federal Office for Information Security Germany
(Bundesamt für Sicherheit in der Informationstechnik) BSI, Deutschland
E-mail: marit.blattner@bsi.bund.de

In Germany CIIP was an important goal of politics and economy long before 9/11. In fact, 1991 the Federal Office for Information Security (BSI) initiated and started underlining the importance of IT-Security for all ICT and its federal planning. With the growing use of ICT in the mid nineties a joint effort of all German ministries was in 1997 taken to analyze CIP's IT dependence. Since the CIIP measures are supported form various ministries by studies, web-sites and expert knowledge.

An initiative of the minister of interior affairs targeted the analysis of CI(I)P in Germany first with the focus on singular ministries, later considering as a national effort. Therefore 1998 an inter-ministerial working group "AG KRITIS" was started and later on the department "Critical Infrastructure Protection" was established within BSI.

Germany is aware, that the challenge of CIIP cannot be solved by exclusively one group. Therefore the cooperativeness is growing step by step including the start of Public Private Partnership PPP.

Working group as AKSIS and BITKOM in economy started to raise awareness in CIIP as well as CIP. Agreements between government agencies and enterprises concerning CIIP as well as bilateral agreements with other nations on all levels address the improvement of Critical Information Infrastructure Protection Situation.

German federal government responded to 9/11 with an Anti-Terror-Program. This program considers CIP as an essential part in counter terror action. BSI got additional positions and did start two centers with this Anti-Terror-Program:

- Penetration Center
- Government CERT

On top of that BSI started infrastructure analysis CIP studies within this Anti-Terror-Program, which are today still a fundamental for CIP tasks also within Federal Crime Agency (Bundeskriminalamt) and the newly Federal Agency for Civil Protection and Emergency Aid (Bundesamt für Bevölkerungsschutz und Katastrophenhilfe).

To improve the protection of German's critical infrastructure, during 2004 a national plan for CIP was developed. Furthermore cooperation on bi- and multilateral level was fostered and the cooperation with the private sector was intensified.

For 2005 the development of a situation analysis center is planned. Its purpose will be to recognize the actual threat level and to be able to react on incidents in the best possible way.

A Cybernetic Approach for Critical Infrastructure Protection

Our world has become more dynamic, more complex, more dependent and more vulnerable. Failures, accidents, physical or cyber attacks can provoke major damages which can proliferate by cascading effects. Novel approaches are needed to analyze and assess critical infrastructure protection.

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 Infrastructure Threats and Assurance) and CI²RCO (Critical Information Infrastructure Research Co-ordination) projects. This article is based on a presentation given at the 1st Annual CZAEE conference "Vulnerabilities and Protection" in Prague, November 21 – 22, 2004.
Phone: +49 (0)89 / 6088-3331
EMail: schmitz@iabg.de
Internet : http://www.iabg.de

Our societies are fully dependent on large complex critical infrastructures (LCCIs). LCCIs are large scale distributed systems that are highly interdependent mainly via Information and communication Technology (ICT). Failures, accidents, physical or cyber attacks can provoke major damages which can impair vital functions of economy, governmental services and society.

Risks and Prevention

Daily news reports of many risks, natural catastrophes, technical disasters, international crime and terrorism. Risks imply the possibility of considerable damage, but they are also characterized by a great uncertainty. Scenarios have to be considered to study also "unthinkable" events and their primary and follow-on effects. Because of the ICT interdependency of critical infrastructures it is irrelevant where primary effects happen, the secondary effects spread over the whole globe like cascades. Although infrastructures have a considerable criticality due to this ICT penetration, their interdependencies are hardly known and are only insufficiently investigated. Risk prevention is indispensable, but demands extensive information about installations, processes, actors etc. and can restrict the informational freedom of many citizens. The challenge is to protect infrastructures especially by technical measures and at the same time to establish a legal framework that facilitates the development and use of such technical solutions.

ICT-related inter-dependencies of infrastructures are hardly known and only insufficiently investigated.

Complex System

To this purpose critical infrastructures have to be considered as a complex cybernetic system. 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. Intervention into the network changes the relationships between the parts and consequently the character of the system. Ecological systems for example are open systems and remain viable through permanent exchange with their environment. Such an exchange causes characteristics like feedbacks and self-regulation that are not contained in the individual components of the system. Therefore the survivability of a complex system can not be derived alone from the survivability of its components. Survivability depends primarily on the fact that the organization of the network follows cybernetic principles.

Prevalent Shortcomings

In dealing with complex systems we make often strategic mistakes such as for example:

- Incorrect Definition of objectives
- Inadequate modelling.

Sub-optimization and selection of inappropriate objective functions are

often observed in dealing with complex systems. Instead to focus on survivability of the whole system, planners often follow repair service strategies or select shareholder value as objective function. The consequence is that sustainability, stability and robustness of the system are not furthered. In the long run sub-optimization of individual system components leads to inefficiency and also often to irreversible erroneous trends.

Aggregation Level

The aggregation levels of system components are often not adequate to the problem. Too many details lead to an information overload. Large quantities of data are collected, that however fail to reveal the system structure. Important relationships and interactions will be overlooked. The bulk of data cannot be evaluated expediently. Systemic analysis means first of all to recognize the interactions of details on a suitable aggregation level.

Without knowledge of the network with interdependencies between the components the performance of the system cannot be assessed even if the individual components are studied in detail. The role of the components in the network remains unknown. Symptoms instead problems are addressed.

Fault Tolerance

Caught up in the web of linear, causal patterns of thinking, people intend to adjust all planning factors as exactly as possible without providing for buffers as if it were a closed system that does not need to worry about disturbances from outside. The better way is to consider fault tolerance mechanisms.

Interrelationships or disturbances of a complex system can reveal surprising effects which are seldom manifested by a direct cause-and-effect relationship between neighbouring elements. This is one of the main headaches in planning and understanding the system, because the effects are so complex, that extrapolation to estimate the results will fail. Instead of simple extrapolation hidden feedback loops and self-regulation mechanisms have to be identified to exploit fault tolerance.

Modelling Principles

We have to think in networks in order to recognize the cybernetic rules of a complex system. We have to learn that a complex system is like an organism and that cause-and-effect chains can not be recovered directly. Survivable systems contain control loops that enable the system to absorb disturbances without external interventions. Thereby the system becomes fault tolerant and robust with regard to disturbances. Faults may happen, but the system does not collapse. The lack of knowledge concerning indirect effects with their time delays leads to the fact that we normally realize the impact of interventions or disturbances too late. Policy-tests have to be carried out. The results of these policy-tests deliver important hints for the solution development. The forecast will refer less to the fact which events when occur, but to the fact how the system behaves and how it reacts to certain events. That means we need a capability to simulate the behaviour and response time of the system.

A simulation capability is needed to investigate the system behaviour in a synthetic environment.

A CIP Process Model

The challenge is to avoid shortcomings discussed above and to find answers on questions like

- How does the system react to certain events?
- How robust and flexible is it?
- How can its behaviour be improved?
- What are suitable leverages for control?
- What cybernetic rules as for example self-regulation or fault tolerance can be exploited?
- What are the critical and uncritical areas of the system?

The knowledge of the individual parts of a system is not enough to answer these questions. First of all we need knowledge of the cross-linking of the parts and a practicable process model that will help to understand critical infrastructures as a cybernetic system and to derive decision support instruments suitable for improving their survivability.

Step 1: Objectives and modelling

The correct description of the problem situation is decisive for a successful problem solution.

Otherwise wrong objectives will be taken and/or only parts of the system will be considered. Context, relationships and interactions between the elements have to be conceived and understood. It is also important to recognize the true objectives which should guide us to the problem solution.

Critical infrastructure description covers at least four hierarchy levels representing different levels of critical infrastructure relevant decision making with different objective functions:

Level 1 represents the “System of Systems” level. This is the level of the economy as a whole, the international community and the organizations like EU and the national governments. Responsible actors are EU, national governments, and trade associations. Objective function is the survivability of the complex system of critical infrastructures.

Level 2 represents the level of individual critical infrastructures. This is the level of the economy and the stakeholders of the individual infrastructures. Objective function is to minimize the risks of an individual critical infrastructure.

Level 3 is the level of systems. Systems are represented by elements belonging to an individual critical infrastructure, single enterprises or a group of co-operating and competing enterprises. Actors are the stakeholders of the individual infrastructure systems, management of enterprises and trade association. Objective function may be to improve the shareholder value.

Level 4 is the level of technical components. At this level technical

simulation algorithms, vulnerability analysis, sustainability and maintainability calculations and experimentation may be applied. Actors are the management and technical experts responsible for security tasks. Objective function is to maximize the technical functionality.

The decision process on each hierarchy level can be supported by decision support tools such as socio-economic models, scenario techniques, gaming, systems dynamics, empirical modelling, cost-effectiveness analysis, simulation, optimization algorithms, risk analysis methodology, human behaviour models, cost-effectiveness models and others.

Step 2: Analysis of Causality

Tools are needed to investigate interrelationships, influences, time periods and changes in order to get a comprehensive understanding of the problem. Networks allow us to describe the causality of the relationships and to analyze their characteristics. The network tools should be able to classify all elements in drivers, driven, critical and buffered elements where

- Elements, which influence strongly elements in the network without being influenced strongly by others, are called “active” or “driver”.
- Elements, which influence faintly others and are influenced strongly by others, are called “reactive” or “passive” or “driven element”.
- Elements, which influence and react strongly, are called “critical”.
- Elements, which neither influence nor react strongly, are called “buffering”.

Critical elements are particularly susceptible for cascading effects and have to be analyzed first of all.

Step 3: Scenario Development

Of course, the future can not be predicted exactly in complex problem situations. A complex system will behave according to its own directive. But we can devise possible scenarios for specific parts of the network and simulate the consequences. Scenario development requires the following work steps:

- Determination of the necessary timeframe
- Identification of the influencing factors within the network
- Selection of the relevant scenario areas
- Development of the basic scenario
- Development of alternative scenarios
- Interpretation of the scenarios.

Step 4: Impact Analysis

In this step control possibilities should be identified. In doing so, we have to distinguish between controllable elements, non-controllable elements and indicators. Controllable elements are to be considered for steering tasks as well as disturbances. Non-controllable elements are to be monitored with respect to preventive actions. Indicators notice the degree of success of a steering measure or the degree of impairment caused by disturbances. Our main task is to improve the survivability of the system of critical infrastructures. So, the question comes up which elements influence the survivability of the whole system. For this purpose it is to determine who should be the controller. According to his competencies he can steer certain elements or not. That means first of all we have to determine the level of the steering activities. Then we can determine the aggregation level and the resolution level of the network. The analysis of the tractability includes also the consideration of reinforcing loops and feedbacks, the time conditions and intensities.

Solutions should adapt to changed situations.

Step 5: Strategies

Planning of strategies and steering measures for survivability improvement is a creative and challenging process. Viable strategies have to consider very carefully aggregation level and system characteristics like reinforcing loops, feedbacks and control cycles, which can be used to control and stabilize the system in case of disturbances. May be that additional elements of technical solution strategies like redundancy, diversification[3], decentralization[4], degradation,[5] decoupled arrangement[6], and / or reduction of complexity have to be introduced into the system.

Step 6: Realizing of Problem Solutions

Problem solutions should be realized in such a kind that they endure also in adverse circumstances and that they are able to adapt to changed situations. Therefore the necessary ability to repair as well as the ability to develop must be integrated into the problem solution. Thereto it is necessary to control progress and to accomplish respective corrections. Premises are to review periodically and to redefine if deviations compared to the start premises have been found. It is important to define early warning signals that indicate deviations and changes as early as possible.

Recommendations

When developing decision support tools for CIP planning, one should therefore look for an approach that cannot only simulate the pattern of interactions but also allows the user to interpret and evaluate the cybernetics thereof. The purpose of such a model is to recognise the stability of the structure, the ability to adapt, the onset of irreversible trends, the risks of dissolution and the actuating elements that allow the planner to steer the system in the desired direction. Modelling and Simulation (M&S) helps to recognize how susceptible his system is and where the risks lie.

[3] Usage of diverse methods, materials and components
[4] distribution of the damage potential
[5] outage in direction of a less bad status
[6] with respect to time and space

Success and risk factors for multi-national CIIP co-operation

Participants from over 20 countries identified success and risk factors for multi-national approaches to critical (information) infrastructure protection during the Swiss-German EAPC/PfP workshop.

Eric Luiijf M.Sc.

Eric Luiijf graduated in 1975 at the Technical University of Delft. Eric is Principal Consultant Information Operation and Critical Infrastructure Protection at TNO Physics Laboratory, 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

During the Swiss-German organised EAPC/PfP/NATO Workshop on Cyber Security and Contingency Planning, held from 25 to 27 September 2003 in Zurich, Switzerland, three working groups were formed. One of the working groups with delegates of over twenty EAPC, PfP, and NATO countries undertook the task to discuss issues related to critical information infrastructure protection (CIIP) and civil emergency planning (CEP). Below, you find some results.

What makes it critical?

The participants agreed that systems and services that play a crucial role in society, economy, politics and ecology form the critical infrastructure or CI for short. It was understood that these –both technical and non-technical– systems/services may have a supra-regional impact when damaged or disrupted. Political and social cohesion and lives of people may be endangered. Loss of confidence in government may hamper international relations, and citizens and enterprises may be impacted by psychological effects when critical infrastructure is deliberately destroyed.

Collaboration on CIIP contributes to peace-building and economic development.

The CI includes systems/services for international co-ordination, services that are only critical when other systems or services are disrupted or lost, and critical infrastructures that support other infrastructures. Furthermore, the more dependencies, the more critical a CI is. It is obvious, however, that scale of the CI usage, the (un)availability of alternate modalities and the type of society determine the criticality of the CI.

Not all countries regard the same sectors as being critical. These differences can be attributed to geographical structure, and societal differences. Energy, health, transport, and government services are recognised as a CI by most countries. Telecommunications and ICT are next.

Threat Spectrum

The threat spectrum comprises natural disasters, design flaws, and human errors. Some countries reported that their current threat spectrum includes deliberate attacks by organised crime, terrorism and state confrontations.

Co-operation

After establishing this understanding of CI's on the first day, the second day workshop investigated what are success and risk factors for multi-national co-operation in protecting the critical information infrastructure.

The participants stated that there are a number of reasons to collaborate: (1) a better, speedier reaction capability, (2) mutual support in case of emergencies, (3) better use of scarce knowledge and resources, (4) supports peace-building and economic development.

Collaboration can have different forms: agreements, sharing of information, common exercises and the creation of standards, procedures and means.

Attention should be paid to: (1) shaping good conditions for co-operation, (2) the complexity of differences in language, culture, history, and so on, (3) mutual agreement between the States, and (4) the co-operation level(s): strategic, tactical, operational, and technical.

Risk Factors

Risk factors that need to be taken into account when countries want to co-operate on CIIP were identified. They include: (1) political trust is required (a lot of political changes lead to less trust), (2) national legal restrictions e.g. data protection acts, and classified info, (3) economic disadvantage or national interest, and (4) the dependency on co-operation and information exchange introduces a different type of vulnerability.

Countries have a different pace with respect to CIIP. Change of approach shall be voluntary and can neither be controlled, nor speed up by other countries. Pro-factors for co-operation and mutual trust shall build the case for collaboration.

Mutual political trust is required and one's own CIIP process pace is leading.

Small knowledge base

The participants recognised that the current awareness and understanding on the CIIP issues, including those affecting the effectiveness of Civil Emergency Planning, still has a small base. For that reason, the representation by a country to international CIIP workshops and meetings shall preferably stay the same. This helps countries to maintain their position at the learning curve and to understand the relevance of new developments to their country.

Benefits of Co-operation

The representatives quickly agreed upon the factors that are beneficial to the international community when countries decide to collaborate on CIIP. Just collaborating may already scare-off potential attackers and may be as deterrence. Information exchange on vulnerabilities, (imminent) threats and solutions may at the same time lead to better protection and less damage with economic and societal impact. And, last but not least, international standards describing best CIIP practices, methods and means will internationally raise the level of protection in a way that is understood by international partners, both from government and private industry.

Involve Private Industry

Regarding private industry, it was recognised that no representatives of the private sector and multi-national companies were invited to the workshop. Most of the critical infrastructure services are nowadays run by private industry, thus international collaboration with them is required. A harmonised international CIIP approach is beneficial for multi-nationals. They will not be confronted with n-different approaches, regulations and laws, which create an ineffective use of resources and – at the end – a high risk.

Mutual political trust is required and one's own CIIP process pace is leading.

Means and Tools

Several suggestions for international support were mentioned when discussing which means and/or tools could be of help to the EAPC/ PfP/ NATO countries, which have not yet developed a CIIP policy.

At first, education is required. Clear objectives, a timeframe, the frequency and duration of courses, and the target level of people shall be narrowed down.

Raising international awareness at all levels is required. The approach shall define objective, the target audience and the specific content and message(s) to be conveyed to the audience.

Sharing information & means

In support of trust-building, information exchange and fast-track development of best practices, the workshop participants recommended that information shall be shared by collaborating countries at various levels of trust, content and classification.
Furthermore, a phone book in order to reach authorities responsible for CIIP in other countries shall be created. In the end, a CIIP agency – may be incorporated in ENISA – may be required.

CIIP touches national sensitive areas. Nevertheless, it was felt that mutual international neighbour support of CIIP „fire brigades" to fight attacks and outages is beneficial to both countries. It, however, requires interoperability at multiple levels. Common exercises, like demonstrated in the CAN-US Blue Cascades exercise, may reveal one's weak points to be addressed. Sharing experts and experience addresses another level of collaboration.

The development of (inter)national CIIP-standards, an international agreed definition of what CIIP is, and book(s) and this newsletter (!) about basics of CIIP in support of awareness and understanding are building blocks high on the wish list of the representatives.

Conclusion

Within only a couple of hours, the representatives of over twenty EAPC/ PfP/NATO countries identified an extensive set of success and risk factors for CIIP co-operation. Co-operation with other countries has so many advantages, that risk factors can be overcome when governments decide to protect their critical infrastructure.

Information Security Enables Citizen Centred e-Government

During this worldwide economic turndown, as governments cut services in an effort to cut costs, a new model for e-government CIIP was presented at the World Summit for the Information Society (WSIS). This new model will allow the delivery of new e-government services utilizing existing infrastructures. E-Government can restore services to the citizens and even decrease socio-economic gaps.

Eyal Adar

Eyal Adar is one of the leading experts in the area of CIIP and Information Security. He is the founder and the CEO of iTcon Ltd., a consulting firm specializing in Enterprise Security Architecture for the financial, industrial and government sectors. He is a senior security strategist working on the Israeli e-Government project and has served as member of the European Commission's ACIP (Assessment of Critical Infrastructure Protection) consortium. This article is based on a presentation given by Eyal, at the EU-WSIS (World Summit for the Information Society) convention in Geneva, 2004.

Eyal Adar
Tel: +972 3 6490039
E-mail: eyal@itcon-ltd.com

In the near future, the Israeli government is planning to launch a project that will offer a wide range of e-Government services. The goal of the project is to simplify citizens' access to various government services. This will be achieved by utilizing electronic interfaces to eliminate the citizens' face to face interaction with government clerks in over-crowed government offices. Some of the intended services include:

- Ministry of Finance: Taxes e-payments, V.A.T, Licenses, Publications
- Ministry of Labour: Social services
- Ministry of Transportation: Driving license, Car license
- Ministry of Justice: Court Fines, Court files.

Needs and challenges

In order to create a revolution in G2G, G2C and G2B services, the e-Government Systems must be opened to the Public, despite the fact that this creates Security risks. In addition, the Israeli Government, like many others, is currently down-sizing and can't afford to build new infrastructures for all the new proposed services. Existing systems must be used in order to make these changes a cost effective alternative. Opening existing systems to the public in order to enable access for citizens for these e-services, creates additional risk factors and security challenges that never existed before.

The challenge was to find a way to open Government IT systems to external Stakeholders, and at the same time, protect the information from misuse. Protecting the citizen is one of the critical elements that must be incorporated into the new systems.

E-Government services threats

Intentionally allowing access to the government's computing infrastructure imposes unique risk factors. Many are the entities that would be interested in attacking the infrastructures; from bored high school students and grunted employees, to hackers or even hostile organizations.

If the IT security isn't designed correctly, and the integrity of these systems is breached, the e-Government services could be abused for malicious activities such as: deleting a tax debt, forging driving licenses, deleting court records, denying a public service, etc.

Government current security status

To observe clearly the risk involved in allowing access to the government's computing infrastructure, consider the following

facts: The Israeli e-Government Web site is faced with a daily dose of 1000 viruses, 400 serious hacking attempts, and thousands of site mappings. These attack attempts are stopped daily by the e-Government security systems. The attackers' goals may be website defacement, information sabotage and manipulation, identity theft by forging governmental identity cards, fraud or denial of government services. Currently, these malicious activities are performed on Government websites which offer limited access to information. This leads to believe that allowing direct access to government systems through websites will increase an attacker's temptations to infiltrate these sites.

Viewing the issue from a centralized, governmental perspective can save money.

Our vision

Considering the importance of e-Government information services, the need for improved integration, collaboration and protection seems obvious. E-Government services should be centralized to improve the overall integration of information and services provided. Additionally, collaboration between the government and the private sector is essential. In order to achieve a high level of protection, this collaboration should include representatives from various vendors, IT architects, and other Critical Infrastructures such as, financial service providers, telecom sector representatives etc.

This initiative will start in one focused, well-defined project and will eventually be implemented throughout the entire system. A uniform security infrastructure will be created in order to meet the security challenges while remaining a cost effective solution. This is crucial since by design, the security infrastructure will integrate with existing and future services. This infrastructure will increase the level of security and privacy, in compliance with the afforded information in the system, and will improve the overall security expertise within the government. It will also achieve a higher level of accountability for government e-services.

New e-government security Model

In order to meet the challenge of opening the e-government infrastructure to the public and protecting it, a unique security model was designed for the Israeli government.

Our vision is to create a new, global model for e-government.

The initiative was created by Mr. Yitshak Cohen, who is the Chairman of the National Computerization Committee and Senior Deputy of General Account, and has been managed by Mr. Boaz Dolev, the Head of the Israeli e-Government Department.

The model has been created and is now in the first phase of its implementation within several pilot projects. The model addresses three areas:

- Security architecture
- Security organization
- Security management

The uniqueness of the model, and ultimately its success, lays in its ability to provide centralized protection for all e-Government services. It also provides for the design of future services with security needs in mind, and presumes that centralized security and forethought reduce overall costs.

Security architecture

The security architecture guidelines of the model address many issues.

The centralization and management of security services, is key to the project, as well as the need to integrate the new system with existing infrastructure and projects.

The multi-layered approach (business, processes, applications, IT infrastructure) is also essential to maximizing the potential of the project, as is the concept of 'Defence in-Depth' (e.g. multiple defence rings, system tiers, etc.), and the use of diverse technology.

The project guidelines also encompass certain philosophies of protection such as: 'Operate through Attack', 'System Security on top of site Security', and an advanced Trust Model. The project's guidelines also address the protection of access channels and the legal and privacy aspects of the project.

Security organization

The proper organization of security entails a number of activities. Creating a secured organizational structure is first among them. Equally important is the creation of e-Government security policies for the following new services:

- Internal Government policies and procedures.
- Industry standards such as: ISO17799, ISO/IEC 15408, Survivability.

Adapting existing projects to these new policies will also be essential to the organization of security. In

addition, periodic compliance verification must be performed within the new system.

Security management

Managing security requires the following services/teams:

- Global Identity Management (IDM).
- Security Operation Centres (SOC).
- CIRT (Central Incident Response Team).
- Early warning mechanisms.
- Real time response.
- Managed security solutions (antivirus, network security, etc.).

Once the system is functioning, these teams can manage the security and maintain the integrity of the system.

Brave new world

The Information Age has altered the world we live in. In order to maximize the benefits of the technology around us we need creative, innovative approaches to security. The convenience and accessibility of e-Government services deployment, cannot come at the expense of information security.

Therefore, this comprehensive, innovative system of IT protection is the key to enabling governments to offer such services.

Relevant links:

- WSIS web site: http://www.itu.int/wsis/
- Israeli Ministry of Foreign Affairs, WSIS site, where the e-government security presentation is available (See: Presentations/iTcon): http://wsis.mfa.gov.il/
- ACIP web site: http://www.eu-acip.de
- ITcon web site: http://www.itcon-ltd.com

The International Critical Information Infrastructure Protection (CIIP) Handbook 2004

An Inventory and Analysis of Protection Policies in Fourteen Countries

Myriam Dunn and Isabelle Wigert

Center for Security Studies, ETH Zurich (Swiss Federal Institute of Technology)
dunn@sipo.gess.ethz.ch
wigert@sipo.gess.ethz.ch

Critical (Information) Infrastructure Protection

Critical infrastructure protection (CIP) is perceived as a key part of national security in numerous countries today and has become the nucleus of the US terrorism and homeland security debate after 9/11. A *critical infrastructure* (CI) is commonly understood to be a system or an asset whose incapacitation or destruction would have a debilitating impact on the national security and the economic and social welfare of a nation.

Protection concepts for strategically important infrastructures and objects have been part of national defense planning for decades, though at varying levels of importance. Towards the end of the Cold War, and for a couple of years thereafter, the possibility of infrastructure discontinuity caused by attacks or other disruptions played a relatively minor role in the security debate only to gain new impetus around the mid-1990s, when a new, delicate problem became apparent: the dependency of modern industrialized societies on a wide variety of national and international information infrastructures.

CIIP is a key issue of national security in numerous countries

First steps in the protection of critical information infrastructures

The US was the first nation to broadly address the new vulnerability of the vital infrastructures. New risks in designated "sectors" like information and communications, banking and finance, energy, physical distribution, and vital human services were identified by the *Presidential Commission on Critical Infrastructure Protection* (PCCIP). The PCCIP concluded in 1997 that the security, economy, way of life, and perhaps even the survival of the industrialized world are now dependent on the interrelated trio of electrical energy, communications, and computers. The commission found that advanced societies rely heavily upon critical infrastructures, which are susceptible to classical physical disruptions and new virtual threats.

Vulnerabilities in these infrastructures are believed to be on the rise due to increasingly complex interdependencies. As most of the critical infrastructures are either built upon, or monitored and controlled by vulnerable ICT systems, the "cyber-" infrastructure has become the new focal point of protection policies (*critical information infrastructure protection*, CIIP).

Following the PCCIP's publication, US President Bill Clinton started initiatives

to increase the protection of critical infrastructures in the US, on the premise that a joint effort by government, society, organizations, and critical industries was needed to defend these vital assets. The issue of CIIP has remained a high priority on the political agenda ever since. The events of 9/11 merely served to further increase the awareness of vulnerabilities and the sense of urgency in protecting critical infrastructures.

In addition, there are several "drivers" that are likely to aggravate the problem of CIIP in the future: these are the interlinked aspects of market forces, technological evolution, and emerging risks. On the one hand, we are facing an ongoing dynamic globalization of information services, which in connection with technological innovation (e.g., localized wireless communication) will result in a dramatic increase of connectivity and lead to ill-understood behaviour of systems, as well as barely understood vulnerabilities.

The CIIP Handbook

Within the last few years, and following the example of the US, many countries have taken steps of their own to better understand the vulnerabilities of and threats to their CII, and have proposed measures for the protection of these assets.

To give an overview of these protection efforts, the *International CIIP Handbook* was first published in 2002 and substantially expanded for the 2004 edition. The Handbook was written by Myriam Dunn and Isabelle Wigert, researchers at the Centre for Security Studies at the ETH Zurich and meticulously reviewed by international experts in the field.

The 2004 edition compiles and analyzes governmental efforts to protect CII in fourteen countries (Australia, Austria, Canada, Finland, France, Germany, Italy, The Netherlands, New Zealand, Norway, Sweden, Switzerland, the United Kingdom and the United States) as well as important International Organizations. The Handbook has two focal points: 1) national policy approaches to CIIP and 2) methods and models used to assess various aspects of the CII.

However, what we are looking at are mere snapshot moments of a very dynamic policy field. As the information revolution is an ongoing and dynamic process that is fundamentally changing the fabric of security and society, continuing efforts to understand these changes are necessary. This requires a lot of research into information-age security issues, the identification of new vulnerabilities, and new ways for countering threats efficiently and effectively. The International CIIP Handbook is a small contribution towards this ambitious goal. In order to stay abreast of the dynamics in the field, more updates of the CIIP Handbook are necessary.

The 2006 edition of the CIIP Handbook (planned publication date: February 2006) is again going to be considerably expanded. Moreover, the *CIIP Handbook 2006* will consist of two volumes: The first volume will focus on country surveys (the existing surveys will be updated and eight new country surveys will be added), the second will be an edited volume, in which various experts address key issues, challenges, and prospects of CIIP.

The Handbook's target group consists mainly of security policy analysts, researchers, and practitioners. It can be used either as a reference work for a quick overview of the state of the art in CIIP policy formulation and CIIP methods and models, or as a starting point for further, in-depth research.

Dunn, Myriam and Isabelle Wigert (2004), *the International CIIP Handbook 2004: An Inventory of Protection Policies in Fourteen Countries* (Zurich: Centre for Security Studies).

(See www.isn.ethz.ch/crn for an online version of the 2004 Handbook).

Selected Links and Events

Actual Upcoming CIIP Conferences in Europe

- The first CRIS International Workshop on Critical Information Infrastructures (CIIW'05), 17-18 May 2005, Linköping, Sweden: http://www.ida.liu.se/conferences/CIIW05/
  The Workshop follows a successful session on Information Infrastructures at the second annual CRIS conference in Grenoble (October 2004) and the Information Infrastructures Survivability Workshop in Lisbon (December 2004). Further, it aims at identifying and discussing the challenges for EUR R&D on cyber blackouts, building also on the findings and outcomes of the Workshop titled "The future of ICT for Power Systems: emerging security challenges" recently organised by the European Commission (February 2005).
- 8th International Workshop on Electric Power Control Centers June 5-8, Les Diablerets, Switzerland: http://epcc8.epfl.ch/
  In relation with the D4 work on interdependencies we signal the 8th International Workshop on Electric Power Control Centers. The workshop will focus on Experiences and Trends in Generation, Transmission and Distribution Control Centers.
- 2nd Conference on Detection of Intrusions and Malware & Vulnerability Assessment, July 7&8 2005, Vienna: http://www.dimva.org/dimva2005/
- 15th Power System Computation Conferences (PSCC), August 22, Liège, Belgium: http://www.pscc2005.org
  In relation with the D4 work on interdipendencies we signal the 15th Power System Computation Conferences (PSCC). The purpose of the conference is to facilitate the interchange of information among scientific and engineering communities concerning the problems and their solutions related to the planning and operation of electrical power systems.
- First International Conference on Security and Privacy for Emerging Areas in Communication Networks, IEEE communication Society, Septemeber 5-9, 2005 in Athens, Greece: http://www.securecomm.org
- CIIP Conference German Informatics, September 19, 2005 in Bonn: http://www.informatik2005.de/143.html and click on CIS: Symposium 19. September 2005
- Applied Security Congress and Exhibition September 21&22, Zurich: www.security-zone.info
- First international CIIP Conference IEEE in Europe of the Taskforce Information Assurance, November 3&4 2005, Darmstadt: http://www.iwcip.org/2005/

Conference Papers

- The Future of ICT for Power Systems: Emerging Security Challenges Rami Workshop Feb 2005, Draft Report https://rami.jrc.it/workshop_05/Report-ICT-for-Power-Systems.pdf
- International Workshop on R&D Strategy for Sustaining an Information Society: http://www.eecs.berkeley.edu/CIP/US-EU/agenda.html
- Critical Infrastructure Protection - Status and Perspectives: http://www.gi-fb-sicherheit.de/vg/informatik2003/sessions/cip-workshop/session-s-17.html

CIP and CIIP Documentation

- Partnership for Critical Infrastructure Security: http://www.pcis.org/
- The Institute for Information Infrastructure Protection: http://www.thei3p.org/
- The Information Warfare Site: http://www.iwar.org.uk/
- Information Assurance Advisory Council: http://www.iaac.org.uk/

European CIP activities

- European Security Taskforce: http://www.securitytaskforce.org/
- Dependability Development Support Initiative: http://www.ddsi.org/
- Analysis & Assessment for Critical Infrastructure Protection: http://www.iabg.de/acip/index.html
- Arbeitskreis Schutz von Infrastrukturen: http://www.aksis.de/
- Swiss Federal Strategy Unit for Information Technology: http://www.isb.admin.ch/
- InfoSurance Foundation: http://www.infosurance.ch/
- Comprehensive Risk Analysis and Management Network: http://www.isn.ethz.ch/crn/
- BSI Kritische Infrastrukturen (Kritis): http://www.bsi.bund.de/fachthem/kritis/index.htm
- Directorate for Civil Protection and Emergency Planning: http://www.dsb.no/
- Stabstelle IKT-Strategie des Bundes: http://www.cio.gv.at/
- The International Institute for Critical Infrastructures: http://www.cris-inst.com/
- Swedish Emergency Management Agency: http://www.krisberedskapsmyndigheten.se/
- National Infrastructure Security Co-ordination Centre: http://www.niscc.gov.uk/
- UK Resilience: http://ukresilience.info
- Information Society Technologies: http://www.cordis.lu/ist/
- Safeguard: http://www.cordis.lu/ist/cpt/dependability.htm

CIP Approaches outside EU

- Public Safety and Emergency Preparedness Canada: http://www.ocipep.gc.ca/
- Australian Government – Information Management Office: www.noie.gov.au/
- Australian Government – National Security: http://www.nationalsecurity.gov.au/
- PreDICT (Australia): www.defence.gov.au/predict/
- Trusted Information Sharing Network for Critical Infrastructure Protection (Australia): http://www.cript.gov.au/
- Centre for Critical Infrastructure Protection (New Zealand): http://www.ccip.govt.nz/
- National information infrastructure protection (New Zealand): http://www.e-government.govt.nz/niip/index.asp

Conference on Detection of Intrusions and Malware & Vulnerability Assessment

DIMVA 2005

www.dimva.org/dimva2005

July 7-8, 2005 Vienna, Austria

Conference of SIG SIDAR
of the German Informatics Society (GI).

In cooperation with the IEEE Task Force on Information Assurance
and the IEEE Computer Society Technical Committee on Security and Privacy.

DIMVA 2004
Report

2005 DIMVA 2005
July 7-8 in Vienna.

www.dimva.org/dimva2005

Call for Papers / Call for Participation
First IEEE International
Workshop on Critical Infrastructure Protection
November 3-4, 2005 – Darmstadt, Germany

The IEEE Task Force on Information Assurance is sponsoring an interdisciplinary workshop on research, policy, and experience in the field of critical infrastructure protection and critical information infrastructure protection in cooperation with the special interest group on critical infrastructure protection (FG KRITIS) of the German Gesellschaft für Informatik (GI).
The workshop seeks submissions from academia, government, and industry presenting novel research, policy, and applications and experience in the field of critical infrastructure protection.

For a list of areas of particular interest for submissions and submission guidance, please refer to

http://www.iwcip.org/2005

Important dates:

Full paper submissions due:	June 17, 2005
Notification of acceptance:	July 15, 2005
Final papers due:	August 5, 2005
Workshop:	November 3-4, 2005

Accepted papers will be published by IEEE Press.

Program Committee

Eyal Adar (IT-Con, Israel)
Jack Cole (US Army Research Laboratory, USA)
Geert Deconinck (K.U. Leuven, Belgium)
Dorothy Denning (US Naval Postgraduate School, USA)
Myriam Dunn (ETH Zurich, Switzerland)
John James (United States Military Academy, USA)
Stephan Lechner (Siemens, Germany)
Eric Luiijf (TNO, The Netherlands)
Tom McCutcheon (Dstl, UK)
Götz Neuneck (U. of Hamburg, Germany)
Lars Nicander (FHS Stockholm, Sweden)
Saifur Rahman (Virginia Tech, USA)

General Chair

Bernhard Hämmerli (HTA Lucerne, Switzerland)

Program Chair

Stephen D. Wolthusen (Fraunhofer-IGD, Germany)

Submissions and questions should be sent electronically to swolthusen@ieee.org.