CIPRNet: EU's Network of Excellence for Resilient Critical Infrastructures

by Eric Luiijf, MS.c.* and Erich Rome, Ph.D.**

With co-funding by the European Union (EU), a European consortium works towards the establishment of a European Infrastructures Simulation & Analysis Center (EISAC). For Europe, the EISAC shall deliver Critical Infrastructure Protection (CIP) related services for Europe like those delivered by the National Infrastructure Simulation and Analysis Center (NISAC) in the United States and the Critical Infrastructure Program for Modelling and Analysis (CIPMA) in Australia.

The Critical Infrastructure Preparedness and Resilience Research Network (CIPRNet) project started on March 1, 2013. This Network of Excellence project is co-funded by the security research program within EU's 7th Research Framework Program (FP7). The CIPRNet consortium comprises six European research institutes (Fraunhofer, ENEA, TNO, CEA, JRC, Deltares), the international union of railways UIC, the universities of Rome, Cyprus, Bydgoszcz (Poland), and British Columbia (Canada), and ACRIS GmbH (Switzerland). The project coordination is by the German Fraunhofer Institute for Intelligent Analysis and Information Systems. The consortium brings together a unique set of knowledge and technology gathered in over sixty previous national and international research and development projects in the CIP field. Each consortium partner also functions as a multiplier by connecting their (inter)national networks and research platforms to CIPRNet's core activities and capabilities.

Within its lifetime of four years, the CIPRNet consortium will make a decisive effort towards providing support from the CIP research communities to emergency responders, government agencies, and policymakers, enhancing their preparedness and response capabilities regarding service disruptions in Europe's complex system of interconnected and dependent critical infrastructures (CI) across the 28 EU member nations and some associated nations.[1]

The expected long-lasting outcome of CIPRNet is an established multi-national operating EISAC with several nodes across Europe delivering CIP simulation, analysis, training, and other support services to national and regional emergency management centers as well as critical infrastructure operators. At the same time, the EISAC will maintain a collective knowledge and technology base on CIP and CI models and data, as well as be a focal point in European CIP research and development.

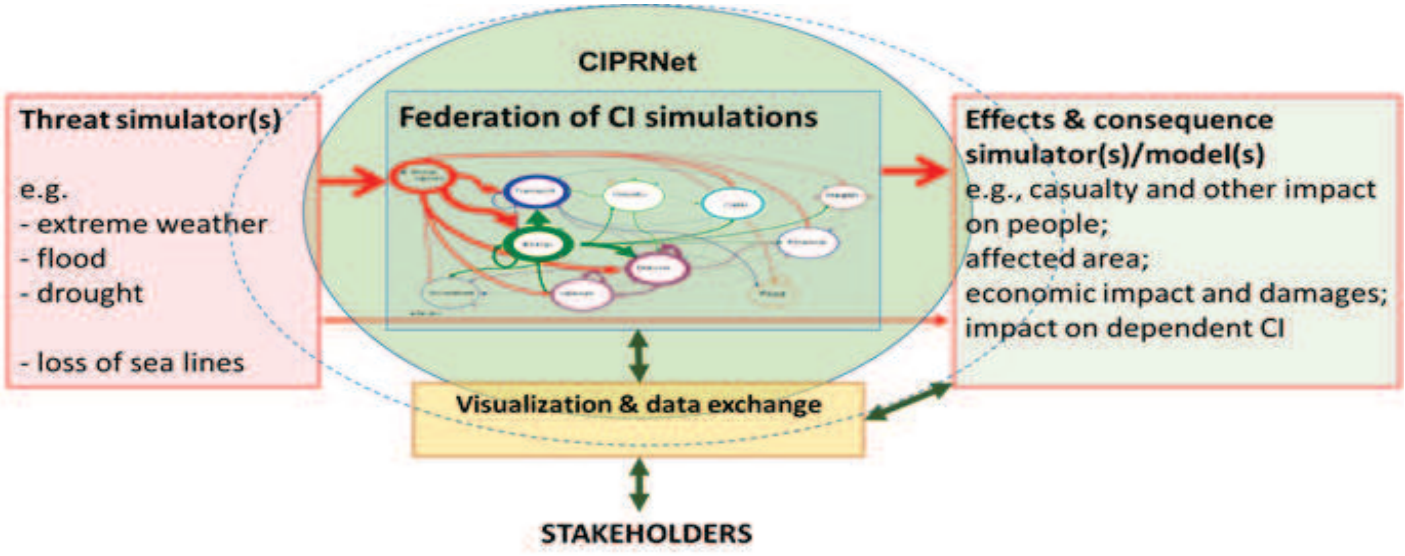
The CIPRNet Community

From the start, CIPRNet has involved its stakeholders in the design of the new capabilities. This is accomplished both by an International Advisory Board of end users and other stakeholders, and by the organization of targeted workshops and training events. The International Advisory Board currently has ten members from civil protection authorities, ministries, industry, and associations

(Continued on Page 3)

[1] The need for better understanding and preparedness is outlined in, H.A.M. Luiijf and M.H.A. Klaver, "Expand the Crisis? Neglect Critical Infrastructure! (Insufficient Situational Awareness about Critical Infrastructure by Emergency Management— Insights and Recommendations)" in: *Tagungsband 61. Jahresfachtagung der Vereinigung des Deutschen Brandschutzes e.V.*, 27-29.05.2013 (Weimar, Germany, 2013), pp. 293-304.

Figure 1: Positioning of CIPRNet



(Continued from Page 2)

fostering security and CIP. An Independent Ethics Board of experts in data protection and privacy ensures project results comply with legal and ethical standards. Moreover, any research group that can bring added-value to CIPRNet (and by that to their own progress) is welcome to connect to the network. Exchanges with other EU co-sponsored projects such as PREDICT (dependencies) and INTACT (extreme weather) are planned for.

New Capabilities

Reaching and maintaining the required level of CIP preparedness and responsiveness requires adequate and fast adaptation to on-going changes of CI. CIPRNet will implement advanced modelling, simulation, and analysis (MS&A) capabilities for supporting more effective responses to emergencies that affect or originate from multiple, dependent CI (see Figure 1). In particular, CIPRNet will create value-added decision support capabilities for national and multi-national emergency management. These capabilities will enable decision-makers and operators to analyze the various possible courses of action, to perform what-if analysis, and to learn about short and long term consequences of their decisions.

Apart from the core set of federated and interacting CI models, the threat side will comprise extreme weather threat models, flood models, and models of other threats that may affect multiple CI directly or through cascading effects. The effects and consequences analysis part will be based on real-time and statistical data, economic and other simulations and models, meteorological data, and more. The development of this new decision support capability will build upon pooling and integrating technologies and resources available though CIPRNet's partners and beyond. As an additional capability, CIPRNet plans to support the secure design of Next Generation Infrastructures like Smart Grids. The development of the new capabilities follows a model-based systems design approach. Key elements of this approach are scenario orientation, requirements engineering, and use cases.

Scenarios & Architecture

CIPRNet creates scenarios at different scales for developing, testing, and training the new capabilities. For instance, a regional scenario in one EU Member State will consider several dependent CI affected by threats like floods, landslides, and earthquakes. A scenario in a densely populated border region between two other Member States will consider a combination of

(Continued on Page 4)

(Continued from Page 3)

cross-border emergencies such as a dike breach affecting local CI with major cross-border impact.

International Capacity Building

In order to provide long lasting support from research communities, CIPRNet also aims at building required capacities. Numerous dissemination and training activities will contribute to this aim, including but not limited to the following:

- Dedicated cooperation workshops with other projects and networks in the field will contribute to increased coherence in the distributed multi-stakeholder community of CIP researchers and experts.

- Dedicated training activities will familiarize experts and potential end users with CIPRNet technology and knowledge. For example, at the end of April 2014, a first training session with over forty attendees took place in Paris.

- Young researchers will be trained via staff exchange between CIPRNet partners and by integrating CIPRNet lectures into the postgraduate Master in Homeland Security course at the Università Campus Bio-Medico in Rome, Italy. The next course will take place in July 2014. The planning for the 2015 sessions is in progress. Announcements and details regarding the training sessions can be found on the CIPRNet website.

- Apart from these external activities, the consortium partners exchange personnel to work on dedicated CIP and MS&A issues.

As outreach, the CIPRNet website contains information on the project, the events, and the ECN—the European equivalent of *The CIP Report*—a magazine on European CIP developments. The website will be extended over time with content and new functions such as:

- CIPedia ™—a wiki with many CIP-related resources, definitions, as well as debates to support CIP practitioners, policymakers, and CI operators.

- Ask-the-CIP-expert ™—a function to access practical CIP knowledge, CIP researchers, MS&A experts, etc., as well as to locate CIP best practices and resources (mainly in Europe).

- A CIP expertise database offering valuable knowledge and resources for stakeholders.

VCCC and EISAC

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

A design study of the EISAC is available from the earlier completed, EU co-funded project, Design of an Interoperable European federated Simulation network for critical InfraStructures (DIESIS).[2] This design study will be employed in CIPRNet in the establishment of the VCCC and later the EISAC. The purpose is to found autonomous national EISAC nodes in Member States that will provide services tailored to the needs of the Member States. A central roof organization at a European level will ensure standardization of basic technology like middleware and modelling approaches, broker bilateral cooperation of EISAC nodes, and provide support at the EU

(Continued on Page 5)

[2] Uwe Beyer et al, Design of an Interoperable European federated Simulation network for critical InfraStructures (DIESIS): D4.1b Final Architectural Design (Sankt Augustin, 2010). Accessed April 30, 2014, www.diesis-project.eu.

(Continued from Page 4)
level.

Since transfer of research results into application and MS&A-based new decision support capabilities will be the focus of EISAC, it will complement the services of networks like the Critical Infrastructure Warning Information Network (CIWIN) and the European Reference Network for Critical Infrastructure Protection (ERNCIP).[3]

If interested in CIPRNet, please visit the website, take part in the events, or contact the authors of this article.❖

Acknowledgments

This article was written by 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. Moreover, the authors gratefully acknowledge the contributions of their CIPRNet partners to this article. It should be regarded as a joint publication of the consortium. The content of this publication does not reflect the official opinion of the European Union. Responsibility for the information and views expressed therein lies entirely with the authors.

**Eric Luiijf, M.Sc.*

Eric Luiijf is principal consultant at the Netherlands Organisation for Applied Scientific Research TNO. As expert he has contributed to many national and EU projects in the field on Critical (Information) Infrastructure Protection, both at the technical and policy levels, since 2000. Eric has published many popular articles, reports, and peer-reviewed publications about cyber terrorism, C(I)IP, process control security, information assurance, and cyber operations. He has been interviewed many times by press, radio and TV on these topics.

***Erich Rome, Ph.D.*

Erich Rome is a senior researcher and project manager at Fraunhofer-Institut für Intelligente Analyse und Informationssysteme IAIS' ART department in Germany. Since 2007, Erich Rome has investigated MS&A for CIP and multi-sensory systems for surveillance and security. He has published numerous peer-reviewed publications, edited several books, and is a member of the steering committee of the workshop series CRITIS. To date, he has coordinated four EU projects, CIPRNet being the current one.

[3] See *infra*, p. 13, for further discussion of the European Reference Network for Critical Infrastructure Protection.