

European CIIP Newsletter

July 14 – October 14, Volume 8, Number 2

ECN

Contents:

Editorial

EU Projects
INTACT and PREDICT

EU SLO Project

EU Exercises and CIP
Scenarios

Data Management and
Information Sharing in
CIPRNet DSS

Cyber Storm

New Books Netonets

CIPRNet Master Class EU

CRITIS 2014



> About ECN

ECN is coordinated 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 to be published can be submitted to:
editor@ciip-newsletter.org

>Questions to the editors about articles 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 Luijff, TNO, eric.luijff@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	Community Building: Why is it that important, and what do we get? by Gregorio D'Agostino and Bernhard Hämmerli	5
-------	--	---

European Activities

EU SLO Project	The Security Liaison Officer as a part of the European Critical Infrastructure Protection Strategy by Maria Carla De Maggio	7
INTACT EU Project	EU project on the Impact of Extreme Weather on Critical Infrastructures by Rene Willems	11
PREDICT EU Project	PREparing for the Domino effect In Crisis siTuations by Dominique Sérafin	13

Country Specific Issues

no		No Page
----	--	------------

Method and Models

EU Exercises and CIP Scenarios	CIP Scenarios: Lessons learnt from EU Exercises by Marianthi Theocharidou	15
Information Sha- ring and Data Management	Data management and Information sharing in CIPRNet DSS by Alberto Tofani, Antonio De Nicola, Antonio Di Pietro, Maurizio Pollino and Luigi La Porta	19

About Associations

Cyber Storm	Cyber Storm Association by Bernhard Tellenbach	23
-------------	---	----

Books on C(I)IP

Netonets	Netonets: Critical Infrastructures as Network of Networks by Gregorio D'Agostino	25
----------	---	----

Conferences 2014

CIP Master Class	Experiences from the CIPRNet Master Class on Modelling, Simulation and Analysis of Critical Infrastructures (CI) by Elena Polykarpou	29
CRITIS 2014	CRITIS 2014 Conference: 9th International Conference on Critical Information Infrastructures Security by Elias Kyriakides	33

Links

Where to find:	<ul style="list-style-type: none">• Forthcoming conferences and workshops• Recent conferences and workshops• Exhibitions• Project home pages• Selected Download Material	35
----------------	--	----

Editorial: Community Building: Why is it that important, and what do we get?

In CIP we need local communities, national, European and worldwide communities. Also it is important that all these communities remain in exchange. And what is the role of journals and books?

The world of research is changing very rapidly from huge governmental after war projects like Manhattan (nuclear bomb) and Apollo (Space, reaching moon) project and peaceful use of nuclear energy to dynamically allocated specific aim projects with dynamically changing teams and, of course, still military projects. In line with this tendency, European countries established high level scientific institution supported with large financial budgets.

Meanwhile we saw a huge increase in the publications far beyond the genuine need for sharing results within the scientific community. This is basically due to the criteria applied for fund allocation and for personal scientific careers that are mostly targeted on literature production and participation to official events.

As a new field of applied research, Critical Infrastructure Protection (CIP) had no community, no allocated budget, no funding schema and no publication channel dedicated to this terrific strategic subject. Initial important work like the paper by Rinaldi et al. – "Identifying, understanding, and analysing critical infrastructure interdependencies, Control Systems, IEEE, 2001" – appeared in a journal on "Control Systems" because dedicated CIP journals were lacking.

After five years of an ad hoc expert group promoting CIP, the European Commission released a Communication of December 12, 2006 on a European Programme for Critical Infrastructure Protection [COM(2006) 786 final – Official Journal C 126 of 7.6.2007] and two years thereafter the EU started to rule the field on legal level by the Directive of Dec 2008.

CIP Newsletter were made available in the US (CIP Report) and in the EU (European CI(I)IP Newsletter from 2002 respectively 2006 and more followed.

National efforts in CIP (conferences and exercises) started late 90ies and have been growing with emerging awareness.

The scarcity of literature has been recognized and we are happy to observe today more than a dozen available books and even more will be edited in the next period. CIP Journals from Elsevier and Inderscience are available, and IEEE provides a journal on dependability. Still, CIP issues are being discussed in journals dedicated to other more classical topics, but this is about to change.

The dissemination framework of CIP is complemented by international conferences such as CRITIS, the International Conference on Critical Infrastructure (CRIS), and recently CIPRE.

Although CIP is of public interest, some achievements have to be kept secret because of national defense, Transparency, otherwise typical in science, is not always first priority in the field of CIP. NISAC in the US represents a compromise between the need for secrets and synergic capability of open scientific communities. The concept of EISAC might be good for Europe as well.

And finally, we are happy that the CIP community, besides researchers, includes also stakeholders like policy makers, suppliers and operators. Their trustful collaboration is a prerequisite for leveraging the R&D investments made in CIP.

We are very happy to announce CRITIS'14 with over seventy submissions on the next page, and offering a coming together of the CIP community.

www.critis2014.org

Enjoy reading this issue of the ECN!

PS: Authors willing to contribute to future ECN issues are very welcome, just drop an email.



Gregorio D'Agostino

Gregorio is a theoretical physicist that received his "laurea" and PhD in Physics at University of Rome "La Sapienza".

email: gregorio.dagostino@enea.it
Phone +39 06 30484776
web: gordion.casaccia.enea.it



Bernhard M. Hämmerli

is Professor at Lucerne University of Applied Sciences and Gjøvik University, CEO of Acris GmbH

e-mail: bmhaemmerli@acris.ch
He is ECN Editor in Chief

Call for Participation

CRITIS 2014

9th International Conference on
Critical Information Infrastructures Security
October 13-15, 2014, Limassol, Cyprus

www.critis2014.org

(see last article
and last page)

The Security Liaison Officer as a part of the European Critical Infrastructure Protection Strategy

The Directive 114/2008/EC is the starting point for a European strategy for the Critical Infrastructure Protection. The SLO project aims to overcome the regulatory gap related to the profile of the Security Liaison Officer.

The conference on “Security Liaison Officer as a part of Critical Infrastructure Protection strategy”, held the 25th June at the Italian Chamber of Deputies in Rome, has been the final act of the European project “SLO – Security Liaison Officer”. The project, co-funded by the “Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks Programme” (CIPS) of the DG Home Affairs of the European Commission, is ending after a 14-month activity. The project has been developed with the cooperation of two main partners, Complex Systems and Security Lab of University Campus Bio-Medico of Rome (Coordinator), supervised by Prof. Roberto Setola, and the Romanian Association for Critical Infrastructures and Services Protection (ARPIC), with the support of the Italian Association of Critical Infrastructure Experts (AIC), BC Manager, ASIS International Chapter Italy, and Transelectrica, as associate partners.

The Security Liaison Officer figure is mentioned in the Article 6 of the Council Directive 2008/114/EC as the contact point between the Critical Infrastructure operators and the public authorities in charge for Critical Infrastructure protection. As stated in the Directive “Security Liaison Officers (SLO) should be identified for all designated ECIs in order to facilitate cooperation and communication with relevant national critical infrastructure protection authorities. With a view to avoiding unnecessary work and duplication, each Member State should first assess whether the owners/operators of designated ECIs already possess a Security Liaison Officer or equivalent. Where such a Security Liaison Officer does not exist, each Member State should take the necessary steps to make sure that appropriate measures are put in

place. It is up to each Member State to decide on the most appropriate form of action with regard to the designation of Security Liaison Officers”. The Directive overlooks many aspects which should characterize the figure of the SLO, namely his background, his tasks and responsibilities, his position inside the company, his role in a critical situation (before, during, or after a crisis), and his relationships with the other European Security Liaison Officers.

The project, aiming to define a common framework regarding the Security Liaison Officer duties, collected the points of view of several countries, in order to achieve a possible standardization of the SLO profile. This research has been carried out through the data acquisition by means of three different sources: review of the most popular standards and regulations on the subject, acquisition of specific information about actual facts and aspects via online questionnaires and interviews, elicitation of ideas via brainstorming activities during workshop cafés.

The data collection from open-sources and most popular standards has revealed the diversity of ideas regarding the Security Liaison Officer figure. While a new Romanian resolution is very clear regarding the role and the background (military) of the SLO, other European Countries have a different implementation of the security-related roles in their organizations, whether recognized as critical or not, sometimes having a clear implementation of a profile similar or corresponding to the SLO.

To find out the opinions of people involved in the security issues, four different online questionnaires have been devised, depending on the role of the responder (Public Authority, Chief Security Officer, Staff Security Officer, Academia).

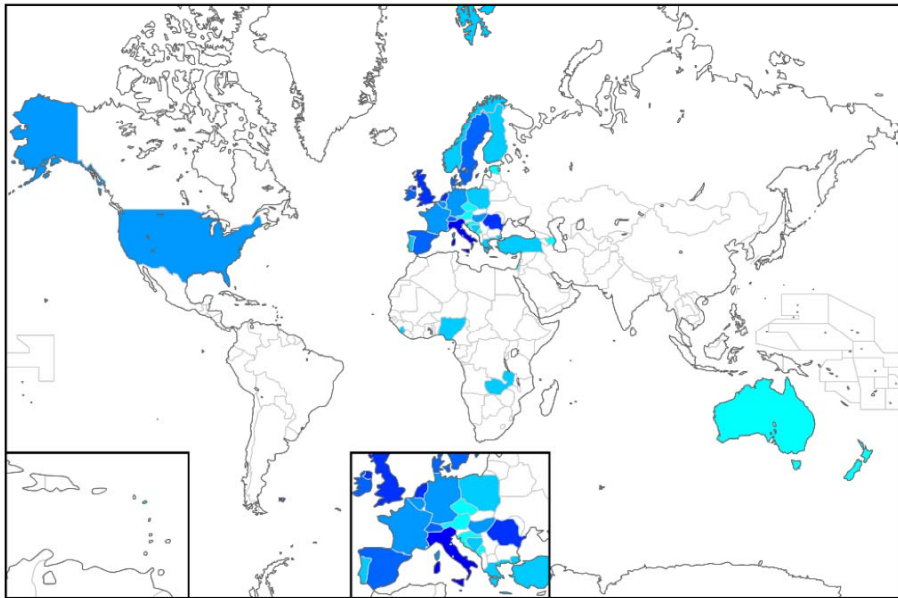


Maria Carla De Maggio

She belongs to the Complex Systems and Security Laboratory of the University Campus Bio-Medico of Rome since 2009, after a working period as junior consultant for a company involved in several European Projects in the ICT, e-inclusion and ethics areas. She currently manages several National and European projects of which the group is coordinator or partner, in both scientific and administrative aspects.

Eng. De Maggio holds a Master Degree in Biomedical Engineering (2007) and a Post Graduate Master in Homeland Security (2011), both from the University Campus Bio-Medico of Rome. She is now studying for a Degree in Economics.

email: m.demaggio@unicampus.it

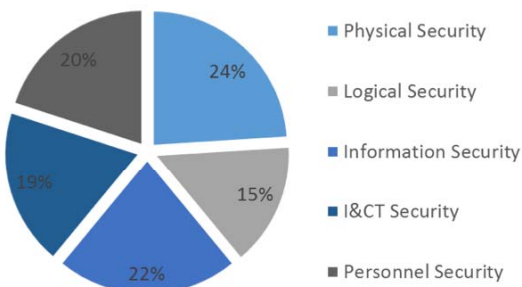


Participation to the SLO survey.

In the period from October 2013 to May 2014, more than 200 questionnaires have been collected, from 34 different countries (19 Member States and 15 non-Member States).

The main objective of the SLO survey is to perform a snapshot of the current organizations' security context and to identify the most relevant trends.

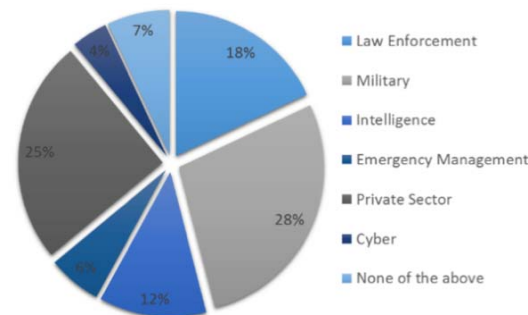
From the collected data, it appears that the security budget for the next five years will be aligned with those experienced in the past. Given the current budgetary constraints within the EU and abroad, this continuing upward trend of funding is further evidence of the sizeable attention that security is garnering. This increase in attention towards security is further emphasized by the data showing an incremental growth in the number of persons involved within the security division.



CSO budget allocation.

Considering the different dimensions of security, the most important aspect results to be personnel security: nearly a quarter of respondents considered personnel security as the most essential domain, stressing the utmost importance attributed to the person-

nel inside a company (a large relevance is also attributed to safety).



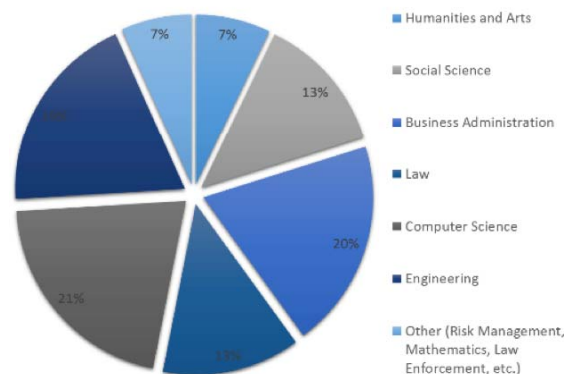
Background of CSOs.

However, the collected data shows that in the last five years there was a considerable boost in the security standards for the physical and cyber security domains, while personnel security standards received much less attention.

The result is a balanced approach towards security, further confirmed by the CSO category answers regarding resource allocation, as showed in the figure.

Another interesting aspect analysed is the background of the personnel involved in security. Indeed, even if 46% of the CSOs have a

background in the law enforcement or military fields, the actual composition of a security team is more articulated with a prevalence of competence in Computer Science, Business Administration and Engineering. This stresses the



Background of Security staff.

importance to complement the education with managerial and process-based competencies.

The SLO project survey shows an increased attention through all aspects of the security in the Critical Infrastructure organizations

Going more in-depth on the aspects directly related to the Council Directive 114/08/EC, there is only moderate familiarity with it (less than 50% of CSOs have knowledge of the EPCIP programme). Even more resounding is our analysis regarding the CIWIN network, which was evaluated as "unknown", "not relevant" or simply unused by the majority of responders. This limited knowledge regarding the EPCIP programme represents a partial contradiction with respect to the conclusions of the European Commission Working Document SWD(2013)318. This discrepancy can be partially explained taking into account that our questionnaires were mainly oriented toward private sector, while the primary customers for the European Commission are the governments (in fact the PAs involved in the questionnaire have a discrete knowledge of the programme).

The SLO questionnaire results have been completed and deepened by several interviews with Critical Infrastructures Security Managers and Public Authorities, which common request is for a regulatory standardization of the Security Liaison Officer professional profile, in order to establish common and cogent guidelines in case of critical situations which can involve European Critical Infrastructures.

A further important mean for elicit

information and opinions from security experts has been the organization of three Workshop Cafés in three different European Countries (Bucharest, Romania – October 2013, Rome, Italy – February 2014, The Hague, The Netherlands – May 2014) in order to collect opinions reflecting Member States' different regulations and cultural business schemes.

The workshop cafés (WSCs) focused on three separate elements of the SLO profile: Skills, Role and Tasks. These elements were analyzed during brainstorming activities and resulted in numerous innovative ideas and future elements for consideration. These results have been achieved thanks to the participation in the WSCs from about 100 Security experts from Academia, Public Authorities and Critical Infrastructure Companies from different countries.

According to most of the WSC attendees, the SLO must have the function of connecting not only structures, but also tasks and persons, playing a fundamental role to integrate the company activities and coordinate the personnel.

He/she must be able to communicate to all directions within the company and to connect all the divisions/departments of the company. Additionally, they must also be in contact with the other Security Liaison Officers, authorities and law enforcement officers. His/her main role must be, therefore, a link between the organization and both the National and European Public Authorities and other Critical Infrastructures.

To carry out these tasks, the SLO must be a person with good communication skills, able to motivate people, and in particular have a strong commitment from the top management. In this perspective,

being primarily a coordinator/facilitator able to effectively communicate inside and outside the organization, the SLO needs to be at a top management level into the company, referring preferably to the company board of directors. The SLO should have experience in management, though not necessarily former experience in the law-enforcement or military field. However, the SLO should have a wide competence on his own organization and his sector, along with knowledge regarding other sectors, technologies and legislations in security matters, and a mandatory continuing training process should be aligned with context changes. He/she must have a security clearance and it is preferable if he/she also had some professional certificate or adequate academic degree. During the WSCs, also novel vulnerabilities stemming from the implementation of dramatically differing policies, particularly difficult for companies operating in many Member States, were analyzed.



The results of the data acquisition has been integrated during the gap analysis phase, where all the information has been merged in order to define common features for the SLO and for his relationships with

the Public Authorities and the other European SLOs.

The first evidence coming from the SLO project data is that the SLO figure is considered, from both CI operators and PA, an effective element to manage the complex relationships existing between CI and PA, where the SLO could allow them to use a common vocabulary, simplify the procedures and construct more effective strategies and solutions.

This is also due to the change of paradigm of the security, that now deals with service continuity, company reputation, management of crisis situations, etc. This imposes to have a multi-disciplinary security team whose numerical dimension has also continued to increase in the last years. Consequently our data illustrates the existence of a strong motivation to establish a standard profile of the SLO figure, and to introduce a more cogent and specific regulation on the subject to allow the cooperation of Security Liaison Officers.

The SLO should have visibility on all security aspects and a very good knowledge of the organization.

From the amount of data collected during the project, it emerged that the term "OFFICER" is quite inappropriate. Several experts expressed some concerns about the term because it could apply a "military-oriented" connotation that might induce a wrong bias with respect to his/her essential role. Indeed the SLO is primarily a "LIAISON", to serve as an interface between the CI organization the PA or other operators. To effectively perform his/her work, the SLO should be familiar with all the threats that are impacting the organization. Hence it is a largely shared opinion to appoint a person already within the company having, then, a deep knowledge of the corporate processes and activities.

However, a mandatory continuing training process should be aligned with contextual changes and an adequate academic background is more and more required.

The majority of data identified a good collocation of the SLO in the Security Department or as member of the Board of Directors.

There is an important debate



regarding the opportunity for the existing CSOs to also serve as the SLO. This is because there are overlapping knowledge/skillsets between these two professional profiles. However, our data stressed that it should be preferable to have two separate professional figures.

To operate effectively, also the Public Authorities should introduce figure similar to the SLO in order to facilitate the information exchange.

A final consideration is on the word "SECURITY" in the SLO label. From the project, the need emerges to mandatorily consider All-Hazard approaches to guarantee the

capability of the different infrastructures to supply their essential services to the citizens. With this vision in mind, it appears more suitable to use the meaning of the Italian term "SICUREZZA", which embraces a holistic vision of both the accidental and malicious threats, hence Safety & Security.

It is highly desirable for the SLO figure to have a unified framework facilitating the definition of his/her role inside a company, for that which concerns his/her relationships with PA and other CIs, and to facilitate information sharing. In this way, the PA can participate in the process of

designating a SLO inside CIs releasing guidelines and criteria for eligibility.

A synthesis of the collected data and results can be found in the Final Report of the SLO project, released during the Final Conference of the project that can be now downloaded at www.coseritylab.it. More information and results about the project can be requested to the project coordinator mailing to contacts@coseritylab.it.



On 1st of May 2014, a new EU project started on the Impact of Extreme Weather on Critical Infrastructures

Critical Infrastructures and Extreme Weather

Resilience of Critical Infrastructure (CI) to Extreme Weather Events (EWE) is one of the most demanding challenges for both government and society. Extreme Weather (EW) is a key phenomenon that can cause severe threats to the well-functioning of CI. The effects of various levels of EW on CI will vary throughout Europe. These effects are witnessed through changes in seasonal means and extreme value frequencies of regional extreme temperatures (high and low), humidity (high and low), extreme or prolonged precipitation (rain, fog, snow, ice, etc.) or prolonged lack thereof (drought), extreme wind or lack of wind, and thunderstorms. The increased frequency and intensity of EW can cause events such as flooding, drought, ice formation, wild fires etc. which present a range of complex challenges to the operational resilience of CI.

The Challenge: Planning for Extreme Weather (EW) and economic life time 50+ years!

The economic and societal relevance of the dependability and resilience of CI is obvious: infrastructure malfunctioning and outages can have far reaching consequences and impacts. The cost of developing and maintaining CI is capital intensive if they are expected to have a realistic functional and economic life (i.e. 50+ years). Hence, future EW has to be taken into account when considering protective measures, mitigation measures and adaption measures to reflect actual and predicted instances of CI failures.

The INTACT project

The INTACT project will address these challenges and bring together innovative and cutting edge

knowledge and experience in Europe in order to develop and demonstrate best practices in engineering, materials, construction, planning and designing protective measures as well as crisis response and recovery capabilities. All this will culminate in the INTACT Reference Guide, the decision support system that facilitates cross-disciplinary and cross-border data sharing and provides for a forum for evidence based policy formulation.

The objectives of the INTACT project are to:

- assess regionally differentiated risk throughout Europe associated with extreme weather;
- to identify and classify on a Europe wide basis CI and to assess the resilience of such CI to the impact of EWE;
- raise awareness of decision-makers and CI operators about the challenges (current and future) EW conditions may pose to their CI; and,
- identify potential measures and technologies to consider and implement, be it for planning, designing and protecting CI or for effectively preparing for crisis response and recovery.

Findings of the project will be accumulated in the INTACT Reference Guide. This guide will support decision makers and CI operators with best practices and methodological approaches to protect their CI against EWE

The INTACT project has been launched on May 01, 2014 and will deliver its final results in 2017. TNO is coordinator of the project consortium with eleven partners from eight countries: CMCC (IT), DELTARES (NL), FAC (IRE), DRAGADOS (SP), HR Wallingford (UK), PANTEIA (NL), NGI (NO), CSIC (SP), UN University (GE), Un Ulster (UK), VTT (FI)

INTACT receives funding from the European Union Seventh Framework Programme (FP7/2007-2013) under grant agreement n° FP7-SEC-2013-606799.



Rene Willems

Rene Willems holds a Master of Science form Eindhoven. He is Senior Policy Advisor Business and Network Development at Defence and Security of TNO in the Hague, The Netherlands.

Amongst others he was head of the division Operations Research and Business Management at TNO-FEL. He chaired the NATO RTO SAS Panel on Systems Analysis and Simulation.

He set up and acted as deputy director of the Hague Centre for Strategic Studies (HCSS), a TNO subsidiary.

He co-created and developed the Hague Security Delta (HSD), the Netherlands' national security cluster.

e-mail: rene.willems@tno.nl
Phone +31 888 66 3224



■ ICS 3C – ICS Cybersecurity Council Conference 2014

Wednesday, 1st October 2014 - Print Media Academy, Heidelberg, Germany

Join industry experts and ENISA (the European Union Agency for Network and Information Security) in a pan-European dialogue on ICS (Industrial Control Systems) Cybersecurity. High-quality presentations, lively discussions and hands-on-workshops address today's issues and tomorrow's solutions in securing industrial control systems and critical infrastructure. Depending on your interest you may focus on organisational or more technically oriented topics:

Track 'M': Management & Organisation

- Benefit from other sectors' expertise
- Gain first-hand insight into European policy-making (e.g. CERT, Certification)
- Address your requirements to vendors, policy makers and end users
- Shape the future European security landscape

Track 'O': Best Practices & Operation

- Learn about best practices for patch management, whitelisting, firewalls and data diodes
- Exchange know-how on cybersecurity issues
- Discuss the "real" solutions
- Leave with practical tools and techniques that you can immediately put into use in your organisation

Confirmed Speakers in alphabetical order:

Adrian Pauna, ENISA, Expert in Network & Information Security / Resilience and CIIP

Andrew Ginter, Waterfall Security Solutions, Vice President Industrial Security

Dimitris Mouzakis, Odyssey Consultants, Senior Information Security Consultant and an ISO 27001 Lead Auditor

Dr. Evangelos Ouzounis, ENISA, Head of ENISA Critical Information Infrastructure Protection (CIIP) and Resilience Unit

Franz Hoheiser, KAV (Major Healthcare Provider), Chief Information Security Officer; Vice President of Cyber Security Austria

Hartmut Manske, Merck, Head of Automation & Electrical Engineering & Services; NAMUR WG „Automation Security“

Herbert Schindelka, Wiener Stadtwerke Holding (Energy Supply and Public Transport Vienna), Chief Information Security Officer

Dr. Hubert Keller, Institute of Applied Computer Sciences, Karlsruhe Institute of Technology

Dr. Konstantinos Moulinos, ENISA, Expert in Network & Information Security / Resilience and CIIP

Marco Thorbrügge, ENISA, Head of Unit "Operational Security" / CERT

Peter Sieber, HIMA, NAMUR WG Automation Security and Member of DKE 931.1 (DIN)

Dr. Ragnar Schierholz, ABB, Head of Cyber Security Process Automation Division & BU Industry Solutions

Sinclair Koelemij, Honeywell Industrial IT Solutions, Technical Lead EMEA

Stefan Woronka, Siemens, Business Development Manager for Industrial Security Services

Thomas Walter, E.ON Nuclear Power, Process IT-Security Manager

Registration Fee:

We aim to establish a well-balanced audience of users, vendors, academia and policy-makers in order to ensure fruitful discussions.

Asset Owners / End-users, Policy Makers, Academia:

EUR 300,00 / 200,00*

System Vendors, Consultants, Service Providers:

EUR 1.000,00 / 700,00*

* Early Bird - until 30th Aug

PREDICT: PREparing for the Domino effect In Crisis situations

The goal of the FP7 PREDICT project is to provide a solution for dealing with cascading effects in multi-sectorial crisis situations.

The PREDICT project is a new research project of the FP7 security call topic SEC-2013.4.1-2: Better understanding of the cascading effect in crisis situations in order to improve future response and preparedness and contribute to lower damages and unfortunate consequences. The PREDICT project has started on April 1st 2014.

Abstract

PREDICT will provide a comprehensive solution for dealing with cascading effects in multi-sectorial crisis situations covering aspects of critical infrastructures. The PREDICT solution will be composed of the following three pillars: methodologies, models and software tools. Their integrated use will increase the awareness and understanding of cascading effects by crisis response organizations, enhances their preparedness and improves their response capability to respond in case of cascading failures.

PREDICT project will start from a deep analysis of recent cases (over 8500 incidents worldwide), which will be accompanied with scenarios of potential crisis. Project partners will set up a generic approach (common framework) to prevent or mitigate cascading effects which will be applied in selected cases agreed with end-users.

As modelling each phenomenon separately in a specific environment is not effective, PREDICT project will propose cohesive and comprehensive models of dependencies, cascading effects and common mode failure which will include causal relations, multi-sectorial infrastructure elements and environment parameters, as well as the human factor aspects.

PREDICT will deliver software tools bundled in PREDICT Incident Evolution Tool, which will consist of two core components: a Foresight and

Prediction Tool (for simulation of the evolution of cascading effect and impact on multi-sectorial dependencies) and a Decision-Support Tool (for determining the best course of action and to calculate the risk associated with them).

The high quality of the developed solutions will be assured by a consortium consisting of a number of experienced partners joining research, industrial (incl. SME), and end-users approaches. End-users will be deeply involved in PREDICT at three levels: as partners of the consortium (there are three end-users in the consortium), members of the Advisory Board, and representatives from relevant organisations across Europe invited to regular workshops.

Objectives

The PREDICT project aims at delivering a comprehensive solution (PREDICT solution) for dealing with cascading effects in multi-sectorial crisis situations covering aspects of critical infrastructures.

The PREDICT solution is composed of the following three pillars: methodologies, models and software tools, which – when used together – will increase the awareness and understanding of cascading effects in crisis situations. It will enhance the preparedness for such effects and improve the capability to respond of various levels (local, regional, national, international) decision makers in case of a crisis.



Dominique Sérafin

Dominique Sérafin (PREDICT project coordinator) is a business developer at CEA in the field of critical infrastructure protection. He is also an expert in the field of electromagnetic effects and their consequences.

e-mail: dominique.serafin@cea.fr

CEA, DAM, GRAMAT, F-46500
Gramat, France

The new methods and tools developed within the PREDICT project may reduce the negative impact of possible, future cascading effects and the improve planning of civil protection and crisis management operations. The PREDICT results will help lowering losses and damages in various fields, including economic or social safety and security. In order to bring this new quality into the cascading effects and crisis management domain, the proposed project will achieve the following detailed operational and technical objectives:

1- Gather and analyse available domain knowledge (e.g. historical data, crisis situation scenarios, policies, and procedures, expert knowledge) in order to create a solid, empirically proven background for the project and explore newly discovered information on cascading effects. Carrying out extensive and detailed analyses will enable investigating currently known and identifying new triggers (originating incidents, purpose acts or natural disasters) of cascading effects in crisis situations. Moreover, taking into consideration dependencies among various interconnected critical infrastructure sector elements and other not considered to be critical under existing policies, together with such triggers will help to determine probable cascade paths. Cascade paths (possible, different chain of events triggered by a single incident or act) will be used to study the influence of the crisis incidents, cascading through specific components of the dependent system (different sectors, products, services etc.). The gathered knowledge will also help identifying and measuring the strongest relationships, assessing threats, risks and magnitude of possible impact associated with the cascading effects and taking into account cross-border effect.

2- Develop a common framework that will be an organised set of definitions, methodologies, scenarios, typologies, best practices etc., building a common base for each specific PREDICT solution end-user, but also for cooperation of various actors. The common framework for understanding cascading effect will gather and structure all of the factors affecting cascading effect and results of the carried analysis. This framework will be also used to define a set of quantitative and qualitative

metrics and indicators for measuring the influence of cascading effect, taking into account econometric information about value of goods and services.

3- Create models of cascading effects and interdependencies being a structured and formal way of describing such effects. These models will include causal relations, multi-sectorial infrastructure elements and environment parameters and possible human influence (human factor) on the state of crisis situation. Moreover, they will identify the key points in the incident evolution where decisions are needed, and the need for specific dependency and cascading risk information from stakeholders. These models also need to identify the type of decisions required, including preventive and preparation decisions. Executable versions of such models will be used for cascading effect simulation purposes.

4- Develop a suite of software tools for the simulation of cascading effects, decision support and creating collaborative expert networks and personnel training. These tools will help the PREDICT solution end-users to introduce new scenarios, simulate them and assess the potential decision-makers procedures in terms of their efficiency and effectiveness during a crisis. Continuous evaluation of the PREDICT solution outputs will be ensured by a dedicated expert network support tool. The developed suite of tools will be used in both preparedness and reaction phase of a crisis, allowing extensive virtual trainings and near real-time analysis of the situation. The developed tools will be suitable for assessing vulnerability of contingency plans, foreseeing consequences of complex crisis situations and determining the preconditions for failure of critical infrastructure.

5- Validate the solution through running simulations based on existing and developed cascading effects scenarios and using the developed models and tools. Such simulations will take into account infrastructure elements and relationships between them, environmental conditions, economic parameters, human behaviour and many other factors directly or indirectly affecting the course of the crisis situation. These simulations will be used to perform models behaviour test, which aim at comparing the simulation-generated

states of crisis situation with the observed reference behaviour. This will ensure the validity of developed solutions and help to improve results of the project. Moreover, such simulation might be used to generate a set of different, possible cascading effect scenarios. Due to a close cooperation with potential end-users, the PREDICT solution is considered to be deployed for them, for testing purposes and possible operational use.

6- Disseminate project results and build appropriate liaisons among various project stakeholders starting from end-users involved in the project (at various levels), members of Advisory Board, other end-users' representatives (five workshops will be organised with end-users external to the project), as well as general public. Moreover, the project results will be presented on forums and conferences related to crisis management and critical infrastructure topics. Additionally, the consortium will build connections between the PREDICT project and other, related initiatives, projects and programmes.

The Partners

CEA (France), ITI (Poland), Fraunhofer (Germany), THALES (France), CEIS (Belgium), TNO (The Netherlands), VTT (Finland), VRZH (The Netherlands), SYKE (Finland), UIC (France), TRT-NL (The Netherlands).

If you would like to know more about PREDICT please visit regularly our website at www.predict-project.eu

"Any publicity made by the beneficiaries in respect of the project, in whatever form and on or by whatever medium, must specify that it reflects only the author's views and that the [the Union] [Euratom] is not liable for any use that may be made of the information contained therein."

"PREDICT has received funding from the European Union's Seventh Framework Programme for research; technological development and demonstration under grant agreement no 607697".

CIP Scenarios: Lessons learnt from EU Exercises

In the CIPRNet project, we explore how to design a threat scenario for CIP.

On the 19-20th May 2014, CIP operators from the Energy, Transport, ICT and Water sectors met in Ispra (Italy) for the 2nd ERNCIP Operators' Workshop, organized by the European Reference Network for Critical Infrastructure Protection (ERNCIP) [1].

Critical Infrastructure operators highlight the need for CIP exercises based on threat scenarios.

Operators highlighted the need for templates of **scenario-based exercises** so as to exercise on hypothetical scenarios where practical decisions are needed. Exercises at national and EU wide scale, based on common threat scenarios, would be needed. Moreover, modelling efforts could drive the development of scenarios to be used for analysing possible cascading effects. While cost and confidentiality are a concern, operators value the opportunity to test their people and systems and to discover problems.

Scenarios in CIPRNet

The CIPRNet project [2] currently designs such scenarios in order to develop, test and train users on the novel capabilities offered by the project. An example scenario is a flood-related, cross-border emergency in a densely populated region of the border between The Netherlands and Germany. In order to design the scenario, existing approaches were reviewed.

While pure CIP exercises on an EU level are quite rare, several exercises are performed annually under DG-ECHO's civil protection mechanism [3]. We explored publicly available information and exercise reports, focusing mainly on flood-related scenarios.

The exercises found were international; several Member States (MS) are participating as players to the

exercise. In most cases though, the actual incident affects a limited geographical area of one MS, which requests assistance by neighbouring MS.

Having a cross-boundary effect in terms of consequences is increasing the complexity of the exercises. It requires the coordination of operations across various countries and it exhausts available resources for international assistance. It also introduces communication problems. Communication and interoperability are identified as key factors in most exercises, even if these are limited within one region.

How to design CIP scenarios?

Most exercises mention **key assets** and their condition. This information is important because (a) infrastructure disruptions affect the population and modify the needs for evacuation, medical care or rescue (water contamination, power disruption etc.) and (b) because they may be a resource for the command control and crews of the exercise. Therefore, it is also important to identify whether the centre of operations and the deployed teams have resources independent of the public and for how long they can maintain functions, without the need for resupplying.

CIP scenarios should identify whether an infrastructure is **critical for rescue or repair operations** (such as a main transportation node, an airport, or a fuel or water supply station needed in order for teams to be deployed or supplied).

One of the most important parameter to model in a CIP scenario is the condition of the **directly affected infrastructures** (e.g. water-related defences, in the threat of a flood). The type of damage or failure on these infrastructures can alter the scenario plot significantly but also the degree of damage it can cause.



Marianthi Theocharidou (JRC)

Marianthi Theocharidou works as a scientific/technical support officer at the European Commission's DG Joint Research Centre (JRC), located in Ispra, Italy. She participates in the activities of the CIPRNet project and the European Reference Network for Critical Infrastructure Protection (ERNCIP).

email:
marianthi.theocharidou@jrc.ec.europa.eu

Scenarios in CIPRNet

The CIPRNet project [2] currently designs such scenarios in order to develop, test and train users on the novel capabilities offered by the project. An example scenario is a flood-related, **cross-border** emergency in a densely populated region of the border between The Netherlands and Germany. In order to design the scenario, existing approaches were reviewed.

While pure CIP exercises on an EU level are quite rare, several exercises are performed annually under DG-ECHO's civil protection mechanism [3]. We explored publicly available information and exercise reports, focusing mainly on flood-related scenarios.

The exercises found were international; several Member States (MS) are participating as players to the exercise. In most cases though, the actual incident affects a limited geographical area of one MS, which requests assistance by neighbouring MS.

Having a cross-boundary effect in terms of consequences is increasing the complexity of the exercises. It requires the coordination of operations across various countries and it exhausts available resources for international assistance. It also introduces communication problems. Communication and interoperability are identified as key factors in most exercises, even if these are limited within one region.

How to design CIP scenarios?

Most exercises mention **key assets** and their condition. This information is important because (a) infrastructure disruptions affect the population and modify the needs for evacuation, medical care or rescue (water contamination, power disruption etc.) and (b) because they may be a resource for the command control and crews of the exercise. Therefore, it is also important to identify whether the center of operations and the deployed teams have resources independent of the public and for how long they can maintain functions, without the need for resupplying.

CIP scenarios should identify whether an infrastructure is **critical for rescue or repair operations** (such as a main transportation node, an airport, or a fuel or water supply station needed in order for teams to be deployed or supplied).

One of the most important parameter to model in a CIP scenario is the condition of the **directly affected infrastructures** (e.g. water-related defences, in the threat of a flood). The type of damage or failure on these infrastructures can alter the scenario plot significantly but also the degree of damage it can cause.

CIP scenarios can serve as a tool to identify the affected infrastructures within the geographic region where the threat scenario is realized. The next step is to identify disruptions that may occur in other infrastructures due to common-cause or cascading effects.

Moreover, several other infrastructures may face **common-cause or cascading disruptions** that augment the impact and complexity of the scenario. In the case of a flood scenario, we identified the following possible disruptions:

- transport disruptions due to flood-related accidents (derailment, collision of road vehicles, collision of maritime vehicles, structural elements collapse or overflow, e.g. tunnels, bridges, airports etc.)
- transport disruptions due to large scale evacuation of civilian causing traffic congestion
- disruptions of water supply or contamination of drinking water or other health hazards
- hazardous substances (CBRN) incidents due to structural damages/flooding on facilities
- hazardous substances (CBRN) incidents due to accidents to transporting vehicles,
- collapse of sewage systems
- electrical power supply disruptions
- telecommunications disruptions
- medical care facilities disruptions, due to power shortage, flooding, increased number of patients or inability of the personnel or supplies to reach the location

- industrial or business disruptions, due to power or communication disruptions.

Such disruptions, related to the threat scenario studied, should be included in the storyline. To increase the difficulty of the scenario, they can also be accompanied by other **unrelated events**, such as natural disasters, accidents or man-made incidents that modify the capacity of infrastructures.

The modelling of **dependencies** between infrastructures also indicates points of **information flow** required between different infrastructures and among different sectors.

Each scenario would be helpful if it is supported with **historical data** on previous, similar experiences in the geographic area. Such sources can provide useful information on the impact of the scenario and whether critical infrastructures can be affected. The scenario can also draw on **similar experiences** in neighbouring countries or regions. If such information is not available, other resources can be used, such as **risk assessments** that support the development of such a scenario in the specific region. CIP scenarios can also be used in order to examine **unprecedented or unlikely events** or **complex scenarios**, as this may also provide useful insight to decision makers, especially in terms of resources and critical infrastructure resilience.

A parameter examined in several scenarios is the introduction of conditions where **resources** are **stressed or exhausted** from previous incidents. Such incidents can be of similar nature but of a smaller scale (smaller scale floods, other incidents caused by the severe weather) or unrelated incidents in neighbouring regions (such as fire accidents, man-made attacks, etc.). Two alternative, but similar storylines can be exercised, where the difference lies on the availability of key resources in a specific point in time.

Most scenarios were supported by maps and screenshots of various phases of the incident. In some cases, the maps were limited, difficult to comprehend or read and with limited explanation. Each designed scenario should aim for **clear and comprehensive visualizations**, as this will enable to demonstrate clearly the

storyline and simulation results of the scenario.

Such visualizations can depict a screenshot of each phase (day, hour, etc.) of the scenario, marking affected infrastructures and other points of interest. For example, in most EU exercises the field exercise areas and the Center of Operations are marked clearly on the map. Other examples, include, locations where manned teams are needed for search and rescue, for repairing key infrastructures, etc.

In several cases, the **timeline** of events remained unclear and time periods were mixed. It would be useful if textual and graphical representation is used in order to describe the situation (state of operation on key infrastructures, location of deployed teams, extent of a natural phenomenon or accident etc.) for **specific, clear and distinct points of time**, in a structured way.

The scenarios can range from **early prognosis** or **alert signs**, several days before the actual initiating event occurs. In some cases, **preceding events** of previous months were described¹. Important points of time are major changes in the development of scenario, e.g. changes in weather conditions, man-made incidents or infrastructure disruptions.

The **time of occurrence** can also alter significantly the outcome of a scenario. For example, the scenario can be affected by **daily** or **seasonal** or **miscellaneous** parameters. For example, an event in the area that increases the population (e.g. a festival, conference or convention) can increase the population affected. Similarly, the time of an event may alter the location of most vulnerable individuals or communities (e.g. event during school hours).

Moreover, a realistic scenario should reflect the interaction and decision-making needed both by **public and private CI operators**. Since public-private cooperation structures differ from country to country, the selection of varying cases or models of cooperation could be interesting to investigate among different scenarios.

Another parameter which needs to be taken into account is the **scalability** of the scenario, as the number of countries, operators and institutions is increasing. Therefore, it would be useful if the scenarios have a **varied level of complexity**, so as to identify the point where the use of the modelling capabilities poses limitations or on the contrary helps decision makers to overcome this obstacle.

When designing scenarios for CIP, a clear timeline is needed.

Each phase should clearly describe the evolution of the threat event over time, coupled with information on the operation status of all affected infrastructures at a given point of time.

One of the few table-top exercises focused on Critical Infrastructure Protection [4] also highlights the fact that the participants in such exercises share **different levels of CIP expertise**, which is a parameter that one needs to take into account when designing CIP scenarios. This means that the exercises should pose **gradual, increasing difficulty** to participants. For example, the scenario should firstly ask the participants to recognize the CIs present, identify their dependencies and then examine the international or cross-sectorial dimension of them.

Summary

In summary, a scenario should serve a clear goal. A threat or a combination of threats (phenomena) needs to be selected for study. Then the scope of the exercise needs to be decided. This may refer to the geographical region, the timeframe, the involved stakeholders or the resources available. Creating a clear timeline is very important and for this reason, in the CIPNet project, we decided to describe each phase according to a specific template which covers the following information:

- **Timeframe / Duration:** This can be marked with specific points of time or specific events
- **Incident description:** This reflects the current situation of the phenomenon/threat studied
- **Affected infrastructure(s):** Information to be included is the name, the sector, the location, the operational status and the mode of operation (e.g. normal, stressed, recovery, etc.) for each affected infrastructure.
- **Maps:** This is needed in order to depict visually the status of each phase.

References

- [1] ERNCIP, Joint Research Center, European Commission: http://ipsc.jrc.ec.europa.eu/index.php/ERN_CIP/688/0/
- [2] CIPNet Project, <http://www.cipnet.eu/>
- [3] The Community mechanism for civil protection, http://ec.europa.eu/echo/policies/disaster_response/mechanism_en.htm
- [4] H.A.M. Luijff, D.J. Stolk, "An international tabletop exercise on critical infrastructure protection: the lessons identified", *Int. J. Critical Infrastructures*, Vol. 6, No. 3, pp.293-303, (2010)

¹ The selection of the **day zero** of a scenario can vary from the EU exercises, as it is usually marked by the activation of the mechanism for requesting international assistance.

This page is intentionally left blank.

Data management and Information sharing in CIPRNet DSS

The CIPRNet DSS enables a 24/7 risk analysis of the CI elements, providing these data to the appropriate national authorities appointed for CIP and CI operators. The nature of the 1) exchanged data and 2) the involved DSS end-users requires a well-defined security plan.

One of the main technological outcomes of the EU-FP7 CIPRNet project[1] will be a Decision Support System (DSS) able to provide a 24/7 service to CI operators and emergency (crisis) decision-makers providing a continuous risk assessment of CI elements due to natural threats. The proposed DSS will encompass the whole workflow of actions ranging from the forecast of natural hazards to the prediction of the physical damages expected for the CI elements as a consequence of the threats manifestations, to the evaluation of the impacts that the physical damages will produce on the services delivered by the CI and the ultimate consequences that the reduction (or loss) of services will produce on citizens, primary services, industrial sectors and the environment.

The architectural design of the DSS has been performed by taking into account security issues. These have been considered at three different levels: physical, informational (IT) and organizational. At the physical level, security concerns with the protection of equipment and resources from damage and harms. Protective barriers and access control protocols are typical physical security measures. The information security concerns with data and information protection against unintended and / or unauthorized access. Organizational security level is, in turn, related to policies, procedures allowing users sharing sensitive information.

In this contribution we will initially recall the CIPRNet Risk Assessment Loop and the DSS architecture. Then, we will focus on some security aspects (i.e. physical and network access security, data and services availability and trusted information sharing) related to the above mentioned security levels.

Risk Assessment Loop and DSS architecture

The CIPRNet Risk Assessment Loop (RAL) is composed of 5 Functional "Bricks" (Bn):

B1 - Monitor natural phenomena. B1 actions feed the DSS Risk Assessment Loop with external data coming from natural events monitoring sensor networks (e.g. geo-seismic, meteorological data) and data resulting from simulation model for natural events forecasting;

B2 - Prediction of natural events. The output of this phase is the prediction of the intensity of the different threats manifestations on a given area. For example, B2 may indicate that, in a given time frame, a particular region and/or city will be impacted by heavy rain and strong wind of specific intensities;

B3 - Prediction of harm scenarios. B3 will compare the B2 output with CI vulnerability data, in order to estimate the CI elements that will be affected (with a given probability) by the predicted natural threats. "Affected" means that the CI elements will be set in off-state or in a state of reduced functionality;

B4 - Impacts and consequences estimation. B4 represents the most complex task as it performs a number of different evaluations and will be performed by a tight collaboration between CIP experts and CI operators. B4 will initially provide the expected impacts on the CI (in terms of reduction or loss of functionality) and then the consequences, due to CI impacts, expected on citizens, industrial sectors, environment and the primary services (e.g. hospitals, schools);

B5 - Design of efficient strategies to cope with crisis scenarios and Reporting.



Alberto Tofani is a staff scientist at ENEA. He is member of the UTMEA-CAL Lab.
e-mail: alberto.tofani@enea.it



Antonio De Nicola is a staff scientist at ENEA. He is member of the UTMEA-CAL Lab.
e-mail: antonio.denicola@enea.it



Antonio Di Pietro is a staff scientist at ENEA. He is member of the UTMEA-CAL Lab.
e-mail: antonio.dipietro@enea.it



Maurizio Pollino is a staff scientist at ENEA. He is member of the UTMEA-TER Lab.
e-mail: maurizio.pollino@enea.it



Luigi La Porta is a staff scientist at ENEA. He is member of the UTMEA-TER Lab.
e-mail: luigi.laporta@enea.it

On the bases of Impacts and Consequences, the DSS could also, in some specific cases, develop optimized strategies to solve critical situations; these strategies could be prompted to the operator's attention, serving as a basis to develop real actions, to take over critical situations.

RAL is implemented through the 4-tier architecture as shown in Figure 1

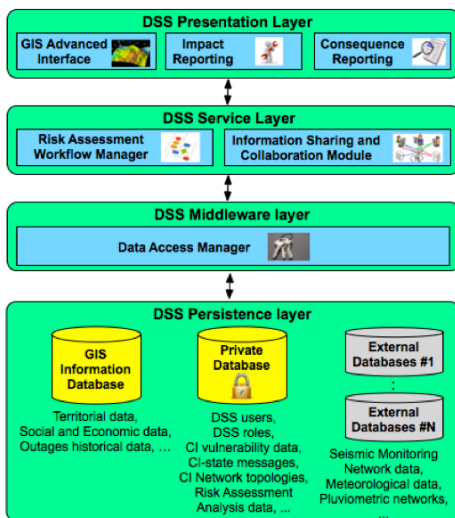


Figure 1 The DSS 4-tier architecture

The *Presentation Layer* contains the different components used to visualize the RAL results in an friendly user interface. In particular, the GIS advanced interface allows the end users to visualize CI elements risk maps and overlay this information with other information as, for example, impacts and consequences analysis results.

The *Service Layer* contains the different modules that realize the DSS business logic. In particular, this layer contains the RAL and the Information Sharing and Collaborative (ISC) platform. Other services are for example DSS System Admin services to manage the platform, DSS Analysis services to manage analysis tasks on the available data/simulations and DSS simulation service to manage and control simulation tasks.

The *Middleware Layer* implements procedures to gather, on a 24/7 basis, data coming from external sources as, for example meteorological data in order to get information to feed models and simulations enabling the prediction of future extreme natural events (e.g. flooding). In particular, the Data Access Manager will implement solutions to make the CIPRNet Persistence Layer compliant with the basic requirements for database and

network security. The first part of this contribution describes the proposed servers and databases configuration (related to the CIPRNet DSS Italian instance) to ensure the physical database integrity and network access control requirements.

The *DSS Knowledge Base Layer* is composed of different sub components:

-CIPRNet data. These are stored and managed using CIPRNet systems and applications. In turn, CIPRNet data will be further categorized as Public (i.e. data that can be accessed by generic end users using web applications and/or web services) that will be stored within the Private CIPRNet DB. Examples of private data are: users, identities and roles data, CI vulnerability data, Information Sharing and Collaborative (ISC) data, CI network topologies data and CIPRNet analysis results data. Private data will be stored within the Private CIPRNet DB. The CIPRNet security plan envisages two network and database different security levels for the two categories of databases;

-External data. In general, external data are stored in external databases. The DSS may rely on external data in different phases of the Risk Assessment Loop. For example, B1 relies on external sources of data. In B1, the DSS continuously receives data form different sources: seismic monitoring networks (e.g. in Italy these data are stored and managed by the Italian

-Data and information shared with DSS end users (e.g. CI operators, Crisis Management, Local Authorities). For example, the DSS RAL requires that CI operators exchange with CIPRnet experts data and information regarding the possible reduction of the QoS of their CI network related to an expected harm scenario (e.g. the DSS builds an expected harm scenario related to a future flooding event in a specific city area). The CIPRNet experts will use these data within the impact assessment phase in order to update the expected harm scenario considering possible cascading and dependency phenomena. As described in the following, the CIPRNet DSS will rely on a secure ISC platform to share and exchange data and information with the CIPRNet end-users.

IT and Physical Security

Figure 2 shows the CIPRNet servers and databases configuration of the Italian CIPRNet DSS instance. The DSS server (running the Risk Assessment Loop, the Data Access Service, GIS modules), the ISC server as well as the CIPRNet Private DB will be hosted in the ENEA UTMEA Computer Centre. The UTMEA Computer Centre has the following characteristics: 1) the hardware and frameworks are hosted in a locked room (only authorized ENEA staff members can access the room), 2) the computer centre is

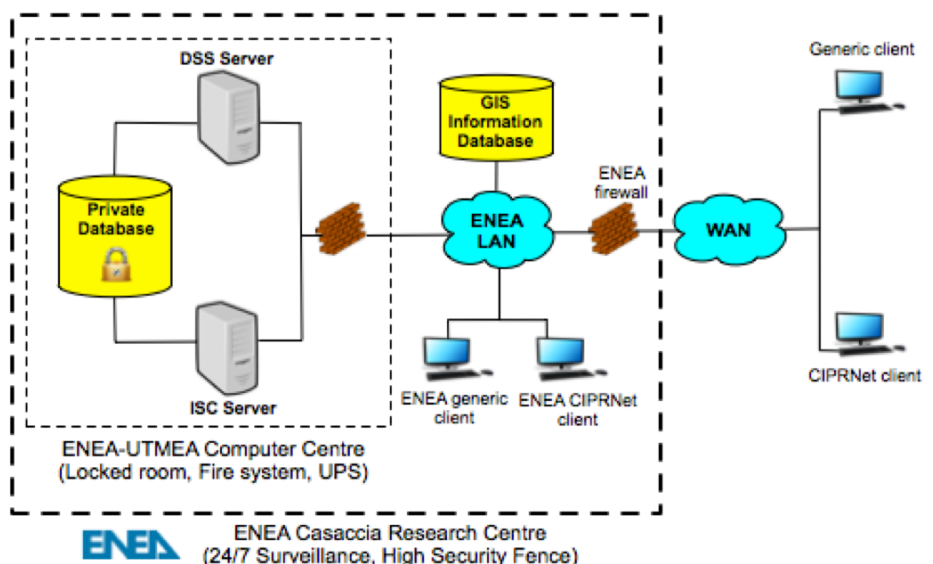


Figure 2 CIPRNet servers and database configuration

Geophysics and Volcanology Institute), meteorological stations (e.g. in Italy the stations are controlled by the Italian Air Force Met Office), pluviometric networks and so on;

equipped with a fire system and UPS system. Moreover, as shown in the Figure 2, ENEA UTMEA building (where CIPRNet servers will be located) is located inside the ENEA Casaccia Research Centre, a 24/7 access controlled Centre equipped with a

system of doubled high security fence. Then, the ENEA server configuration is compliant with the basic physical security requirements.

Regarding network access control requirements, the DSS servers and the CIPRNet Private DB are protected by two firewalls: a) the CIPRNet servers software-based firewalls and b) by the ENEA Casaccia firewall and monitoring systems that constitutes the main barrier to ensure access control to CIPRNet data and systems. Another relevant aspect in information security is the availability requirements to ensure that DSS services and data will be accessible as much as possible (in general the availability requirements are specified through minimum acceptable thresholds percentage of the time the service is available) to final end users even in case of equipment failures. In the following, the solution adopted for the Italian CIPRNet DSS instance for data and services replication will be described. In particular, this second part of the contribution concentrates on the technological solutions adopted to ensure a High Available server system.

slave is managed as a warm standby server, that is, it cannot be accessed until it is promoted master (another possible solution would be to have hot standby server, that is, it can accept connections and serves read-only queries). In order to guarantee the synchronization and the coherence of the database replica, the adopted solution will make use of Transaction Log Shipping [2]. Using this technique, the warm server is kept current by reading a stream of write-ahead log (WAL) records. In particular, the master server sends to the slave server log files containing all transactions that have been performed in the master database. In case of failure, the slave database server can use the log file to update the slave database with the last logged transactions. In general, this replica solution can be applied to manage redundant distributed geographically database servers (Figure 3). For example, for the Italian DSS instance the standby servers may be hosted in the Deltares (The Netherlands) research centre. Then, the Italian DSS may be operative even in the case the ENEA UTMEA Computer Centre is totally not operative.

share sensitive documents and information in order to increase the confidence level about a future extreme natural events prediction and share this information with other actors like Civil Protection, Police Force, Crisis Managers and DSS operators.

During the B3 and B4 phases, DSS operators and CI operators will exchange sensitive information in order to build an Expected CI Harm Scenario is the result of an extreme natural event (e.g. flooding). Figure 4 shows the information sharing process involved in the CI Harm Scenario Impact Assessment Loop that produces as result the Expected CI Harm Scenario.

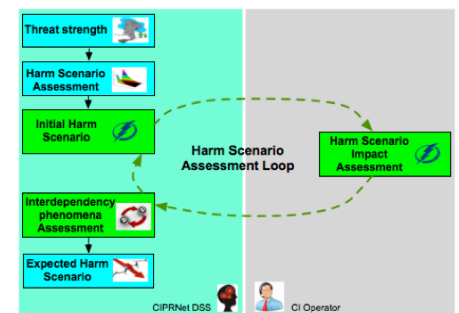


Figure 4 CI Harm Scenario Impact Assessment Loop

For example, let suppose that within the B2 phase the DSS predicts a flooding (the threat) of a certain intensity on a particular area of the city of Rome. The flooding intensity data and the CI elements vulnerability data w.r.t to flooding events will be used in B3 in order to build the so called Initial CI Harm Scenario. In this initial scenario some CI elements of different CI networks may be in failure state. The DSS operator will send this information to all involved CI operators. In turn, the CI operators are requested to provide to the DSS the expected impact (in term of the reduction of the QoS) induced by these failures on their networks. This information will feed an "system of systems" simulator to evaluate possible cascading effects induced by dependency and interdependency phenomena among CI. These phenomena, in general, may change the CI Harm Scenario and these information will be circulated with the CI operators within the CI Harm Scenario Assessment Loop until the Expected CI Harm Scenario is produced when a predefined equilibrium criteria is reached.

Last but not least, the DSS operator would need to share sensitive information with crisis decision makers

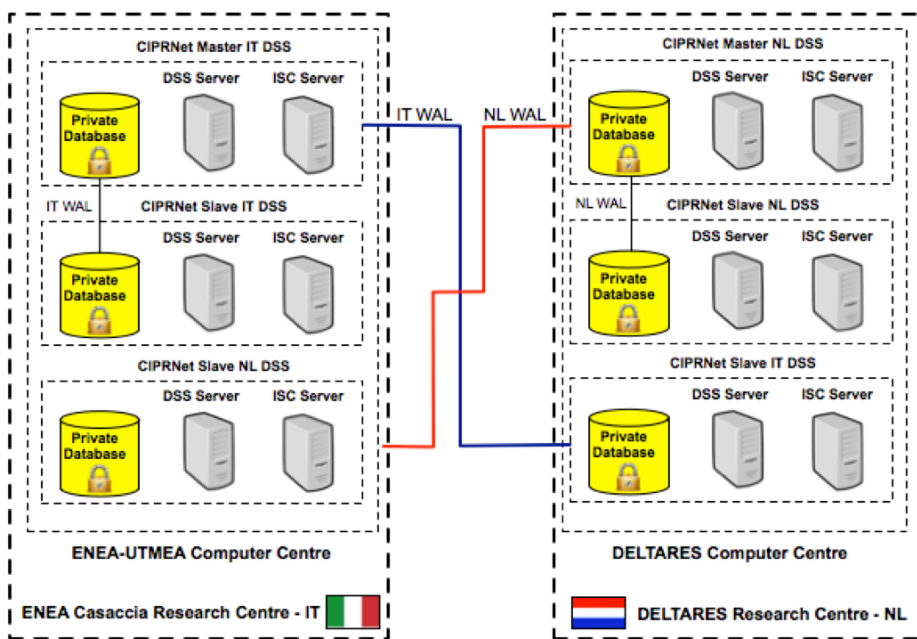


Figure 3 CIPRNet Master/Slave configuration and geographically distributed replication schema

Figure 3 shows the master/Slave CIPRNet DSS configuration. In particular, this configuration envisages the set-up of a replica of database servers, file system as well as the other main DSS services (Risk Assessment Loop, ISC and GIS services). In the described configuration, only the master or the primary server can modify data. The

Trusted Information Sharing

Within the DSS RAL there are different phases where there will be the need of exchanging trusted and confidential information among different players. For instance, during the B1 and B2 phases, scientists can

during the B5 phase in order to distribute the Risk Assessment and Consequences Report to the involved actors.

At the end, the CIPRNet DSS needs to share information of various types with different players. In general, the process of sharing information in different DSS RAL phases would require the application of different policies and different security constraints. To meet these requirements, we have designed the "CIPRNet Information Sharing & Collaboration (ISC) Module" that will be inserted into the DSS RAL by purposely customizing the outcome of a previous EU project (NEISAS, National & European Information Sharing & Alerting System [3]). NEISAS project aimed at increasing security and trust in the exchange of information between CI operators and stakeholders. To this aim, NEISAS developed a framework consisting of a model and a platform for information sharing, attempting to ensure data integrity, confidentiality (anonymity) and trust, security and service availability.

The NEISAS information-sharing model guarantees information sharing by means of "trust circles".

A trust circle consists in a group of people exchanging information using the NEISAS platform. It is composed of users with trustmaster and member role. The former role has management functionalities, as the ability to define advanced sharing rules between different trust circles, which are not enabled to the latter. The trustmaster is seen as a trusted

coordinator and manager of a trusted information-sharing group. She/he is a member of a government agency or a trusted member elected as a representative of the group.

Fehler! Verweisquelle konnte nicht gefunden werden. shows possible trust circles sharing sensitive information within the CIPRNet DSS.

The NEISAS platform provides the following advanced functionalities:

- Traffic-light protocol for alerts [4]. It is a policy used to categorise information as white (unrestricted information), green (community-wide, but not released outside the community); amber (limited distribution on a need-to-know basis), and red (personal, for named recipients only).
- Information sharing on a one-to-one basis or with a specific group of members or other trust-circles
- Anonymous posts [5]. If sensitive information to be shared could potentially cause embarrassment to the originator's organization from a business perspective, the trustmaster could play a key role. The originator of the information may ask the trustmaster to advise other members about a specific topic, but to conceal her/his identity.
- Information Rights Management [6]. It offers a further level of security, as the content of an IRM protected alert cannot be copied or printed

Finally, besides the security aspects (at technical and organizational level), the NEISAS platform has been conceived as a Web 2.0 platform in the critical infrastructures domain by managing users (with their roles and digital identities), content and data to be shared.

CIPRNet DSS Security Plan

In this contribution some aspects related to computer security have been described in the context of the CIPRNet DSS implementation. In particular, the contribution described the solutions and configurations adopted for the Italian instance of the DSS. The CIPRNet security plan encompasses many security aspects ranging from data base security to network security. In general, the CIPRNet security plan will drive the choice of every technologies and/or system that will be adopted. In this contribution we described in detail: Physical Database Security, Database and services availability, Network Security (Access control) and Organizational Security (Based on the NEISAS trust-circles).

Acknowledgement

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.

References

- [1] CIPRNet FP7 EU Project - www.ciprnet.eu
- [2] PostgreSQL 9.3 manual
- [3] NEISAS (National & European Information Sharing & Alerting System) European Research Project (Project ref: JLS/2008/CIPS/016)
- [4] Sutton, D., Cappelli M., Das-Purkayastha A., Bologna S., De Nicola A., Rosato V., Garwood A., Harrison J., Pollard D., Skellorn W. (2011). NEISAS Dissemination – Final Report.
- [5] Sutton, D., Harrison, J., Bologna, S., & Rosato, V. (2013). The Contribution of NEISAS to EP3R. In Critical Information Infrastructure Security (pp. 175-186). Springer Berlin Heidelberg.
- [6] Information Rights Management. [http://technet.microsoft.com/it-it/library/dd638140\(v=exchg.150\).aspx](http://technet.microsoft.com/it-it/library/dd638140(v=exchg.150).aspx)

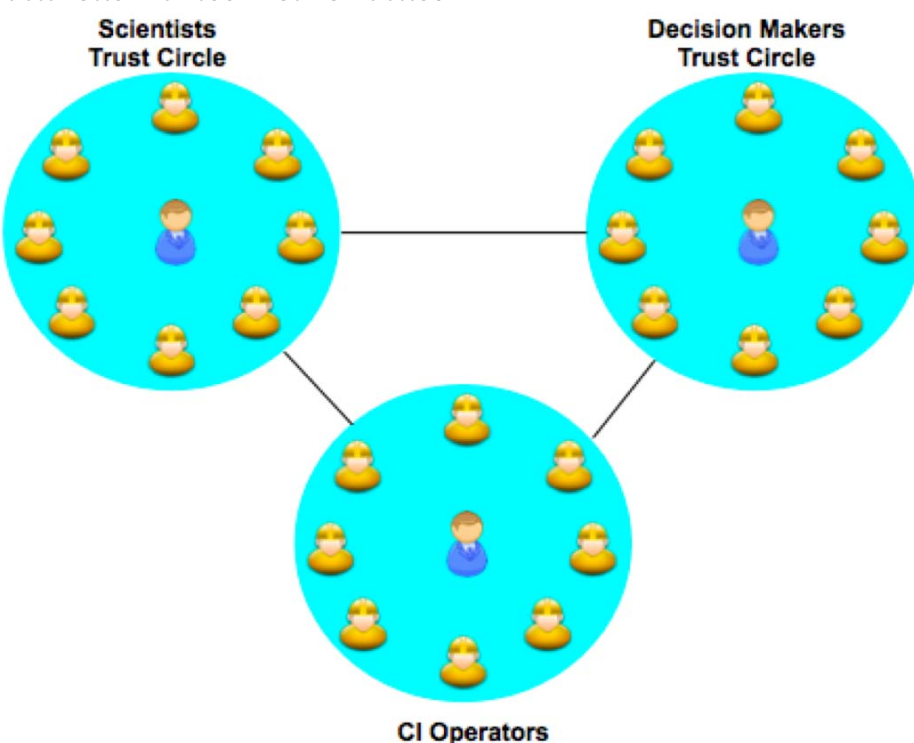


Figure 5 Example of CIPRNet DSS trust circles

Meet the Future Cyber Talent

Swiss Cyber Storm is performing a National Cyber Security Competition

With national concern about cyber security greater than ever, what can we do to help the public and private sector to stay ahead of today's and tomorrow's cyber security threats?

There is a huge demand for cyber security professionals willing to put their energy and passion into the field of cyber security research and defense. We need professionals who will network, who are willing to further their education and do not shy away from political discussions.

We, the Swiss Cyber Storm association, believe that it is the community's own responsibility to find, train and coach the most talented people for now and the future. That's why Swiss Cyber Storm is providing a suitable platform where security professionals can obtain and exchange information with regard to current cyber risks and cyber-attacks and defense topics.

However, another, maybe even more important point is to motivate enough young talents to pursue a career in IT security to meet the growing demand for cyber security professionals.

Getting involved

One problem with this is that there are so many "cool" opportunities in IT which are much more visible to young talents than a career in IT security. To improve the odds, we have to make IT security more visible and tangible to both scholars and students.

And that's exactly where Swiss Cyber Storm comes in. Its purpose is:

- Encouraging young talents to pursue a career in IT security and to promote this topic among scholars and students
- To organize an international IT security conference on Cyber Attacks and Defense at which decision makers, IT security professionals and young talents meet to discuss current and future challenges in IT security.

Security Challenges

Inspired by the success of the Cyber Security Austria association, who initially performed their first national cyber security challenge back in 2012, we decided to adapt the concept for Switzerland. The first Swiss challenges were then performed back in 2013. Suddenly the topic became quite a lot of attention not only among scholars and students but also in the media publishing reports and stories about the challenge.

A simple receipt

Organizing a challenge following the model of CSA is quite straightforward. First, you need a platform that can provide and run a wide variety of different security puzzles. Challenges include many different disciplines, for example web application security, crypto, forensics, penetration testing or reverse engineering tasks.

Fortunately, the provider of the challenge platform (Hacking-Lab) being used by CSA was willing to support Swiss Cyber Storm on its way to organizing a similar event to those in Austria.

Using Hacking-Lab, we then invited the most talented scholars and students to participate in the Swiss Cyber Storm Security Challenge final run in parallel to the Swiss Cyber Storm IT security conference in Lucerne.

Crossing borders

Since cyber security requires cooperation and trust,



Bernhard Tellenbach

Bernhard Tellenbach is a lecturer and researcher at Zurich University of Applied Sciences. His interests are focused on IT security, coarsely ranging across network security, system security and network monitoring.

Prior to being appointed by ZHAW he was with ETH Zurich, University of Applied Sciences Rapperswil, Consecom AG, and ran his own IT consultancy business. He was a visiting scholar at Microsoft Research Cambridge and Institut Eurécom.

His works have been published in several journals, and conferences. He serves as a technical reviewer for several international journals and conferences.

e-mail:
president@swisscyberstorm.com

we wanted to reflect this by partnering with Cyber Security Austria. Together we set up the "Security Alpen Cup" where the most talented contestants from Austria and Switzerland "fought" against each other. This cooperation boosted the visibility of this initiative considerably and was for the benefit of both CSA and Swiss Cyber Storm, even though the Swiss team won the first Security Alpen Cup.

Thinking big

The next step now is to internationalize the idea and the event even further. A first step has

been taken this year by inviting Germany to participate in this cross-border event. Since the name "Security Alpen Cup" is no longer appropriate for an internationalized competition, the name has been changed to "European Cyber Security Challenge".


To make the challenges even more interesting and to foster international collaboration among young cyber talents, we invite other European countries to join the European Cyber Security competition.

Becoming part of it

If you now feel like doing the same in your country or if you just want to have a closer look at the next Swiss Cyber Storm Security Challenge, please do not hesitate to contact us at president@swisscyberstorm.com.

Please save the date and visit the upcoming Swiss Cyber Storm conference and award ceremony on October 22nd, 2014 at the KKL in Lucerne. For more details, please visit www.swisscyberstorm.com



 Schweizer Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Informatiksteuerungsorgan Bund ISB
Nachrichtendienst des Bundes NDB
Melde- und Analysestelle Informationssicherung MELANI



Netonets: Critical Infrastructures as Network of Networks

During last years a new community was born aimed at combining experts from the Critical Infrastructures Protection and the Complexity Science. A book reviewing the state of the art of the field has recently appeared

During last decades the complexity of the full developed society has been steadily increasing. Any modern device is now endowed with some intelligent tools to improve its capabilities, to enhance its robustness and resilience, to reduce energy consumption, to moderate its price, to ease its recycling and optimize other characteristics such as size, portability etc. The introduction of the intelligent layer is not limited to the tools or devices, it extends to small or even large infrastructures. Any Museum, library or other public place is usually endowed with SCADA system for safety (anti-fire, anti-intrusion etc.) and governance reasons. Those SCADA systems allow for a constant monitoring and real time governance of the activities. The most dwelling and relevant systems that are presently permeated by intelligent devices are the large infrastructures such as pipelines, gas-ducts, power plants, data centres, aqueducts, etc. All full developed infrastructures do strongly rely on the communication network, the electronic control system and automation software. Moreover almost all other infrastructures depend on others such as the Electric System, the Transport (at least for employs availability and maintenance) and most of them on water supply. The owners of the Infrastructures are normally able to handle the majority of undesired situations by means of suitable measures (often also organic contingency plans) and in several cases the resilience of the service they provide is assured. However even the actuation of measures requires the availability of (at least some) other infrastructures they depend on. Therefore, a "systemic approach" is required to build up global measures and contingency plans implying the synergistic cooperation of the different infrastructures. In other words one has to deal with the "System of Systems" as a holomorphic unique entity. Due to the advent of the "smart society" the complexity of this "system of system" is destined to

increase and hence the role of the systemic framework is expected to become central.

As commonly understood, the "Systemic Risk" is a concept employed in the world of finance to refer to the danger related to a potential collapse of an entire financial sector (or a market) due to its global structure and not to a specific weakness of one of its components. The same concept can be extended to full developed societies which functioning depends on a multitude of different interdependent infrastructures. The most important infrastructures, that is those providing vital resources and sustaining the "quality of life" in the full developed countries, are often referred to as "Critical Infrastructures" (CI) and represent the core of such a complex organism that is human society.

The functioning of CI's requires a strong control of several technologies and management capabilities that are essential for providing the service or good they are devised for. Those technicalities do deeply depend on the type of infrastructure and represent a fundamental know-how that needs a constant upgrade. Despite these differences, all the infrastructures share some common characteristics. The most relevant is their partition into units (components) that are geographically and functionally separated and connected by cables, pipes or other links that allow transfer of the primary good or service. This characteristic is very special as it lends to a conceptualization of those systems as "networks" or, from the mathematical point of view, "graphs". Moving steps from this fundamental observation at the end of the past century a novel discipline was born: the "Complexity Science" [1]. This branch of the human knowledge results from the combination of the Statistical Mechanics and the Graph Theory.



Gregorio D'Agostino

Gregorio is a theoretical physicist that received his "laurea" and PhD in Physics at University of Rome "La Sapienza". He is presently Senior Researcher at ENEA (Italian National Agency for the New Technology the Innovation and the Sustainable Economic Development); Visitor Researcher at Boston University and Visitor Scientist at LIMS (The London Institute for Mathematical Sciences). He is President of the AIIC (The Italian Association of Experts in Critical Infrastructures) and a member of the OSN (Observatory for National Security). He has been project manager and coordinator of the European project MOTIA aimed at Modeling Interdependencies among ICT critical Infrastructures and is currently involved in different EU projects. In collaboration with Antonio Scala he is leader of the international organization Netonets.

Phone +39 06 30484776
website: gordion.casaccia.enea.it
email: gregorio.dagostino@enea.it

The underlying idea is that when the number of components of a system increases (strictly speaking going to infinity) a collective "emergent behavior" is observed and simple rules start governing its temporal evolution. Similarly to what happens to gases, we can disregard the details of interaction between molecules and the system is governed by simple thermodynamic equations. Analogously, when a, large enough, system of computers is attacked by a malware, its epidemic spread does not depend on the details of the propagation mechanism, but on the topology of the system and on the mere infection rate.

The complexity Science paradigms has been successfully applied to several field from the biology to the social Science. However, as explained above, to study the CI's one has to deal with systems of systems, that is, according to the complexity science paradigm, with "Networks of Networks" or "Netonets". It is worth stressing that netonets may result not only from the interdependences between networks of different types, but also from the aggregation of homogeneous

is represented by the ENTSOE (European Network of Transmission System Operators for Electricity). In this case each of the TSO's governs a high voltage (400kV) transmission electric infrastructure while receiving or providing power to other networks.

All critical infrastructures share some common characteristics: Most relevant is their partition into units (components) that are geographically and functionally separated and inter-connected ...

The ENTSOE system provides energy to some 500 millions people, assuring a complete phase synchronization all over the "Old Continent". For this reason, it has been named the European "Beating Heart". Another example of network of homogeneous networks is given by the Autonomous Systems (AS's) of the Internet. The owner of each autonomous system provides names and IP numbers

Fig. 1 represents the graph of all AS's on Internet as it appeared on April 2012: the system consisted of some 30,000 AS's linked by some 300,000 different connections.

Despite the huge development of the Complexity Science, the technological community for the Protection of Critical Infrastructures has not yet fully benefit of that discipline. The Netonets community and its relative website (www.netonets.org) were born to fulfill the need of a bridge between the Complexity Science community and that of CIP (Critical Infrastructure Protection). Netonets rises from the coordinated efforts by Gregorio D'Agostino and Antonio Scala, aimed at inspecting the potentiality of such a hybrid community. Netonets has its own international committee formed by Raissa D'Souza, Shlomo Havlin, Wolfgang Kroegeer and Gene Stanley that are among the most outstanding personalities in this emerging field.

Under the egida of the Netonets community, several conferences on "Network of Networks" have been organized. Among them it is worth noting the series carrying the same name: Netonets that took place

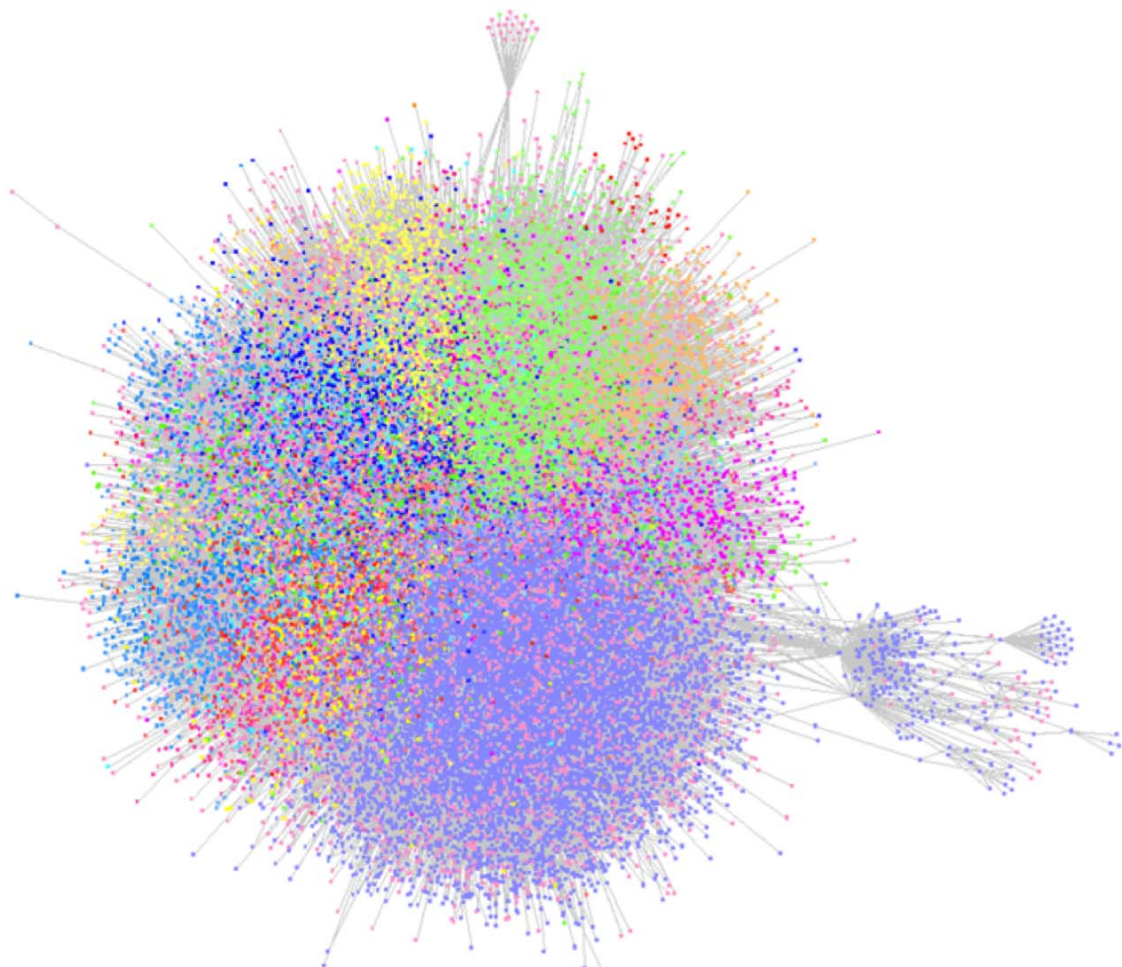


Figure 6: Internet represents a prototype of "Network of homogeneous Networks": each point represents an autonomous IP networks which color depends on the nationality of the owner. The picture has been obtained within the European Project "MOTIA" coordinated by ENEA

and 2014 (in Berkeley (CA)) and the COINETs series: 2012 (in Bruxelles) and 2014 (in Lucca). During the former events the majority of scientist involved in the Netonets research have been invited, thus covering a great part of the whole subject. The network of excellence CIPRNET (www.ciprnet.eu) and the European project Multiplex (www.multiplex.eu) are among the most important European activities on the subject, moving from the CIP and the Complexity perspectives, respectively. They both have endorsed different initiatives such as Netonets and Coinets, and have contributed significant presentations to the conferences.

Several information on the different activities performed under the Netonets behalf are available on the website. To be kept informed on main improvement and events in netonets community, one may register in the website.

The last frontier of Complexity Science

Quite recently, the Netonets community has produced a book that represents an attempt to provide an organic presentation of the state of the art of the discipline. It presents most of the different applications of the "Network of Networks" paradigm to different fields from Physiology to CIP. This book has been entitled "Network of Networks: the Last Frontier of Complexity" [2] as it represents one of the most recent challenges of the Complexity Science. The book tries to present and combine the efforts from both the Complexity and the CIP community. Several theoretical models are presented, starting from the percolation of interdependent networks by the Boston University Group that has imposed the subject of "Network of Networks" to the wide scientific audience attention [3]. However the first real attempt to apply Complexity to Netonets was due to Ian Dobson, Carreras and David Newman [4] that dealt with the problem of failures propagation on interdependent networks (Hawaii conferences). Moreover an other important step toward the application to real networks (in his case the North America inter-connected electric systems) is due to Raissa D'Souza's group [5].

Beside this leading activities, quite recently, the problem of epidemics

on Network of Networks has been also dealt with by a mere spectral approach at topological level [6] thus proving interesting exact inequalities to predict the behavior of the global system. The influence of topology on synchronizability of netonets has been recently investigated [7]. These further develops are not presented in the book.

The book is a good reference point for members of the novel hybrid community...

Other approaches to interdependent networks at basically topological level have been presented in the book. Among others it is worth mentioning the "Multiplex" approach that is the oldest one (coming from early works in sociology) and has been applied to social and financial netonets. The slight difference with the previous approach is that the set of nodes is common to all nets while the type of links have different types.

All the former theoretical works show that some emergent behaviors are observed and even the mere topology of the systems play a non trivial role for its robustness. This could provide important advices for future network expansions and re-designing. However to achieve improvements in different directions, such as assessing contingency plans, dynamical risk assessment and "what if" analysis, the pure topological approach is not enough and some details on the actual functioning of the different systems and their interdependencies need to be introduced. To this purpose, the book provides best practices for risk assessment, agent base modeling and the software federation approach. As for the workshops, several authors from both the CIPRNET and Multiplex contributed to the book

The book also provides realistic risk estimates for interacting networks (included financial systems), significant applications to transport and even to physiology. Also a human body can be conceptualized to a system of systems and the techniques of analysis of signals in interacting system do represent an other useful tool that deserves more inspection also for technological infrastructures.

We do believe that the book represents a good reference point for

members of the novel hybrid community; however it can not be considered exhaustive: several other theoretical approaches have not been treated or deserve some further treatments. Certainly the I/O models should have been included among the most abstract conceptualizations and the systemic risk analysis is under-rated.

Future develops and needs

From the mathematical point of view a very important field needs to be developed, that is the Statistical Mechanics of systems with finite or even small size. This is actually a critical point as real systems do exhibit a finite number of degrees of freedom. On the other side, there is a very important problem that is central and yet not appropriately treated that is the role of human arbitry. Decision makers and the collective behavior of operators and customers upon undesired events or unexpected situations should account for this issue in order to provide prediction for both the management of the different infrastructures. Understanding and modeling those critical elements requires the synergistic application of different disciplines such as Sociology, Psychology, Economy and the domain knowledge required to predict the consequences of the potential measures. Most of people or groups share similar interests and hence they are expected to exhibit common behaviors; therefore, again, netonets paradigm may represent a versatile tool to predict collective emergent behaviors.

References

- [1] A. L. Barabasi, R. Albert Science 285 (1999) 509
- [2] "Networks of Networks: The Last Frontier of Complexity" G D'Agostino, A Scala - Springer Berlin Heidelberg (2014).
- [3] Buldyrev et al Nature 464, (2010) 1025-1028
- [4] I Dobson, B.A. Carreras, DE Newman Probability in the Engineering and Informational Sciences 19 (1), 15-32
- [5] C.D. Brummitt, RM D'Souza, EA Leicht PNAS 109 (2012), E680--E689
- [6] H. Wang et al. Physical Review E 88 (2), 022801
- [7] J. Martin Hernandez et al. Physica A 404, 92 (2014)

Understanding Complex Systems

Springer :
COMPLEXITY

Gregorio D'Agostino
Antonio Scala *Editors*

Networks of Networks: The Last Frontier of Complexity

 Springer

Experiences from the CIPRNet Master Class on Modelling, Simulation and Analysis of Critical Infrastructures (CI)

The Critical Infrastructure Community from multiple countries was reunited in Paris with the occasion of the first edition training event of CIPRNet.

The Master Class on Modelling, Simulation and Analysis of Critical Infrastructure was held on 24-25 April 2014 at the International Union of Railways (UIC) Headquarters in Paris, France. The aim was to perform training and activities for the Critical Infrastructure Protection community. This 1.5 day training event is the first edition of a series of training events organised within the European FP7 Project CIPRNet – Critical Infrastructure Preparedness and Resilience Research Network. The Master Class was successfully organised by the University Campus Bio-Medico of Rome in coordination with the International Union of Railways – UIC and the French Alternative Energies and Atomic Energy Commission – CEA.

This meeting gave the opportunity to different research institutions to talk, exchange ideas, better know each other and create common views. The training attracted about 40 experts from CI operators, Public Authorities and researchers and experts from the Critical Infrastructure Protection research communities. The participants had the chance to learn about modelling, simulation and analysis of Critical Infrastructure. They were informed of its applications in analysis, decision support and training. Experts from the CIPRNet's network presented lectures in order to explain basic concepts and advanced aspects related to federated simulation and the use of the Open Modelling Interface (OpenMI).

The event was announced via the CIPRNet website and the registration was online. The number of participants was limited to 40 but was free of charge.

Master Class: Day One

The Master Class was opened with a warm welcome to the event by J. Pires from UIC who hosted the event. The entire Master Class was organized into 14 sessions. In the first session, E. Rome, from Fraunhofer Institute for Intelligent Analysis and Information Systems (IAIS), Germany introduced us to CIPRNet. He started by describing CIPRNet and defining Critical Infrastructures. He stated all the capabilities, benefits and goals of CIPRNet and how they will be achieved.

Participants of the Master Class had the chance to interact with experts from diverse areas of Critical Infrastructures, share their opinion on problems and their solutions and create the first contacts for future collaborations.

The second session focused on critical infrastructure protection and critical infrastructure resilience. C. Pursiainen from the Joint Research Centre of the European Commission presented this session. Through his talk he explained everything about the concept of critical infrastructure resilience. Origin, approaches, dimensions, definitions, enhancement and how to measure and test technological resilience.

The next session "Simulation of Critical Infrastructures (CI): relevant applications", by E. Luijff, from Netherlands Organisation for Applied Scientific Research (TNO) explained



Elena Polykarpou

Elena Polykarpou is a Research Associate at the KIOS Research Center for Intelligent Systems and Networks at the University of Cyprus. She is also working towards her PhD degree.

Elena received her BSc with Honors in 2010 and her MEng in 2012 from the Department of Electrical and Computer Engineering at the University of Cyprus. Her research interests include monitoring, security and control of power systems, modeling and parameter estimation of loads.

e-mail:
polykarpou.elena@ucy.ac.cy

where CI Protection MS&A can be applied and the added value for stakeholders. He also outlined some existing activities all over the world and what we are looking forward to.

Principal modelling techniques was the focus of the fourth session. M. Eid from Atomic Energy and Alternative Energies Commission explained modelling of complex systems and what solutions we can have. We were also showed CI as a collection of heterogeneous interacting components.

Modelling and investigating dependencies was the next topic presented by R. Setola from University Campus Bio-Medico of Rome. In this session we learned the importance of (inter)dependencies and how the most common phenomena can be modelled. We were showed some events and failures so that we could understand the consequences that can result if we neglect to capture them.

V. Rosato from Italian National Agency for New Technologies, Energy and Sustainable Economic Development analysed us the topological properties of complex networks and their relevance for CI. In his talk Dr. Rosato introduced us to graph theory and explained how it is related with complex system properties. It was showed that functioning properties of complex networks can be found by the topological properties and for specific topological shapes of networks that represent CI, robustness and functionality criteria can be met.

The seventh session, "Hybrid engineering/phenomenological approach to simulate systems of systems" was presented by J. Marti, from the University of British Columbia, Vancouver. Prof. Marti discussed how multiple CIs interact in case of disaster response and other critical applications. I2Sim multi-system engineering/phenomenological modelling was also presented. The i2Sim modelling framework allows the integration of both engineering and human systems. I2Sim allows real-time solutions of large multi-CI system of systems. The objective is to have a real-time disaster response optimization. Partitioning of the solution may be used for large and complex systems.

The first day sessions were closed by B. Becker and A. Burzel from Stichting Deltares who introduced us to OpenMI (Open Modelling Interface). We were showed the basic concepts and a life demonstration example. OpenMI is an open model interface standard. It is designed for hydro-related models and is already used by several institutions. With OpenMI time-dependent models can exchange data during runtime at each time step. OpenMI is used for coupling models either of different processes either of the same type allowing this way to simulate interaction processes. We were demonstrated how an open channel flow model is coupled with a real-time control model.

The first day was closed by a welcome cocktail at the UIC grand hall. This cocktail gave the participants the opportunity to know each other better and share their thoughts after attending the first eight sessions. It was a nice and warm break for the attendees giving them the opportunity for networking. Since the Master Class attracted experts from various fields they could discuss their different opinions so that they can overtake any issues that may arise and head to the goal of CIPRNet to create new capabilities, build the required capacities and provide knowledge and technology.

Master Class: Day Two

The Master Class continued the second day with the ninth session presented by W. Huiskamp from the Netherlands Organisation for Applied Scientific Research. This session focused on the federated approach for the simulation of complex systems. Mr. Huiskamp outlined the available

architectures and standards. He explained High Level Architecture (HLA) and Distributed Simulation Engineering and Execution Process (DSEEP).

Modelling, simulation and analysis techniques for CIP were described by A. Usov from Fraunhofer Institute for Intelligent Analysis and Information Systems (IAIS). Following the previous session for federated simulation a comparison was made with integrated modelling and simulation. For a better understanding, an example for both approaches was analysed, i2Sim framework for the integrated approach and DIESIS architectural approach for the federated. In this session it was showed that for many CIP applications modelling and simulation is very useful and the analysis of multi-CI is challenging.

E. van Veldhoven from the Netherlands Organisation for Applied Scientific Research highlighted the importance of verification and validation. In this talk Mr. Van Veldhoven convinced us for the need of verification and validation in a structured way and with the right technique. He explained that more benefits are gained by V&V in comparison to the cost. An overview of the techniques was presented and how we should choose the right one for our CI models. In the end, we were outlined the four basic categories of tests that can be used.

The eleventh session was presented by M. Pollino from the Italian National Agency for New Technologies, Energy and Sustainable Economic Development. Mr. Pollino discussed the Geographical information systems for visualisation and analysis. The basic concepts and functionalities of Geomatics were



outlined. We were presented examples of applications, integration of the technique and computational modules. In addition, the case of an earthquake event was analysed to show us the resulting impact and the consequences.

Real-time event prediction was described in the twelfth session by A. Zijdeveld from Stichting Deltares. Mrs. Zijdeveld explained that measurements and sensors enhance the accuracy and reliability of forecasting whereas probabilistic forecasting can create uncertainties. Hazard prediction may result by combining the available measured data and model simulations. In addition, we were also showed some examples for better illustration. Nowadays, the real-time services are increasing both in quality and lead-time.

The sessions closed V. Rosato from Italian National Agency for New Technologies, Energy and Sustainable Economic Development. The focus was on the Decision Support system (DSS) in the area of risk management of CI. We were presented the DSS and how it is used in the risk management of CI. A DSS must be able to observe and predict an event, the harm scenario, the impacts and consequences from damages and help decision makers to compile useful information, identify critical situations and take decisions.

The Master Class finished with a very interesting discussion by everyone. With the final comments it was obvious that the goal of the Master

Class to strengthen the links and create common views was achieved. Various opinions from many sides were expressed.

Master Class Summary

The Master Class was very well organized and accomplished all its initial goals. It attracted people from various areas making the discussions particularly interesting. The participants consisted of people from multiple countries all over the world giving the opportunity to each one expressing their opinion based on their own experiences and points of view. It achieved to give the chance for networking, bring diverse communities together and give the chance for future collaborations. The attendees had also the chance to learn about modelling, simulation and analysis of CI from the best in the field experts. By having people of

all ages and levels of expertise it was like a baptism for entering the professional community. The event surpassed everyone's expectations.

Further Information

More info along with the full program of the Master Class can be found at the official website of the event <https://www.ciprnet.eu/endusertraining.html>. All the presentations are archived at <https://www.ciprnet.eu/login.html> and are available to all the participants.

The next Master Class will be held in Rome, Italy where the focus will be on DSS. Keeping the high level of the training schools of CIPRNet, experts will be invited to talk and share their knowledge to everyone that will attend the Master Class.



This Page is intentionally left blank.

CRITIS 2014 Conference: 9th International Conference on Critical Information Infrastructures Security

Bringing together researchers and professionals from academia, industry and governmental organizations working in the field of the security of critical infrastructure systems.

On behalf of the Steering Committee and the Local Organising Committee we are excited to invite you to submit papers and attend the CRITIS 2014 conference. CRITIS 2014 will be held in October 2014 in Limassol, Cyprus and it continues a well-established tradition of successful annual conferences. It aims at bringing together researchers and professionals from academia, industry and governmental organisations working in the field of the security of critical infrastructure systems.

Modern society relies on the availability and smooth operation of a variety of complex engineering systems. These systems are termed Critical Infrastructure Systems (CIS). Some of the most prominent examples of critical infrastructure systems are electric power systems, telecommunication networks, water distribution systems, transportation systems, wastewater and sanitation systems, financial and banking systems, food production and distribution, and oil / natural gas pipelines.

Our everyday life and well-being depend heavily on the reliable operation and efficient management of these critical infrastructures. The citizens expect that critical infrastructure systems will always be available and that, at the same time, they will

be managed efficiently (i.e., they will have a low cost). Experience has shown that this is most often true. Nevertheless, critical infrastructure systems fail occasionally. Their failure may be due to natural disasters (e.g., earthquakes and floods), accidental failures (e.g., equipment failures, software bugs, and human errors), or malicious attacks (either direct or remote). When critical infrastructures fail, the consequences are tremendous. These consequences may be classified into societal, health, and economic.

Conference web site:
<http://www.critis2014.org>

Conference dates
13-15 October 2014

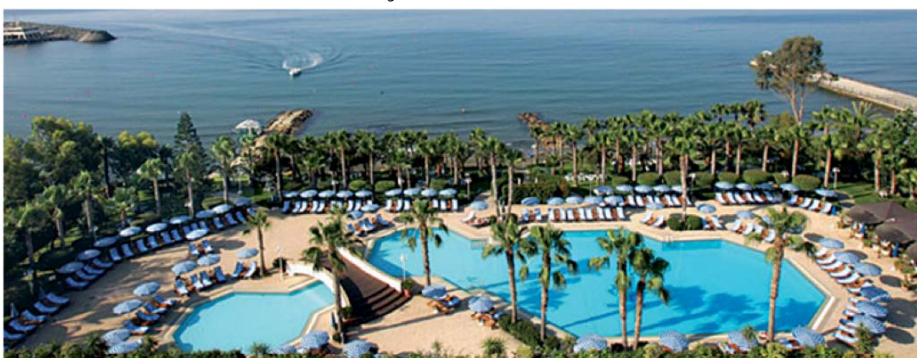
The venue of the CRITIS 2014 conference will be the magnificent Grand Resort Hotel, in Limassol, Cyprus. The hotel is set in over 20,000 square meters of beautifully landscaped gardens with exotic trees and subtropical plants, which extend right down to the seashore.



Elias Kyriakides

is an Assistant Professor at the Dept of Electrical and Computer Engineering and the Associate Director for Research at the KIOS Research Center for Intelligent Systems and Networks, University of Cyprus

e-mail: elias@ucy.ac.cy



Conference Topics

- Infrastructure resilience and survivability
- Security and protection of complex cyber-physical systems
- Self-healing, self-protection, and self-management architectures
- Cyber security in critical infrastructure systems
- Critical (information-based) infrastructures exercises and contingency plans
- Advanced forensic methodologies for critical information infrastructures
- Economics, investments and incentives of critical infrastructure protection
- Infrastructure dependencies: modelling, simulation, analysis and validation
- Critical infrastructure network and organizational vulnerability analysis
- Critical infrastructure threat and attack modelling
- Public-private partnership for critical infrastructure resilience
- Critical infrastructure protection policies at national and cross-border levels
- Fault diagnosis for critical infrastructures
- Fault tolerant control for critical infrastructures
- Security and protection of smart buildings
- Detection and management of incidents/attacks on critical infrastructures
- Preparedness, prevention, mitigation and planning

Sponsorship and Exhibition Opportunities

The CRITIS 2014 Conference is a unique opportunity for organizations to connect with up to 150 leading experts in the fields of security and protection of critical infrastructure and critical information systems who work in a variety of government, academic, and private sectors. This would be a wonderful opportunity for your organization to have significant visibility in front of an audience who could benefit and value from your participation at this conference.

We are delighted to invite you to sponsor and/or exhibit at the CRITIS 2014 Conference. The Organizing Committee is committed to providing an exciting and informative program

of speakers, and facilitating networking and business opportunities for sponsors.

Sponsors and exhibitors will receive acknowledgement prior to, during and after the conference through conference materials, the web site, and the plenary sessions, and enjoy significant contact with delegates during the exhibition and social events. The exhibition will be open for the duration of the conference. Our sponsorship and exhibitor packages are very attractive and cost-efficient.

Please do not hesitate to contact us to discuss how we can customize a package that meets your marketing objectives. We are happy to work together with you to create an individual offer to ensuring the best result for your company.

CRITIS 14 is where the CIP expert and researchers meet and exchange. Align with newest trends and get inspired: Don't miss this chance!

Conference Proceedings

All accepted papers will be included in the conference proceedings which will be distributed during the conference. Selected papers will also be included in a special volume and published by Springer-Verlag Lecture Notes in Computer Science.

Conference Program

The Conference Program and registration details will be announced along the announcement of the accepted papers. Please stay tuned at the conference web site.

CIPRNet Young CRITIS Award (CYCA)

An award for outstanding research in Critical Infrastructure Security and Protection sponsored by the EU FP7 NoE CIPRNet will honour winners at CRITIS 2014. It is a unique chance for young researchers to be recognised. For more information: cyca.critis2014.org



Organisers and Contact Information

General Chairs:

Marios Polycarpou (University of Cyprus)
Elias Kyriakides (University of Cyprus)

Program Chair

Christos Panayiotou (University of Cyprus)

Program Co-Chairs

Vicenç Puig (Universitat Politècnica de Catalunya)
Erich Rome (Fraunhofer Institute for Intelligent Analysis and Information Systems)

Publications Chair

Georgios Ellinas (University of Cyprus)

Publicity Chairs

Demetrios Eliades (University of Cyprus)
Cristina Alcaraz (University of Malaga)

For more information:

Elias Kyriakides (elias@ucy.ac.cy)
Or visit <http://www.critis2014.org>

Links

ECN home page <http://www.ciprnet.eu>
ECN registration page free registration on www.ciip-newsletter.org

Forthcoming conferences and workshops

IDRC 2014	http://idrc.info/programme/call-for-abstracts	24-28.08.14	Davos, Switzerland
EAIS 2014	https://fedcsis.org/2014/eais	7-10.09. 14	Warsaw, Poland,
CRITIS 2014	www.critis2014.org	13-15.10.14	Limassol Cyprus
Swiss Cyber Storm	www.swisscyberstorm.com	22. 08.14	Lucerne Switzerland

Exhibitions

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

Master Class

Program and info <https://www.ciprnet.eu/endusertraining.html>
Presentations (on request only: <https://www.ciprnet.eu/login.html>)

Associations

Global Risk Forum Davos www.grforum.org
Swiss Cyber Storm www.swisscyberstorm.com/

Institutions

National and European www.neisas.eu
Information Sharing & Alerting System
Networks of Networks <http://gordion.casaccia.enea.it>
Mechanism for civil protection, http://ec.europa.eu/echo/policies/disaster_response/mechanism_en.htm

Project home pages

FP7 CIPRNet www.ciprnet.eu
EU Security Liaison Officer www.slo-project.eu
Conference contributions: www.coseritylab.it (for download)
FP 7 INTACT www.meteo.unican.es/projects/intact
PREDICT www.predict-project.eu

Interesting Downloads

Critis' 12 Conf. Proceedings: www.springer.com/computer/security+and+cryptology/book/978-3-642-41484-8
Critis' 13 Conf. Proceedings: <http://link.springer.com/book/10.1007/978-3-319-03964-0>

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"
ENISA www.enisa.europa.eu/activities/Resilience-and-CIIP

Websites of Contributors

Joint Research Centre <http://ipsc.jrc.ec.europa.eu>

CRITIS 2014

9th International Conference on
Critical Information Infrastructures Security
October 13-15, 2014, Limassol, Cyprus
www.critis2014.org

