FP7 Grant Agreement N° 312450

CIPRNet

Critical Infrastructure Preparedness and Resilience Research Network

Project type: Network of Excellence (NoE)

Thematic Priority: FP7 Cooperation, Theme 10: Security

Start date of project: March 1, 2013 Duration: 48 months

D8.511 European CIIP Newsletter

Due date of deliverable: 30/06/2013
Actual submission date: 26/08/2013

Revision: Version 1

ACRIS GmbH (ACRIS)

Project co-funded by the European Commission within the Seventh Framework Programme (2007–2013)		
Dissemination Level		
PU	Public	**X**
PP	Restricted to other programme participants (including the Commission Services)	
RE	Restricted to a group specified by the consortium (including the Commission Services)	
CO	Confidential, only for members of the consortium (including the Commission Services)	

Author(s)	Bernhard Hämmerli (ACRIS) Erich Rome (Fraunhofer)
Contributor(s)	

Security Assessment	**This deliverable is excluded from security assessment**
Approval Date	–
Remarks	See Annex I – DoW. Two CIPRNet articles (by Rome and Martí) have been security assessed and received clearance.

The project CIPRNet has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 312450.

The contents of this publication do not reflect the official opinion of the European Union. Responsibility for the information and views expressed herein lies entirely with the authors.

TABLE OF CONTENTS

1 INTRODUCTION – RATIONALE OF THIS DOCUMENT 4
1.1 Target audiences and scope 4
1.2 Activities for the re-launch of the ECN 4
2 CONCLUSION 5
3 REFERENCES 5
APPENDIX: ECN ISSUE 15 (VOL. 7, NO. 1) 7

1 Introduction – Rationale of this document

This deliverable contains the first new issue (issue 15) of the European CIIP Newsletter (ECN) as a formal deliverable. During the term of CIPRNet, a total of 12 issues are planned, and all are formal CIPRNet deliverables. In this first deliverable, we briefly describe the purpose and history of the ECN, and the activities related to the re-launch of the ECN after a pause of more than three years.

The European CIIP Newsletter (ECN) is a focused dissemination organ for fostering the cooperation between the Critical (Information) Infrastructures Protection (C(I)IP) research communities and Critical Infrastructures (CI) and Critical Information Infrastructures (CII) stakeholders. The need for such a news organ had been identified 10 years ago, in 2003, on the first CIP conference in Germany. Since 2006, 14 issues of the ECN have been published, partly supported by the EU projects CI^{2}RCO [CIR2CO] and IRRIIS [IRRIIS]. CIPRNet continues to support the publication of the ECN until 2017 as Joint Activity 8.3 "Publications" of its Work Package 8 "Dissemination and spreading of excellence" [DoW]. The ECN will serve as an instrument for disseminating information and news on all the main topics related to CIP and specifically about CIPRNet. The continuation of this established newsletter allows inheriting its reputation and visibility and provides a strong instrument of communication with a large diffusion right from the start of CIPRNet.

The main responsible of the ECN and editor-in-chief is Bernhard Hämmerli of ACRIS (partner 12). For each of the twelve new issues, one of the CIPRNet partners will act as a co-editor, so that all CIPRNet partners will have co-edited an ECN issue at the end of CIPRNet.

1.1 Target audiences and scope

As core target audiences, The ECN addresses the CIP and CIIP research communities, policy makers, CI operators, crisis managers and civil protection agencies.

The scope of the ECN includes but is not limited to:

- Descriptions of new CIP and CIIP related research projects Including SCADA and Smart Gird Security, both on national and EU levels (up to 2 pages)
- Feature articles of project results (up to 4 pages)
- Expert articles on hot CIIP and CIP issues (up to 4 pages)
- Best practices in CIIP and CIP (2 pages)
- Announcements of CI(I)P related events (up to half a page)
- Reviews of new books on CI(I)P topics (up to one page)
- Conference attendance reports (up to two pages)

1.2 Activities for the re-launch of the ECN

The planning of the contents of the first three new ECN issues started at the CIPRNet kick-off meeting in March 2013. Given that the design and layout of the early ECN (Figure 1 (a)) were a bit dated, the coordinator decided together with ACRIS to design a new layout (Figure 1 (b)) that can also be easily handled by authors of ECN articles.

So far, former issues of the ECN were archived on the web site of the completed IP IRRIIS. CIPRNet has given the ECN its own homepage (Figure 2) as part of the CIPRNet website [CIPRNet]. Also, the archive of former ECN issues has been transferred to the CIPRNet website so that all issues can be retrieved from one source.

Fraunhofer was the main contributor to the redesign of the ECN and to creating the ECN home page.

Figure 1: (a) Old ECN title design (left), (b) new ECN title design (right)

2 Conclusion

The re-launch of ECN is on a very good way. The pipeline of planned articles is filled, and the ECN has a new layout and a professional homepage. The publication of the first issue is delayed by several weeks as compared to the original due date, but this is due to the singular overhead related to the re-launch and to the current summer vacation season. For the following issues, the original planned schedule will apply.

3 References

[CIPRNet] FP7 NoE CIPRNet homepage: http://www.ciprnet.eu

[IRRIIS] FP6 IP IRRIIS homepage: http://www.irriis.org

[DoW] Annex I – Description of Work (Annex to the Grant Agreement of CIPRNet).

[CI2RCO] Executive summary of the CI^{2}RCO project: ftp://ftp.cordis.europa.eu/pub/fp7/ict/docs/security/ci2rco-executive-summary_en.pdf

Figure 2: ECN homepage at the CIPRNet website

Appendix: ECN issue 15 (Vol. 7, No. 1)

European CIIP Newsletter

August–October 2013, Volume 7, Number 1

CRITIS 2013

Conference:

Register now!

ECN

Contents:

Editorial: The Meaning of a C(I)IP Community

Justifying security measures for CIP

Managing Complexity: Electric Power and Inter-dependent Systems

CRITIS 2012: Risk Assess-ment Findings

CIIP & Resilience

Effective Surveillance for Homeland Security

CRITIS 2013: Register Now!

CIPR Net

> About ECN
ECN is co-ordinated with
The European Commission, was initiated by Dr. Andrea Servida,
today funded by the European Commission
FP 7 CIP Research Net CIPRNet Project
under contract, Ares(2013) 237254

>For ECN registration ECN registration & de-registration:
www.ciip-newsletter.org

>Articles can be submitted to be published to:
editor@ciip-newsletter.org

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

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

>Download site for specific issues:
www.ciprnet.eu

The copyright stays with the editors and authors respectively, however people are encouraged to distribute this CIIP Newsletter

>Founders and Editors
Eyal Adar, Founder and CEO, WCK www.wck-grc.com
Christina Alcaraz, University of Malaga, alcaraz@lcc.uma.es
Bernhard M. Hämmerli, HTA, Initiator and Main Editor bmhaemmerli@acris.ch
Eric Luiijf, TNO, eric.luiijf@tno.nl
Erich Rome, Fraunhofer, erich.rome@iais.fraunhofer.de

>Country specific Editors
For France: Michel Riguidel, ENST, riguidel@enst.fr
For Spain: Javier Lopez, UMA, jlm@lcc.uma.es
For Finland: Hannu Kari, HUT, kari@tcs.hut.fi
to be added, please report your interest

> Spelling:
British English is used except for US contributions

Editorial

Intro	The Meaning of a C(I)IP Community by Erich Rome & Bernhard Hämmerli	5

European Activities

FP 7 CIPRNet	EU Network of Excellence for more resilient Critical Infrastructures by Erich Rome	7
FP 7 ValueSec	How to rationalise and economically justify security for CIP By Reinhard Hutter and Christian Blobner	9

Country Specific Issues

DR-NEP, Canada	Managing Complexity: Electric Power and Interdependent Systems by José R. Martí	13

Method and Models

Risk Assessment	Food for thought: Risk Assessment Panel Results CRITIS12 by Marieke Klaver	17

Books on C(I)IP

CIIP and Resilience in ICT	Critical Information Infrastructure Protection and Resilience in the ICT Sector by Paul Theron and Sandro Bologna	
Homeland Sec	EFFECTIVE SURVEILLANCE FOR HOMELAND SECURITY by Francesco Flammini, Roberto Setola and Giorgio Franceschetti	21

CRITIS 2013 Conference

CRITIS 2013	CRITIS Conference 2013: Register now! by Eric Luiijf	23

Links 24

Editorial: The Meaning of a C(I)IPCommunity

New challenges need new structures and alliances. Therefore community building tools such as conferences, exchange between researchers industry and government as well as books and journals are essential.

During the First International CIP Conference in Frankfurt supported by Willy Stein from BSI Federal Office for information Security (Germany), and Stefan Brem from Ministry of Foreign affairs Switzerland, the wish of community building arose with the following targets:

1. Create at least one CIP book which could be used at Universities for teaching and for getting a common understanding for PHD students.
2. Create a Newsletter in which the community can exchange with each other and get an understanding of what is going on in Europe and internationally.
3. Have an annual conference on the topic of CIP, integrating the stakeholders from government, administrations, industry, service providers and research, such that a dialogue and debate can be lead.

Ten years passed and that wish has become reality. It was not only the engagement of many experts of the community, but also just the developing history, which confirmed all technical expertise by CI related incidents. It is the fatal alliance of security with the destiny, that incidents only move the topic forward. Incidents create facts: this has been confirmed by more than 2000 years of military defence history.

In the current phase, the awareness of governments on threats to CII has been raised based on experiences like Red October, Flame Duke, Stuxnet and similar on both ends of the security theatre:

1. There is an economic and cheap way to get far better and more information than at any time before in history at minimal cost.
2. The bet can be used – beside of intrusion – for reaching impact on the enemy or competing party.

And the other side:

3. Each nation is permanently exposed to attacks on their confidential information and never knows how far others are able to penetrate.
4. Each nation sees itself as a victim of permanent attacks which may lead to third party having control on their data and infrastructure. In the physical space this could create relevant damage.

In this respect, the European CIP community has a legitimate hope that cooperation will happen and create common values, leading to synergies. And this is what we want to stimulate and to learn about how to identify these domains of collaboration.

Some frameworks supporting collaboration already exist: For instance, ENISA (European Union Agency for Network and Information Security) developed a CIP program that assists EU States and Commission to better understand the emerging CIIP landscape. However, this is not enough.

The Report at the Centre for European Policy studies CEPS on "the critical Infrastructure of the EU" clarified that there is a third stakeholder party beside service providers and governments: the suppliers. We have to be aware of the powerful position of the suppliers and to integrate them in all phases of incidents, according to the need of the running services and infrastructures.

It is lead to each expert to reflect the trust into the suppliers, and how to design the architecture of the tuple "Legal contract" – "Technical design and architecture" – "Exposures and Dependencies".

However, all these thoughts are far beyond the comfort zone, but unhappily completely irresponsible to not reflect on it!

Erich Rome is a senior researcher and project manager at Fraunhofer IAIS' ART department.

erich.rome@iais.fraunhofer.de

Bernhard M. Hämmerli is
Professor in Information Security and CEO of Acris GmbH
He is President of Swiss Informatics Association SI www.s-i.ch
e-mail: bmhaemmerli@acris.ch

As always, selected links – mostly derived from the author's articles – and events conclude this issue.

Enjoy reading this issue of the ECN!

PS. Authors willing to contribute to future ECN issues are very welcome.

CIPRNet: EU Network of Excellence for more resilient Critical Infrastructures

»CIPRNet« aims at establishing a European Infrastructures Simulation & Analysis Centre. Providing new capabilities for crisis managers and building capacities of researchers and trained experts are key elements of CIPRNet.

The EU-sponsored Critical Infrastructure Preparedness and Resilience Research Network (CIPRNet) project will establish a European Infrastructures Simulation and Analysis Centre (EISAC). This centre will provide substantial improvements for fast and adequate responses by authorities and critical infrastructure owners to complex emergencies affecting or originating from critical infrastructures. The research network will integrate knowledge and technologies to create added-value decision support capabilities for national and multi-national emergency management.

On March 1, 2013, the Critical Infrastructure Preparedness and Resilience Research Network (CIPRNet) project commenced. CIPRNet is a Network of Excellence activity in civil security research, co-funded by the European Commission's 7th Research Framework Program (FP7). Within four years, the CIPRNet consortium will make a decisive effort towards providing support from the Critical Infrastructure Protection (CIP) research communities to emergency responders, governmental agencies and policy makers, enhancing their preparedness against service disruptions of Europe's complex system of interconnected and dependent infrastructures.

The CIPRNet Consortium

CIPRNet comprises six European research institutes (Fraunhofer, ENEA, TNO, CEA, JRC, Deltares), the International Union of Railways UIC, three European universities (Rome, Cyprus, Bydgoszcz), a Canadian university (UBC at Vancouver) and ACRIS GmbH from Switzerland. The project coordination is by the Fraunhofer Institute for Intelligent Analysis and Information Systems IAIS. The CIPRNet consortium of research organisations, universities and end-users brings together a unique set of knowledge and technology gathered in over sixty previous research projects in the field of CIP. Each partner also functions as a multiplier by connecting to national and international networks and research platforms.

> "A lack of situational awareness and protection of critical infrastructures by emergency management operations may result in the unwanted extension of the duration and size of emergencies with more casualties, more suffering, and more damage than needed."
>
> E. Luiijf, M. Klaver, 2013

New capabilities

Reaching and maintaining the required level of preparedness requires adequate and fast adaptation to ongoing changes of Critical Infrastructures (CI). CIPRNet will implement advanced modelling, simulation and analysis capabilities for supporting more effective responses to disasters and emergencies that affect or originate from multiple CI. In particular, CIPRNet will create added-value decision support capabilities for national and multi-national emergency management. These capabilities will enable decision-makers and operators to analyse the various possible courses of action, to perform "what if" analysis, and to learn about short and long term consequences of their decisions. The consequence analysis will be based on real-time and statistical data, status information on involved CI, meteorological data, and more. The development of this new decision support capability will build upon pooling and integrating technologies and resources available at CIPRNet's partners and beyond.

As an additional capability, CIPRNet plans supporting the security design

Erich Rome

Erich Rome is a senior researcher and project manager at Fraunhofer IAIS' ART department. In 1983, he received a diploma in Computer Science (U. Bonn). Thereafter, he worked as a researcher at GMD (merged in 2001 with Fraunhofer), investigating topics in Expert Systems and AI. In 1995, he received a PhD degree in Engineering Sciences from the University of Bremen and started research in robotics. Since 2007, Erich Rome investigates modeling, simulation and analysis for critical infrastructure protection and multi-sensory systems for surveillance and security. He published numerous peer-reviewed publications, edited several books and is a member of the steering committee of the workshop series CRITIS. So far, he coordinated four EU projects, CIPRNet being the current one.

e-mail:
erich.rome@iais.fraunhofer.de

of Next Generation Infrastructures like Smart Grids.

Scenarios & Architecture

CIPRNet creates scenarios at different scales for developing, testing and training the new capabilities. A regional Italian scenario will consider several infrastructures and threats like floods, landslides, and earthquakes. A scenario in a densely populated region of the border between The Netherlands and Germany will consider cross-border emergencies.

The development of the new capabilities follows a model-based systems design approach. Key elements of this approach are scenario orientation, requirements engineering, and use cases. Using questionnaires, CIPRNet will gather general requirements for decision support and simulation systems from potential end users.

As a field test of the new capabilities, CIPRNet will demonstrate timely, actionable, risk-informed CIP analysis and strategies for authorities.

Capacity building

In order to provide long lasting support from the research communities, CIPRNet aims also at building the required capacities. Numerous dissemination and training activities will contribute to this aim, including but not limited to the following. Dedicated cooperation workshops with other projects and networks in the field will contribute to a better coherence in the distributed multi-community of CIP researchers and experts. Dedicated training activities will familiarise experts and potential end users with CIPRNet technology and knowledge. Young researchers will be trained via staff exchange between CIPRNet partners and by integrating CIPRNet lectures into the Master in Homeland Security course at the Università Campus Bio-Medico in Rome, Italy. The CRITIS conference series will contribute to dissemination and visibility of CIPRNet results.

The CIPRNet Community

From the start, CIPRNet will involve its stakeholders in the design of the new capabilities. This will be accomplished both by an International Advisory Board of end users and other stakeholders, and by targeted workshops and training events. The International Advisory Board has currently ten members from civil protection authorities, ministries, industry, and associations fostering security and CIP. An Independent Ethics Board of experts in data protection and privacy ensures compliance of the project results with legal and ethical standards.

VCCC and EISAC

For achieving a long-term impact and improvement, the new capabilities need to be consolidated and sustained beyond the duration of the project. For the development, consolidation and dissemination of the new capabilities, CIPRNet will establish a virtual centre of competence and expertise in Critical Infrastructure Protection, the VCCC. The VCCC is a virtual facility since during the term of CIPRNet it will neither be a legal body nor a built structure. But it will serve as a foundation for a European Infrastructures Simulation & Analysis Centre (EISAC), with the ultimate goal of sustaining the new capabilities and further innovations beyond the duration of CIPRNet.

A design study of EISAC is available from the completed EU project DIESIS and will be employed in CIPRNet. The idea here is to found autonomous national EISAC nodes in Member States who would support this. These nodes shall provide services tailored to the needs of the Member States. A central roof organisation at a European level shall ensure standardisation of basic technology like middleware and modelling approaches, broker bilateral cooperation of EISAC nodes, and provide support at EU level.

Since transfer of research results into application as well as modelling, simulation and analysis based new decision support capabilities will be the focus of EISAC, it will be complementary to the services of networks like CIWIN (Critical Infrastructure Warning Information Network) and ERNCIP (European Reference Network for Critical Infrastructure Protection).

Acknowledgments

This work developed from the FP7 Network of Excellence CIPRNet, which is being partly funded by the European Commission under grant number FP7-312450-CIPRNet. The European Commission's support is gratefully acknowledged.

The author gratefully acknowledges the contributions of his CIPRNet partners to this article. It should be regarded as a joint publication of the consortium.

References

Final report of the DIESIS project available at www.diesis-project.eu

Luiijf, H.A.M., Klaver, M.H.A., Expand the Crisis? Neglect Critical Infrastructure! (insufficient situational awareness about critical infrastructure by emergency management – Insights and Recommendations), in: Tagungsband 61. Jahresfachtagung der Vereinigung des Deutschen Brandschutzes e.V., 27-29.05.2013 Weimar, Germany, pp 293-304.

CIWIN: https://ciwin.europa.eu/

ERNCIP: https://erncip.jrc.ec.europa.eu

CRITIS 2013: http://www.critis2013.nl

More information

www.ciprnet.eu

How to rationalise and economically justify security for CIP

Developing efficient security requires advanced methodologies for transparent planning and decision support. This includes dynamic scenario forecast, use case experiments, and advanced tools for the organisations and users involved

There has been a tradition across Europe (and the US) of military security planning over at least 50 years. Cold war postulated mainly one scenario option until 1990. Most countries (and NATO [1]) had their dedicated analytical capabilities to support military organisation, planning, procurement and operations, the latter – fortunately – only in simulated, never in real scenarios. This relatively clear process changed, gradually during the nineties and more radically since 09/11 and its aftermath. NATO has to struggle for new options, and the EU successively develops its own security and defence role.

What is new?

The discussion here analyses the considerable shift in the security paradigm from the military and the cold war to homeland security and the changing threat spectrum. This has mainly been a shift to complexity and uncertainty. At least three major changes have to be realised, understood and transferred to processes and tools which allow for "optimal" decisions in today's and tomorrow's fast changing world:

1. Needs for **organisational** changes require a novel type of political decision processes
2. The **scenarios** of changing vulnerabilities, threats and risks require good foresight and continuous updating
3. The **planning and decision process** of necessary security measures requires powerful tools and methods of application

While the armed forces have been one organisation/administration with by and large one typical mission, "Homeland Security" in western countries is typically planned and enforced by eight to ten different organisation and up to thrity administrative bodies at different political levels, e.g. in Germany by various federal, state and communal/ local authorities.

The two-block [2] military scenario of territorial and sovereignty defence was more and more replaced by the variety of possible threats (terrorism, technical and natural disasters), and vulnerabilities. The focus shifted from thinking in categories of territorial sovereignty to security of societies who are heavily relying on (critical) infrastructures.

> Requirements for security planning and decision have substantially changed

Whereas military life cycles lasted 30 to 40 years, civil security measures need to be implemented in rather short periods and be flexible for adaptation to fast changing priorities.

We will not speculate about the need for changing **organisations** and processes of cooperation and coordination between the different organisations. This is mainly political business. Rather we will give a few examples on how things are improving at EU level concerning forecast and assessment of **scenarios**, and then we will mainly concentrate on an effort which should help systematise the process of planning of and decision making on security measures.

[1] NATO with its SHAPE Technical Center STC, later NCI, the NATO Consultation, Command, Control Agency

[2] NATO and Warsaw Pact

Reinhard Hutter

Technical Director, CESS GmbH. He has been senior vice president on Information and Communications Systems at IABG. In 2007 he co-founded CESS, the Centre for European Security Strategies.
e-mail: hutter@cess-net.eu

Christian Blobner

Project Manager at Fraunhofer Institute for Factory Operation and Automation IFF, focusing on security research, from 2006 ongoing. Coordinator of the EU-FP7 ValueSec project.

christian.blobner@iff.fraunhofer.de
Photo: © by Dirk Mahler

The EU 7th Framework Program in its Thematic Area 10 "Security" has, since 2008, allocated €1.3bn and funded an estimated 200 projects. Many of them focus on technologies, but increasingly also on future threat and protection scenarios. As far as CIP and CIIP is concerned, there is a coordinated overlap to the FP7 ICT theme.

The FOCUS project[3] has developed several long-term foresight scenarios, one being focused on Critical Infrastructure and supply chain protection which not only sees the technical vulnerabilities but more so the future role of the EU and EU research, societal aspects, cross-border requirements, and comprehensive risk assessment. The time horizon envisaged is 2035.

Another, still on-going project, CATO[4], deals with CBRN (chemical, biological, radiological, nuclear) crisis management architecture, technologies and operational procedures. It will develop an "open toolbox" for managing non-conventional terrorist attacks or attacks on facilities holding CBRN material. Again, solutions will be tested in concrete simulated and/or experimental scenarios.

Decision support

Let us now elaborate in some more detail on the challenge of decisions for security. The provision of a public good like security through market mechanism is difficult, to say the least, as every citizen benefits from it but has little incentive to voluntarily contribute to its realisation. This calls for responsibility and action of public stakeholders, i.e. of the government and public bodies. Governments have to create the legal, organisational and financial framework to provide security. Security related decision-making in the public sphere needs to take into account a complex socio-economic and political environment. A cost benefit analysis in the field of security related public decision making, therefore, always has to consider a variety of possible scenarios and a considerable number of quantitative and qualitative factors. This together with the discussed complexity of organisations and the uncertainties on future scenarios comprise the main challenge because a systematic analytical planning and decision process supported by validated support tools is widely missing.

The Approach

The ValueSec[5] project is attacking this multi-dimensional challenge with a comprehensive methodological approach that – to our knowledge – has not been tried before. After an intensive survey and evaluation of more than 50 candidate theories, methodologies and tools on the one hand, and the analysis of the immense number of different factors influencing security related decisions on the other, it became obvious that the one single "general purpose decision support" will never[6] be feasible.

> We need to better foresight scenarios

Therefore, the decision space was separated into three decision subareas. It should be emphasised that ValueSec is not dealing with tactical/operational, i.e. short-term, decisions during an incident. The project addresses planning of security measures and evaluating decision alternatives on a strategic, i.e. medium- to long-term horizon. The spectrum of possible security measures may range from legislation, organisation and procedure changes, investment in new or more technologies or improving preparedness by training and exercising. This decision making of public stakeholders in the field of security is embedded in a complex web of interdependencies, which can obscure the full costs and real benefits of decisions but also their different consequences, sometimes hard to identify, to trade-off against each other, and to attribute to the specific decision. This complexity has to be reflected in the way decisions should be supported from an analytical point. Potential effects and consequences of decisions have to be made transparent. The ValueSec project, therefore, establishes a comprehensive approach based on three pillars of analytical methods and tools:

- RRA = Risk Reduction Assessment: Calculating the expected reduction of risks caused by the security measure(s) in question
- CBA = Cost Benefit Analysis: Comparing those positive and negative effects of security measure(s) which can be expressed in monetary terms
- QCA = Qualitative Criteria Analysis: Evaluating all criteria which influence the decision, that cannot be expressed in quantitative terms

Accordingly, a typical evaluation of a security measure will follow the three steps in close sequence:

- Risk reduction is usually the starting point of an evaluation, as the reduction or mitigation of damages and/or of the likelihood of an incident is usually the most important driver for any security policy decision. Different tools are offered like simulation, heuristic hierarchical models and evaluation methods based on probability theory.
- The cost-benefit calculations need input from the RRA as the CBA model will balance the cost of a security measure against the monetary savings in case of security incidents. It is based on a classical life-cycle cost modelling approach (planning, development, procurement, maintenance etc.). It is deliberately limited to those effects which can be expressed in money.
- All other decision criteria (which are often implicit part of a CBA), have been structured in a separate utility analysis tool based on the methodology of MCDA [7] which has been tailored towards the specific requirements of security related decisions.

At the end of these steps, the three different results need to be commonly interpreted and aggregated to recommendations for the decision maker. Furthermore, sensitivity analysis and comparison of alternative measures are enabled.

[3] http://www.focusproject.eu/knowledgeplatform/workbench (2011-2013)

[4] http://cordis.europa.eu/search/index.cfm?fuseaction=proj.document&PJ_LANG=EN&PJ_RCN=12533818&pid=28&q=FD8A9BBC079BD5FCECD584ADBD3CE6A7&type=adv (2012-2014)

[5] http://www.valuesec.eu

[6] Never say never, but at least not within a reasonable frame of time and money

[7] http://en.wikipedia.org/wiki/Multi-criteria_decision_analysis

Decisions driven by qualitative criteria

In security, much more than in usual political or business investment decisions, many (sometimes most) driving factors are not quantifiable in numerical, physical or commercial units. This particularly holds for questions like:

- How does society react to and accept security measures, including questions of civil liberty, data protection and privacy?
- How do security measures interfere or comply with the national and international legal and procedural frameworks?
- Which are expected consequences for the environment, for ethical settings etc.?
- How do political factors like compliance to the political agenda or to competing or rivalling political forces influence the security decision?
- How attractive or counterproductive is the security measure from scientific/technological and economic/commercial point of view?

The in-depth analysis of these different "intangibles" revealed how complex security decisions may be. The categories above have been broken down into a total of almost 100 different criteria which will, in a concrete evaluation case, be subject to selection, weighting and a normalised pseudo-quantification via so called Utility Functions.

The progress beyond state of the art

In summary, the decision rational when using this 3-pillar methodology follows a systematic and transparent evaluation of decision parameters such as threats and risks, budget restrictions as well as political and societal needs. The overall assessment finally has to integrate the results of these three pillars of risk, costs, and concepts of value. This method provides a novel holistic analytical view. It comprises the huge number and variety of decision parameters in security planning and decision processes. This helps to base decisions more on rationale rather than on intuition, and to make the processes fully transparent.

Scenarios and use cases

The ValueSec toolset is being integrated into a common user interface and a remotely accessible software architecture for distributed use. Its performance is being evaluated with respect to three dimensions: The adequacy to the decision maker's security problem, the efficiency of setting up and exercising evaluation rounds for concrete applications, and the acceptance by the end-user (complexity, understanding, usability and user interface). The evaluations have been started with five different so called scenario based Use Cases all of which are addressing the wider domain of improving security of critical infrastructures:

1. Improving protection of visitors of a public mass event through better screening and surveillance technology
2. Protecting passenger trains from being compromised with explosives
3. Improving airport security by introducing advanced liquid/aerosol/gel (LAG) scanning systems
4. Reducing damages in a flood-prone area by improved dyke and water management systems
5. Reducing vulnerabilities in SCADA systems with improved communications and organisational coordination.

This spectrum of rather different applications serves as a platform of demonstrating the multi-purpose applicability of the developed toolset. Valuable feedback has been generated during a stakeholder Workshop on 26 June, 2013, and final results and conclusions will be presented at the final ValueSec conference in December 2013.

One basic question remains for the time being: Will decision makers welcome or fear a more transparent planning and decision process?

The authors would like to acknowledge the work of the whole ValueSec consortium without whom this article would not have been possible. Furthermore, the authors acknowledges the funding of the research work carried out in the ValueSec project by the European Commission in the 7th Framework Program – FP7 (Contract number 261742). For more information see www.valuesec.eu.

(left intentionally blank
for double sided printing)

Managing Complexity: Electric Power and Interdependent Systems

Modern critical infrastructures constitute highly complex systems that challenge our technical and cognitive capability to effective manage their behavior

Divide and conquer strategies have been advanced throughout the years to cope with the complexity of power system networks and allow for real time simulation and control. More recently, these techniques have been applied to the problem of critical infrastructure protection and disaster response. Models that can incorporate multiple layers of interaction among economic, social, human, and physical systems are needed to bring "order among chaos" in the rapid expansion of the twenty-first century power grid and in an effective disaster response.

Complex systems

In a classical definition, a complex system is a network of heterogeneous components that interact nonlinearly to give rise to some emergent behaviour. The complexity of the interactions increases considerably when humans are part of the system.
For example in disaster response, "humans in the loop" appear in the form of victims of the disaster, first responders, decision managers, and policy makers. Interactions among agents form dynamic continuum of past, present, and future actions and consequences.

An early effort to model the complexity of human and physical system interactions was made by Forrester (Forrester 1971). In his work he sets out to model the entire world of resources, production, capital, trade, environment, and population growth. He aptly called his model "World Model" and was the basis of the influential work "The Limits to Growth" by the Club of Rome.

A technical definition

From a technical point of view, we can relate our perception of complexity to our capability of cognition of the process. We can postulate three principles that determine our ability for cognition: 1) Our understanding of the process, 2) The sophistication of our modelling tools, and 3) Our capability of measuring the parameters. Our ability to observe and measure the process determines what the system looks like to us. Our thinking about what we see determines our ability to establish relationships among the parts. Properties of the objects and the relationships among objects allow us to form system models that can be used to predict the expected outcome from the system for situations not yet observed.

> Complexity is related to our capability of cognition of the process.

As our means of cognition improve, so does our tendency to build even more complex systems. However, as complexity challenges our ability of cognition, the tolerances to control the processes become narrower. For example, in meshed power systems, as opposed to radial systems, the settings of the protection and control devices have to be kept under much narrower margins.

Growth of the power grid into a complex system

The electric power grid has been called by the IEEE the largest machine ever built by humanity. Edison's single-generator DC system that could carry electrical energy over a distance of 3 km to 59 customers was quickly replaced by Tesla-Westinghouse's AC system that can carry electrical energy through hundreds of kilometres provided that all generators in the network turn together in "synchronicity".

José R. Martí

José R. Martí Professor, Electrical and Computer Engineering, The University of British Columbia, Vancouver, Canada

e-mail: **jrms@ece.ubc.ca**

The North American electrical grid is the largest in the world, with a capacity of about 1300 GW and total assets of over $1 trillion. It comprises three major extensive interconnected areas: the Eastern, Western, and Texas systems. The AC grid's extension and its synchronicity requirement (a generator in Alberta has to run in sync with a generator in Arizona) make the AC grid one of the most complex systems ever created.

The paradigm of large generating plants operating synchronously and long transmission lines carrying electricity over large distances defined the nature of the power industry. Single companies owned generation, transmission, and distribution forming monolithic structures in terms of ownership and operational requirements. Because of the physical constraints of the system, deregulation models that were successful in the telecommunications industry met with very limited success in the power industry.

The extraordinary growth of the power grid in industrialised countries in the twentieth century, together with the grid's reliability, made it the centre of the national system of critical infrastructures (CI's) in modern societies. In Canada we define ten CI's: energy, water, food, manufacturing, finance, ICT, transportation, health, safety and order, and government and defence. Problems in the power grid affect all other infrastructures and large blackouts have severe consequences.

The Emerging Distributed Grid

The twentieth century power grid was very successful in making electricity available at reasonable prices and with high reliability. Nonetheless, its structural model was unsustainable. A number of crises and concerns emerged at the end of the last century and continue aggravating in the twenty-first century that are driving a new paradigm.

The energy crisis, the economic crisis, the environment concerns, and the sustainability challenges are driving the electrical grid into a heterogeneous world of distributed ownership of clean, renewable energy sources.

The continued indiscriminate use of carbon-based fuels is having grave consequences for the environment. Using coal to generate 1 kWh of electricity, each hour that a person sits in a room with a couple of lamps, a couple of computers, and some heating or cooling, one kilogram of CO_2 is released into the atmosphere. Half a kilogram is released if natural gas is used for generation, but only 5 to 50 grams are released if alternative renewable sources, like wind, water, or solar are used to generate the electricity.

Network models

In terms of its topological structure, the power grid tends to follow a scale-free small-world network model where the average strength of the nodes is of polynomial order. The network contains denser sub-regions with links joining the sub-regions. In mathematical terms, the matrices representing the system states tend to be block-diagonal.

> The electric power grid is at the centre of the national system of critical infrastructures.

The emerging distributed grid will maintain this basic structure and even though there will be more independent nodes in terms of generation, there will be a stronger need to share storage to balance out the non-dispatchable nature of alternative sources.

In terms of ownership, the traditional grid constitutes a monolithic hierarchical structure with relatively few points of interdependency between business decisions and operational decisions. The new distributed-generation grid, on the other hand, will have multiple ownerships and a trading market will emerge which will more tightly integrate operational and business decisions. Modelling this new paradigm will require more of a "world model" that closely integrates economic, social, and developmental layers with the physical layer of producing and distributing electricity.

"Divide et impera": breaking complexity in the power grid

An effective way to manage complexity is to break a large system into subsystems joined by links. In social and biological networks this is known as Community Structure Theory. For electric power networks this concept has been extensively applied to achieve faster solutions in very large networks (Martí et al. 2002).

The Multi-area Thévenin Equivalent concept (MATE)

MATE conceptualises a complex system as made up of "independent subsystems" that exchange resources through a mediating "links subsystem".

The MATE solution involves three steps. First, the independent subsystems are solved separately, without considering the links. Next, the links subsystem is solved. Third, corrections are applied to the subsystems to account for the flow through the links.

The MATE approach allows each subsystem to be solved as a separate entity and each subsystem may use a different solution technique and different time constants. The links subsystem provides a common ontological framework where the interactions among subsystems can be resolved. During the links solution, the independent subsystems are represented by a reduced-order equivalent of a dimensionality equal to the number of external nodes. In the case of electric circuits, this concept corresponds to the Thévenin / Helmholtz Theorem.

I2Sim for disaster management

During large disasters, such as earthquakes, tsunamis, floods, and others, multiple critical infrastructures may suffer damage in their physical integrity or on their ability to provide their services. This results in a reduction of the available resources (e.g., electricity, water, food, shelter, transportation, etc.) and in a congestion of some of the essential services (e.g., transportation, hospitals).

The proportion in which the available resources are distributed to the units that require those resources will determine the functionality of those units.

For example, the ability of a hospital to treat the victims of the disaster will depend on the availability of electricity, water, doctors, nurses, medicines,

etc. If, after damage in the electrical substation, most available electricity is given to the hospital, there might not be enough electricity for the water pumping station to supply the hospital. In this case, the hospital might be severely limited, not for lack of electricity but for lack of water. A better decision would have been to split the power between the hospital and the water pumping station.

In the example above, the power network and the water network can be considered as independent subsystems, with the power substation, the hospital, and the water pumping station as the links subsystem joining the power and water networks.

The i2Sim framework (Martí et al 2008) was developed to model the links subsystem that ties in multiple critical infrastructures providing resources to a community.

The decision nodes where resources allocations are determined are part of the i2Sim subsystem. The human decisions layer where policy makers, managers, and responders come together to make an allocation decision is interfaced, through control signals, with the i2Sim physical subsystem layer. To help foreseeing the consequences of allocation decisions, multiple i2Sim optimisation loops can be run performing "what if" scenarios.

In the i2Sim framework, the power network, the water network, etc. can be modelled using conventional off-the-shelf simulation tools for the particular domain. i2Sim provides the common ontological framework where the interdependencies among multiple dissimilar subsystems come together.

Disaster Response Network Enabled Platform (DR-NEP)

The Disaster Response Network-Enabled Platform (DR-NEP) project of Canada's Advanced Research and Innovation Network (CANARIE 2013) provides an online platform that can integrate experts and simulation tools across multiple geographical locations.

> I2Sim provides a common ontological framework to resolve interdependencies among dissimilar critical systems.

DR-NEP's main node at the University of British Columbia hosts an Enterprise Service Bus architecture (ESB) where multiple domain simulators are interfaced through software adapters to a common database that follows the i2Sim ontology. i2Sim is also interfaced to this ESB bus. Data is exchanged through this common bus among domain simulators and i2Sim. A software controller keeps the timing and synchronisation among the domain simulators and i2Sim.

User interaction is provided by web services that can be accessed using a common web browser. Through this browser interface, the user or group of users can run complex disaster management simulations involving disaster event simulators, damage assessment simulators, multiple domain simulators, and decision optimisation tools.

References:

Forrester Jay W (1971) World Dynamics 2nd Ed. Wright-Allen Press, Massachusetts

Martí JR et al (2002) OVNI: Integrated Software / Hardware Solution for Real-Time Simulation of Large Power Systems. In: Proceedings of 14th PSCC, Seville, Spain, June 24th – 28th, 2002

Martí JR et al (2008) I2Sim Modelling and Simulation Framework for Scenario Development, Training, and Real-Time Decision Support of Multiple Interdependent Critical Infrastructures during Large Emergencies. In: Proc. of NATO (OTAN) MSG-060 Symposium on "How is Modelling and Simulation Meeting the Defence Challenges out to 2015?" Vancouver 7-8 October, 2008

CANARIE (2013) Canada's Advanced Research and Innovation Network. Disaster Response Network-Enabled Platform (DR-NEP). http://www.canarie.ca/en/network-programs/network-platforms/nep/projects. Accessed 28 May 2013

(Left intentionally blank
for double sided printing)

Food for thought: Risk Assessment Panel Results CRITIS12

Close interaction between CIP researchers and CI stakeholders required

CRITIS12

In 2012, the yearly international CRITIS Conference on Critical Information Infrastructure Security took place in Lillehammer, Norway. The conference continued the CRITIS tradition of presenting innovative research and exploring new challenges for the protection of critical infrastructures. As in previous years, invited speakers and panel discussions complemented a program of original research contributions.

In the spirit of the past conferences, CRITIS12 also provided a forum for stakeholders from the academic but also government and industry sides to discuss challenges openly in a constructive atmosphere.

The final panel discussion treated some of the main issues that were identified during the conference. This article describes the result of the final panel discussion.

The current level of security

The conference reflects the knowledge of many cyber security experts. The panel was asked for their expert opinion on the current level of security: are we doing enough? The various panel members stated that it is difficult to be assured that we are doing enough. The results and approaches presented are based on the current knowledge of experts. We are, however, still not confident that we have the right approach. Moreover, it proves hard to compare the level of security across sectors or companies lacking for instance a set of comparable metrics. For example, the level of security at SWIFT is regarded as very high; but in order to compare that level to the energy sector, a more detailed analysis is required of, e.g., the security characteristics of the different sectors, the risk appetite and where the cost of the security measures lies.

Are current risk management methodologies adequate for all situations (especially regarding the ICS domain)?

Industrial Control Systems (ICS) have a different role in companies than general ICT systems and fall often under different organisational control. Therefore, stakeholders may need other methods for risk assessment and business impact analyses to deal with ICS. Also for ICS less reliable historical data is available as input for the risk assessment.

> It proves hard to assess the current level of security for CI; good metrics are still missing

Another issue for risk assessment is how to include the risk related to external dependencies, e.g. due to external service providers for maintenance or outsourcing. As an example, when a certificate providing service company in the Netherlands had serious security problems (DigiNotar) in 2011 and ceased to exist, it proved to be very difficult for the government to identify all the key processes in municipalities that would be affected by revoking their 3500 certificates at once. Most organisations did not have a second (backup) certificate supplier and did not have spare certificates by them at hand.

Marieke Klaver

Marieke Klaver is a programme manager at TNO, the Netherlands. Her areas of research are Critical Infrastructure Protection and Cyber Security.

e-mail: **marieke.klaver@tno.nl**

Dissemination of research results/getting the message across

We need to share results and start learning from each other. We do present results at conferences such as CRITIS, but we do not bring our main messages across to other communities and organisational levels such as decision makers and the C-level. In order to bring the topic to a higher level, leadership is required and national authorities and decision makers need to be convinced of the need to act.

Research can support decision makers, but in order to reach the C-level, research results need to be explained in their language and habit of thought. The problems and issues should be linked to their main business-driven areas of concern, for instance by showing that insecurity may affect the revenues or the organisation's imago. Also learning from past incidents may prove to be an important factor in getting the message across. Story telling of the real story and sharing the lessons learned may be very convincing. In some companies, the top level is aware of dangers coming, but in day-to-day business at the lower organisational levels there is still a constant struggle for budget and resources. As long as cyber security is not a key performance indicator, all budget and resource decisions have to be fought for.

Towards a culture of security

Changing the culture of an organisation is a challenging and time consuming process. It can be done, e.g., Alliander is working throughout the company on energy transition. The company aims to include privacy and security from the start of this process and not as an add-on at the end. However, it takes time to incorporate security at all levels of the organisation. Security should be built-in from the start in all processes, e.g. in the development and acquisition of material or services.

> Learning from past incidents and "story telling" may help to bring research results across to decision makers

Some members of the audience and the panel stated that the only way to really change the culture of security is a high public visibility of major incidents. There is no need for managers to invest additional resources for cyber security without larger scale incidents occurring which may potentially affect their operations as well.

Security is only worth to pay for if something goes badly wrong. Stuxnet has raised the awareness on security for cyber-physical systems a little, but on a smaller scale than the effect that 9/11 had on physical security measures.

More collaboration required

More collaboration between researchers and industry is necessary since the problem that we face is large and complex. For increased collaboration, a more abstract and common language is needed in order to exchange results more effectively, both within the research community, in the collaboration with industry, and in convincing the C-level.

The current status shows a wide variety of R&D approaches and results, no generally accepted good practices and even partly contradictory risk assessments. This makes it very hard for the decision maker in the board room and other decision-making units to act on these results.

Towards CRITIS 2013

Based on the results of the CRITIS12 panel discussion, the CRITIS 2013 programme will include many opportunities for the research community and CI stakeholders to interact closely.

Critical Information Infrastructure Protection and Resilience in the ICT Sector

Book published by IGI Global: Editors Paul Theron and Sandro Bologna

Overview CIIP in EU

Over the past years, the rise of our interconnected, interdependent society combined with terrorist attacks and natural disasters has posed new challenges to the community of critical infrastructure protection.

Resilience has become an important dimension of the critical infrastructure protection mission, and a key element of the value proposition for partnership with the government because it recognises both the need for security and the reliability of business operations.

Resilience is not a specific, easily definable term. Several definitions can be found in a wide range of literature, addressing all manner of public and private concerns.

Situation in UK

The UK Cabinet is very sensible in terms of resilience. Within their Critical Infrastructure Resilience Programme, they defined resilience as "the ability of a system or organisation to withstand and recover from adversity".

ENISA

In line with this approach, but going in more details towards a technical approach, rather than an organisational one, is the approach followed by ENISA. ENISA has, in fact, defined resilience as "The ability of a system to provide & maintain an acceptable level of service in the face of faults (unintentional, intentional, or naturally caused) affecting normal operation." At the present the European Commission through ENISA is very active in establishing scientific foundations for the concept of resilience applied to Critical Information Infrastructures (CII), and also possible metrics [1], [2].

Enhancing the resiliency of critical infrastructure can be achieved through the appropriate combination of security measures to address intentional and accidental incidents; business continuity practices to deal with disruptions and ensure the continuation of essential services; and emergency management planning to ensure adequate response procedures are in place to deal with unforeseen disruptions and natural disasters.

European Parliament and Commission

On 30 March 2009, the European Commission adopted a Communication to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Region, entitled "Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience", followed by another Communication on 31 March 2011 ("CIIP Communication" from now on) [3], [4].

The CIIP Communication represents an important element of the Commission's strategy in the field of Network and Information Security. It addresses the commonly perceived need to raise the level of preparedness and resilience of critical ICT infrastructures across the European Union, as the first line of defence against cyber-threats – complementarily to the policies for fighting cyber-crime and cyber-terrorism and in coherence with international efforts in this area.

The high dependence on CIIs, their cross-border interconnectedness and interdependencies with other infrastructures, as well as the vulnerabilities and threats they face raise the need to address their security and resilience in a systemic perspective as the frontline of defence against failures and attacks.

Co-Editors of the book:

Critical Information Infrastructure Protection and Resilience in the ICT Sector

Paul Theron

and

Sandro Bologna
s.bologna@infrastrutturecritiche.it

Scope of the Book

The Book "Critical Information Infrastructure Protection and Resilience in the ICT Sector", edited by Paul Theron and Sandro Bologna, and published by IGI Global, [5] aims to address the following points:

How do we understand the concept of Resilience in the ICT sector? What is the state of play in the domain of Critical Information Infrastructure Protection and Emergency Preparation? How can states and telecommunication operators, and all their partners improve the protection and resilience of complex critical infrastructures?

Book Overview

This book seeks to present some of the views held in the scientific and professional community about Resilience in the ICT sector, Major Incident Analysis and Lesson Learning, Critical Information Infrastructure Protection and Emergency Preparation, Interdependencies Modelling and Risk Analysis in a context of uncertainty and lack of data about potential threats and hazards. These views are drawn from the most recent research work. It seeks delivering authentic pictures of the current state of play, for the benefit of academia, governments, Telcos, and other organisation engaged or interested in CIIP, Resilience and Emergency Preparedness in the ICT sector. It is organised in three Sections, with the intent to present three perspectives over CIIP and Resilience:

Section 1 focuses on general aspects of the subject: threats and incidents, lessons from major crises that help to understand the dynamics of these phenomena and of the resilient response of stakeholders, the European CIIP Governance Framework and a definition of resilience, and the socio-economic aspects of CIIP.

Section 2 focuses on the central question of mutual dependencies analysis of which it provides a variety of views to show that new methodological and technological developments are still much needed.

Section 3 draws a panorama of the issues of trust and co-operation among stakeholders in the European CIIP programme and shows that such a programme requires a shift from corporate strategies to collective, cross-sector and cross-border governance. It shows also that such a shift will have impacts on standardisation within bodies such as ISO TC223 and CEN TC391 or ETSI and even NATO.

References

[1] ENISA Activities www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents%20reporting/metrics/metrics

[2] "Enabling and Managing end-to-end Resilience", ENISA Report, 2011, www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/e2eres

[3] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions of 30 March 2009 on Critical Information Infrastructure Protection – "Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience" [COM(2009) 149 final]

[4] Communication of 31 March 2011 from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection 'Achievements and next steps: towards global cybersecurity' [COM(2011) 163 final]

[5] Paul Theron, Sandro Bologna, "Critical Information Infrastructure Protection and Resilience in the ICT Sector, IGI Global 2013, www.igi-global.com/book/critical-information-infrastructure-protection-resilience/70773

EFFECTIVE SURVEILLANCE FOR HOME-LAND SECURITY

Balancing Technology and Social Issues – Book published by CRC Press

As the debate continues to swirl around the most appropriate solution(s) to Homeland Security scenarios, one common denominator lingers at the forefront of every method: proactive behaviour. Many books before this one have illustrated that a 'reactive' approach will not suffice; however, increases in technology are changing the way Homeland Security experts and patrons alike are defining 'proactive behaviours'. As legislation outlines appropriate regulations regarding surveillance, advancements in tracking technologies have reconsidered and redefined the appropriate privacy parameters , as: high-resolution satellite imaging, people scanning, Radio-frequency Identification (RFID) tagging, intelligent multimedia (audio–video) analytics, web surfing monitoring, etc... Recognising the need to draw attention to the frequently overlooked aspects of advanced surveillance, this book addresses the 'holes' in existing literature between technology developments and the sensitive issues related to their social impact.

The book, consisting of 21 chapters, has been written by experts in different aspects of Homeland Security. These chapters deal with three broad areas: (i) surveillance technologies; (ii) legislative and social aspects of Homeland Security operations; and (iii) advanced issues on surveillance operations, such as advanced analytics and multimodal surveillance. A novel scheme is applied, which is unusual in technical books on security and surveillance, as shortly illustrated in the following.

Part I – "Surveillance and Society" is not dedicated to technological aspects, focusing instead on the societal dimension of surveillance; this choice stresses the importance of societal acceptability as a precondition to any surveillance system. Beginning with that general depiction, Part II- "Physical and Cyber Surveillance" focuses on advanced technologies for surveillance. Most of those developing technologies are part of a framework, whose aim is to move from a simple collection and storage of information toward proactive systems, able to fuse several information sources, in order to detect relevant events in their early incipient phase. Such a trend leads to security information management systems that are increasingly smart. Finally, some relevant applications of surveillance systems, used in the framework of Homeland Security, are collected in Part III- "Technologies for Homeland Security".

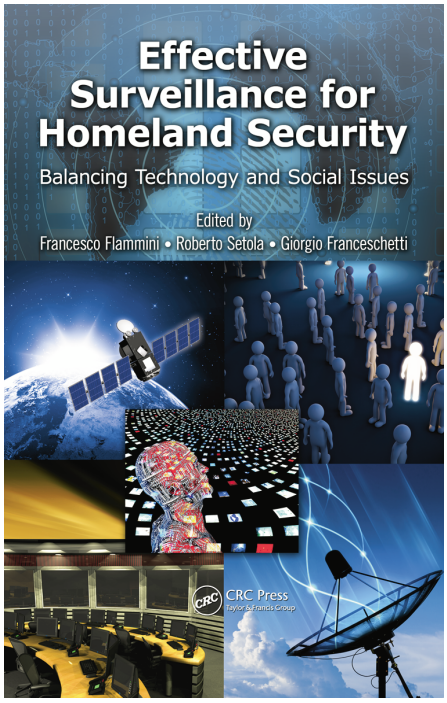
> This book applies a novel scheme that is unusual in technical books on security and surveillance.

These real world case studies are intended to show how innovative technologies can be used to effectively improve the security of sensitive areas, without violating the rights of the involved people. For example, the authors of Chapter 15 present the details of the project GEPSUS (Geographical information processing for Environmental Pollution-related Security within Urban Scale environments) to demonstrate how GEOgraphical INTelligence (GEOINT) technologies can significantly help in designing solutions for enhancing the security of humans and infrastructures against human-launched or natural disasters.

Intended Audience for the Book

Combining inputs from Homeland Security experts all over the world, this book provides a rare glimpse into the on-going battle between technological advances and personal privacy.

While related literature has succeeded in acknowledging the struggle, few have provided such in-depth analysis of the issues **AND** delivered



Editors :

Francesco Flammini

e-mail: **Francesco.Flammini@ansaldo-sts.com**

Roberto Setola

e-mail: **r.setola@unicampus.it**

Giorgio Franceschetti

e-mail: **gfrance@unina.it**

"Effective Surveillance for Homeland Security: Balancing Technology and Social Issues",

CRC Press, May 2013

practical solutions. For a better discussion of this point, we refer to Chapter 5 of the book, whose authors provide good example of enforcing the required operations while preserving and managing privacy information (understanding and relaying the issue to the reader) through the application of a practical solution.

> While related literature has succeeded in acknowledging the struggle, few have provided such in-depth analysis of the issues AND delivered practical solutions.

The authors propose a privacy-preserving video surveillance system, which can help to protect privacy-sensitive information by using a rate-distortion optimised data-hiding scheme; this scheme allows retrieval of private data with a robust, yet anonymous authentication module, which utilises encrypted biometric signals. This, and many other examples in the book, leaves the reader feeling challenged, motivated, and hopeful about the prospective landscape of the Homeland Security environment.

"Effective Surveillance for Homeland Security" is a valuable resource for engineers, researchers and policy-makers, working in the area of Homeland Security solution design and development; law enforcing agencies (local, state, federal, international); operators of critical infrastructures; faculty members and graduate students in schools and universities; and similar other categories of potential readers.

CRITIS 2013: Register now!

CRITIS 2013 will take place in Amsterdam, The Netherlands, September 16-18.
Key topic: Resilience of Smart Cities.

Register now: CRITIS 2013!

The CRITIS conference series will continue with the 8th International Workshop on Critical Information Infrastructures Security in Amsterdam, The Netherlands, September 16–18, 2013.

First day: Innovation

The CRITIS 2013 conference on Critical Information Infrastructures Security continues a tradition of presenting innovative research and exploring new challenges for the protection of critical information-based infrastructures. This years' focus is on the challenges the resilience of smart cities, a topic that will be highlighted by thought provoking and visionary keynote speeches on the first afternoon and by conference papers. Some attention will be given as well to 12.5 years of CIP and CIP R&D in The Netherlands and.

Second Day

The second day of CRITIS 2013 will focus on the dialogue between the critical infrastructure operators and stakeholders of government and industry and research. The agenda of that day will stimulate the infrastructure stakeholders to present their short and long term R&D needs. The academic and applied research community will be stimulated to discuss, sketch and collaboratively seek for solution directions to address these needs along the set of these needs and by providing original research contributions which aim to bridge existing gaps between R&D and operational needs ('market').

Third Day: Young CRITIS

The third day program addresses C(I)IP R&D advancements and Young CRITIS, an initiative to build-up of a (virtual) strong community of young researchers in this field. A special LinkedIn group has been established where young researchers (and others) can ask questions, ask for pointers to existing R&D, approaches, and so forth. Build the international CIP and Resilience of Smart Cities community by joining the special LinkedIn Group Young CRITIS now!

CRITIS 2013 invites critical (information) infrastructure protection (CIP/CIIP) end-users (government, operators, industry, etc.) and the CIP/CIIP-related (academic) research communities and disciplines. CRITIS encourages discussions between all types of stakeholders and multi-disciplinary approaches to relevant CIP problems.

> With the eight edition, CRITIS has been established as "the European C(I)IP Conference": 57 submissions were at least from three experts evaluated. The best papers will be presented at CRITIS 2013.

Registration opens mid of June and will be possible only till September 1st (logistic reasons). The conference program has been published at the CRITIS 2013 website www.critis2013.nl .

See you at CRITIS in Amsterdam!

Eric Luiijf , Annemarie Zielstra
and their local host team by TNO:

- Marieke Klaver
- Imelda van de Voorde
- Yennie Lam

Eric Luiijf

Eric Luiijf is Principal Consultant Critical (Information) Infrastructure Protection and Cyber Operations at TNO, The Hague, The Netherlands.

Local co-chair CRITIS 2013.

e-mail: **eric.luiijf@tno.nl**

Register at

www.critis2013.nl

Links

ECN home page http://www.ciprnet.eu

Forthcoming conferences and workshops

CRITIS 2013 16.-18.9.2013 Amsterdam, The Netherlands
http://www.critis.nl

Future Security 2013 17.-19.9.2013 Berlin, Germany
http://www.emi.fraunhofer.de/veranstaltungen/details/id/4/

The Grand Conference 5.11.2013 Amsterdam, The Netherlands
http://www.thegrandconference.org

CIPRE 12.-13.2.2014 London, UK
http://www.cipre-expo.com

Recent conferences and workshops

CRI!SE 28.5.2013 Weimar, Germany
http://www.bbk.bund.de/SharedDocs/Termine/BBK/DE/2013/CRISE_Fachtagung_Weimar.html

ISCRAM 2013 12.-15.5.2013 Baden-Baden, Germany
http://www.iosb.fraunhofer.de/servlet/is/35401/

ANDROID conference October 2012 Estonia
http://www.disaster-resilience.salford.ac.uk

Exhibitions

Interschutz 2015 8.-13.6.2015 Hannover ,Germany
http://www.interschutz.de/86385

Project home pages

FP7 CIPRNet http://www.ciprnet.eu
FP7 ValueSec http://www.valuesec.eu

Interesting Downloads

European Network and Information Security Agency www.ENISA.eu publishes reports and other material on "Resilience of Networks and Services and Critical Information Infrastructure Protection"
www.enisa.europa.eu/activities/Resilience-and-CIIP

Centre for Protection of National Infrastructure UK, www.cpni.gov.uk has a variety of interesting material available e.g.:
www.cpni.gov.uk/advice/cyber