Informatik 2003
Frankfurt a.M., 29.09 - 02.10.03
<www.informatik2003.de>

CRITICAL INFRASTRUCTURE PROTECTION (CIP)

- STATUS AND PERSPECTIVES -

Preprints of the First GI Workshop on CIP, Frankfurt a.M. 2003

Edited by Willi Stein, Bernhard Hämmerli, Hartmut Pohl, & Reinhard Posch

Fraunhofer SIT Institut Sichere Telekooperation

Bundesamt für Sicherheit in der Informationstechnik

Fraunhofer ISST Institut Software- und Systemtechnik

An International Two-Days Workshop (Sept. 29-30, 2003)
within the Annual Meeting "Informatik 2003"
of the German Informatics Society (GI: Gesellschaft für Informatik)
at JWG University, Frankfurt a.M. (Sept. 29 - Oct. 2, 2003).

Johann Wolfgang Goethe-Universität Frankfurt a.M.

Sponsored by
Gesellschaft für Informatik (GI) e.V. Bonn (FB Sicherheit),
Fraunhofer ISST Berlin, and
Fraunhofer SIT Darmstadt.

Contents

SESSION 4: Policies and Methods

SESSION 5: Applicational Aspects and Assessments

Preface

This volume represents the preprints of the first workshop on Critical Infrastructure Protection (CIP) of the German Informatics Society (GI: Gesellschaft für Informatik e.V., Bonn). This international two-days workshop was held, as one part of the Annual Meeting "Jahrestagung Informatik" (Sept. 29-Oct. 2, 2003) of the German Informatics Society, at the Johann Wolfgang Goethe-Universität in Frankfurt a.M. on September 29-30, 2003.

But what do we mean with CIP? Protecting critical infrastructures (CI), such as communications, transportation, and energy, against disruption of any kind is increasingly crucial in maintaining both domestic stability and national security. CIP includes cyber, physical, and psychological levels to secure systems and assets.

Critical Infrastructure Protection and Information Security

The Critical Infrastructure Protection (CIP) approach logically includes the information security (InfoSec) approach and, in addition, has to consider a broader spectrum of risks and threats. The nature of risks and vulnerabilities in modern societies is becoming more and more transnational today.

An open, non-hierarchical dialog on newly recognised vulnerabilities at the physical, cyber, and psychological levels is needed to create a better understanding of new risks and their causes, interactions, probabilities, and costs.

Indeed, CIP is needed in each country, but CIP is extremely demanding, and implementing an effective CIP solution can easily exceed the scientific, technological, and organisational resources of a country.

CIP is a challenge within each nation's own responsibility that can be supported by bilateral and transnational activities. Therefore new forms of co-operation and/or partnership have to be developed: between scientific communities, between private and public actors, and between countries.

Origin of this workshop

The idea leading to this workshop evolved during talks, which we had one year ago with Dr. Manfred Reitenspiess (Munich) at an EU/DDSI meeting in Brussels (19-20 September 2002). Due to the "genius loci", we perceived the national, the European, and the transnational dimensions of CIP, and we tried to understand CIP as an IT-driven network-centric approach being indispensable in a more and more networked world. Sure, that is an IT-oriented position from an IT-oriented meeting.

Hence the present group of editors started organising this workshop by using initiatives from Austria, Switzerland (e.g., www.infosurance.ch) and Germany, including the co-operation mechanisms of the national informatics societies, i.e., GI, ÖCG, and SI.

One of our goals was to bridge the (still in all countries existing) gaps between the communities of information security (InfoSec) and of critical infrastructure protection (CIP/CIIP).

For the "Call for Papers" of this CIP Workshop we constituted an "International Board of Workshop Coordinators" having these members:

- Herbert Fiedler, U. of Bonn (Germany) herbert.fiedler@gmd.de
- Bernhard Hämmerli, HTA Lucerne (Switzerland) bmhaemmerli@hta.fhz.ch
- Eric Luiijf, TNO/FEL The Hague (Netherlands) luiijf@fel.tno.nl
- Jan Lundberg, SEMA Stockholm (Sweden) jan.lundberg@krisberedskapsmyndigheten.se
- Hartmut Pohl, FH Bonn-Rhein-Sieg (Germany) Hartmut.Pohl@sang.net
- Reinhard Posch, A-SIT Vienna (Austria) Reinhard.Posch@cio.gv.at
- Willi Stein, BSI Bonn (Germany) willi.stein@bsi.bund.de
- Gerhard Weck, Infodas Köln (Germany) GerhardWeck@compuserve.com

Acknowledgements

We wish to thank the Division „Security" of the German Informatics Society (GI-FB Sicherheit) and its speaker (Dr. Manfred Reitenspiess, Munich), the Fraunhofer Institute SIT Darmstadt (Prof. Dr. Claudia Eckert), and the Fraunhofer Institute ISST Berlin (Dr. Christoph Thiel) for sponsoring this volume.

In particular, we are deeply indebted to Daniel Bircher (EBP Zollikon), Helen Gill (NSF Washington), Carl Landwehr (NSF Washington), Eric Luiijf (TNO/FEL The Hague), Jan Lundberg (SEMA Stockholm), Jan Metzger (ETH Zurich), Andrea Servida (EU Brussels), and Samuel Varnado (SANDIA National Laboratory, Albuquerque) for supporting this workshop, either by communicating ideas or by opening doors to other experts.

We further express our appreciation to the authorities and the organising team of the annual meeting, and in particular to Silke Eberhardt (TU Ilmenau), Prof. Rüdiger Grimm (TU Ilmenau), Sabine Landvogt (U. Frankfurt), Jens Nedon (ConSecur, Meppen), Prof. Andreas Oberweis (U. Frankfurt), and Prof. Kai Rannenberg (U. Frankfurt).

Proposals for future European projects

We pointed out that CIP is a challenge within each nation's own responsibility, and that network-centric co-operative approaches are the way of acting in the interconnected society.

In our understanding, the next scientific steps on the way to an Europe-wide co-operative protection of critical infrastructures could include projects like these:

- European CIP Platform,
- European CIP Workshop,
- European CIP Newsletter,
- European CIP Network of Excellence, and
- European CIP Website.

For the editors of the CIP preprints:

Willi Stein

Critical Infrastructure Protection (CIP) Workshop – Introduction and Goals

Willi Stein, BSI Bonn (Germany) willi.stein@bsi.bund.de
Bernhard Hämmerli, HTA Lucerne (Switzerland) bmhaemmerli@hta.fhz.ch
Hartmut Pohl, FH Bonn-Rhein-Sieg (Germany) Hartmut.Pohl@sang.net
Reinhard Posch, A-SIT Vienna (Austria) Reinhard.Posch@cio.gv.at

Critical Infrastructure Protection (CIP)

Protecting critical infrastructures (CI), such as communications, transportation, and energy (see Figure 1), against disruption of any kind is increasingly crucial in maintaining both domestic stability and national security. The Critical Infrastructure Protection (CIP) approach is broader than the information security approach.

CIP includes both, cyber and physical measures to secure systems and assets whose incapacity or destruction would have a debilitating impact on the national security, and the economic and social well being of a nation (and its neighbours in physical and cyber space).

CIP and CIIP

Critical Information Infrastructure Protection (CIIP) is a subset of CIP. CIIP focuses on the protection of information technology systems and assets including components such as telecommunications, computers/software, Internet, satellites, etc., and on interconnected computers and networks, and the services they provide [from CIIP Handbook 2002].

CIP is a challenge within each nation's own responsibility that can be supported by bilateral and transnational activities.

Origin of the concept

The core concept of CIP, as in the process of implementation now, was developed in the US between 1996 and 1999, where the scientific and socio-technological foundations of CIP had been worked out by the RAND Corporation www.rand.org, beginning about 1989.

Detailed CIP and CIIP documentation is provided at www.ciao.gov/, www.pcis.org/, www.thei3p.org/, www.iwar.org.uk/ and at other links. Sector and layer models are used as illustrations for how critical infrastructures are organised. Meanwhile there exists an increasing number of CIP/CIIP-related activities outside the USA.

Critical infrastructure approaches in Germany www.bsi.bund.de/fachthem/kritis/index.htm, e.g., include the sectors:

1. telecommunications and IT infrastructures;
2. energy (i.e., electricity, oil and gas);
3. banking, finance and insurance;
4. transport systems;
5. public health care (including food and potable water);
6. emergency and rescue services;
7. government and public services (incl. police, customs and armed forces)

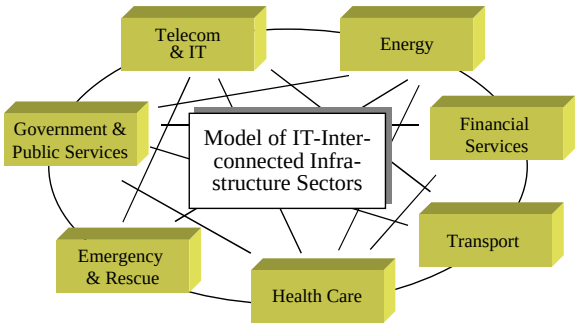

Figure 1: Model of IT-Interconnected Infrastructure Sectors

European CIP activities

European CIP activities presently include, e.g.:

1. the EU-supported initiatives DDSI www.ddsi.org/ (with country surveys), ACIP www.eu-acip.de/, and AMSD www.am-sd.org/;
2. the German private industry initiative www.aksis.de/;
3. Swiss Federal Strategy Unit for Information Technology (FSUIT) www.isb.admin.ch , the InfoSurance Foundation www.infosurance.ch/ and the Comprehensive Risk Analysis and Management Network (CRN) www.isn.ethz.ch/crn with conferences, documentation, and the CIIP Handbook (2002);
4. Norwegian protection approaches, started already in the early 1990s www.dsb.no/;
5. the Netherlands infrastructure studies www.tno.nl/instit/fel/ts/prj/critical-infrastructure-protection.html;
6. the CIO activities of the Austrian government www.cio.gv.at/;
7. the Swedish National Center of IO/CIP www.fhs.mil.se/institut/kvi/cios/english/index.html, the CRIS institute www.cris-inst.com/ and the Swedish Emergency Management Agency (SEMA) www.krisberedskapsmyndigheten.se/;
8. the UK activities at the National Infrastructure Security Co-ordination Centre www.niscc.gov.uk/ , at UK Resilience http://ukresilience.info/ and at the Information Assurance Advisory Council (IAAC) www.iaac.org.uk/;
9. explorations for a US-EU collaboration www.eecs.berkeley.edu/CIP/US-EU/agenda.html;
10. and, last not least, the Research Activity EU/IST (FP6) www.cordis.lu/ist/ with "Dependability" www.cordis.lu/ist/cpt/dependability.htm (including, e.g., the projects Examine and Safeguard) and Key Action 2 "Dependability of Information Infrastructures" www.cordis.lu/ist/ka2/dependability.html.

CIP activities outside the USA and outside Europe

Of further interest are the CIP activities outside the USA and outside Europe, e.g.:

1. of Canada www.ocipep.gc.ca/;
2. of Australia www.noie.gov.au/ www.nationalsecurity.gov.au/ www.defence.gov.au/predict/ www.ag.gov.au/ www.cript.gov.au/;
3. and of New Zealand www.ccip.govt.nz/ www.e-government.govt.nz/niip/index.asp.

Goals of the workshop

This workshop is intended to promote IT-oriented research and development in the emerging field of Critical Infrastructure Protection (CIP) and to contribute to the definition of R&D strategies with an European CIP focus.

More precisely, the workshop tries to promote the exchange of ideas, focus on national policies and common interests, gain in understanding/deepening of central research questions, and perception of interdisciplinary challenges.

Based on initiatives from Austria, Switzerland and Germany, this is one of the first CIP workshops with an IT orientation in Europe. Thus one goal of the workshop should be bridging the (in all countries still existing) gaps between the communities of information security (InfoSec) and of critical infrastructure protection (CIP/CIIP).

The target group of this workshop consists of officials, policy analysts, practitioners and researchers involved in the protection of international critical infrastructures against cyber-security threats.

In our understanding, the next scientific steps on the way to an Europe-wide co-operative protection of critical infrastructures could include projects like these:

- European CIP Platform,
- European CIP Workshop,
- European CIP Newsletter,
- European CIP Network of Excellence, and
- European CIP Website.