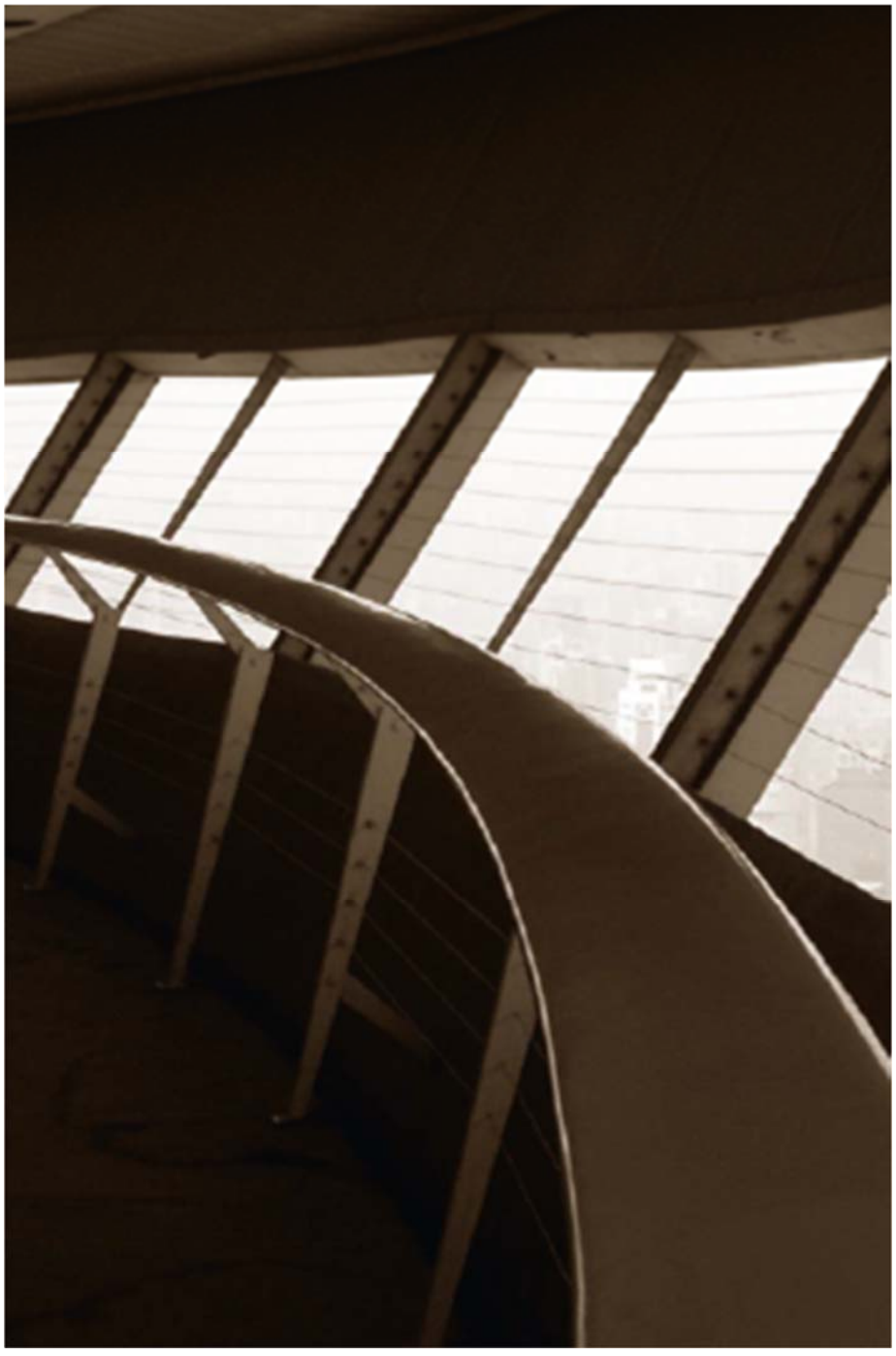
European CIIP Newsletter

Special Issue

CRITIS 2015

October 15 - February 16, Volume 9, Number 3



ECN

Contents

CIPR Net

> 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

> Spelling:
British English is used except for US contributions

Editorial: Strengthening collaboration among research projects within the EU

Increasing the resilience of European Critical Infrastructures through science requires closer collaboration of projects with similar scope, close communication with end users and links to EU policy.

The protection and resilience of Critical Infrastructures (CI) remains a priority for Europe, as reflected by the funded security projects under the 7th Framework programme and the on-going ones under the Secure Societies H2020 programme. As Dr. Martínez-Garcia explains in the first article of this issue, upcoming **H2020 calls for innovation projects** (2016-2017) will focus on physical and cyber protection for critical infrastructures, building on the research work been performed and strengthening the link with end users, the industry and standardisation bodies.

EU-funded projects should interact in order to benefit from past results, to avoid duplication of effort and to increase exploitation by end users within the EU market. For this reason, the EC has initiated the development of a **Community of Users in Disaster Risk and Crisis Management**. This issue of the ECN series continues to contribute towards this direction, as its past issues. It aims to act as a forum of dissemination but most importantly of synergy among projects, both EC funded ones and national research ones on CIP topics.

To this end, the issue welcomes articles by two recently funded H2020 projects **IMPROVER** and **RESIN**, which focus on **resilience**. IMPROVER aims towards a risk-based approach combining different dimensions of resilience to four living labs. RESIN develops standardised approaches to help city administrators, the operators of urban infrastructure networks, and related stakeholders to develop their adaptation strategies and ensure that their decisions strengthen the resilience of a city. The Geospatial Risk and Resilience Assessment Platform (**GRRASP**) –a JRC project- is also presented. It is a collaboration and analysis tool that can be used by authorities and operators for risk and resilience assessment at local, regional, national and international scale.

The issue continues with **national approaches and initiatives**. The novel national approach for CIP and resilience in the **Netherlands** is presented. Other national initiatives include the Center for Cyber and Information Security, in collaboration with the long-standing Network Information Security Lab in **Norway**, and the launch of the Research Centre on Resilient Information and Control Systems in **Sweden**. On the cyberspace front, alternative **Cyber Defence** national strategies are presented and analysed.

The issue concludes with insights on **cybersecurity**, as well as **CI research** and **training**. To start, new advances in **identity and access management** are presented. The article discusses how these could affect the security market. Two seemingly different research topics are compared, i.e. **asset management and critical infrastructures**. The article identifies similarities and potential areas for collaborative research. On the **training** side, two courses on **Homeland Security** in Italy and USA are compared to guide readers to useful conclusions when planning and conducting such courses.

We would like to remind you that the CIP community has a rendezvous in Berlin at the **10th edition of the CRITIS conference** (October 5-7). We also announce that the 2nd student award is presented at this year's CRITIS conference. As this tradition will continue to upcoming conferences, young researchers are encouraged to apply for the 2016 award.

Enjoy reading this issue of the ECN!

PS: Please have a look at CIPedia©: http://www.cipedia.eu. Please bring your knowledge in to contribute to a real CIP compendium!

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

Marianthi Theocharidou

Marianthi Theocharidou works as a research fellow at the European Commission's DG Joint Research Centre (JRC), working for the CIPRNet, IMPROVER and ERNCIP projects.

marianthi.theocharidou@jrc.ec.europa.eu

Bernhard M. Hämmerli
Is CEO of ACRIS GmbH and Chair of ICT Security Activities at Swiss Academy of Engineering Sciences

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

ACM CPSS'16 CALL FOR PAPERS

2nd ACM Cyber-Physical System Security Workshop

Xi'an, China – May 30, 2016 (in conjunction with ACM AsiaCCS'16)

http://icsd.i2r.a-star.edu.sg/cpss16/

Important Dates

Submission due: Dec 5, 2015 Notification: Feb 15, 2016 Camera-ready due: March 15, 2016

Cyber-Physical Systems (CPS) consist of large-scale interconnected systems of heterogeneous components interacting with their physical environments. There are a multitude of CPS devices and applications being deployed to serve critical functions in our lives. The security of CPS becomes extremely important. This workshop will provide a platform for professionals from academia, government, and industry to discuss how to address the increasing security challenges facing CPS. Besides invited talks, we also seek novel submissions describing theoretical and practical security solutions to CPS. Papers that are pertinent to the security of embedded systems, SCADA, smart grid, and critical infrastructure networks are all welcome, especially in the domains of energy and transportation. Topics of interest include, but are not limited to:

- Adaptive attack mitigation for CPS
- Authentication and access control for CPS
- Availability, recovery and auditing for CPS
- Data security and privacy for CPS
- Embedded systems security
- EV charging system security
- Intrusion detection for CPS
- IoT security
- Key management in CPS
- Legacy CPS system protection
- Lightwight crypto and security
- SCADA Security
- Security of industrial control systems
- Smart Grid Security
- Threat modeling for CPS
- Urban transportation system security
- Vulnerability analysis of CPS
- Wireless sensor network security

Steering Committee

Dieter Gollmann (Hamburg Uni of Tech, Germany)
Ravishankar Iyer (UIUC, USA)
Douglas Jones (ADSC, Singapore)
Javier Lopez (University of Malaga, Spain)
Jianying Zhou (I2R, Singapore) – Chair

Programm Chairs

Jianying Zhou (I2R, Singapore)
Javier Lopez (University of Malaga, Spain)

Publicity Chair

Cristina Alcaraz (University of Malaga, Spain)

Publication Chair

Ying Qiu (I2R, Singapore)

Submission Instructions

Submitted papers must not substantially overlap papers that have been published or that are simultaneously submitted to a journal or a conference with proceedings. All submissions should be appropriately anonymised (i.e., papers should not contain author names or affiliations, or obvious citations). Submissions must be in double-column ACM SIG Proceedings format, and should not exceed 12 pages. Position papers and short papers of 5 pages describing the work in progress are also welcome. Only pdf files will be accepted. Authors of accepted papers must guarantee that their papers will be presented at the workshop. At least one author of the paper must be registered at the appropriate conference rate. Accepted papers will be published in the ACM Digital Library**. There will also be a best paper award.**

Paper submission site: https://easychair.org/conferences/?conf=cpss2016.

Contact

Email: cpss2016@easychair.org
CPSS Home: http://icsd.i2r.a-star.edu.sg/staff/jianying/cpss/

Horizon 2020 CIP Programme: 40 Million Available for Competition

Soon new opportunities for CIP researchers and operators are coming up. "What are the topics" and "how to build successful a consortia" in this industrial, research and innovation partnership is disclosed from first hand.

The Secure Societies Societal Challenge of the European research programme Horizon-2020 has recently approved by the Member States (MMSS) and the European Commission (EC) a new focus area entirely devoted to physical and cyber-protection for critical infrastructures (CI). Two calls for innovation action projects will be opened both in Spring 2016 and in Spring 2017. In total, the programme will grant up to 20 million Euros each year for selected actions that should include in the consortia, as mandatory, the participation of at least two operators of CI from two different member states and associated countries and, at least, one innovative technological small and medium enterprise (SMEs).

This initiative is in line with the aim of the EC for reducing the vulnerabilities of Europe's CI and for increasing its resilience across all the MMSS and in all relevant sectors of economic activity. The Secure Societies H2020 programme contributes to support the EU's 2008 Directive on European Critical Infrastructures and to build common approaches and tools for the protection, resilience and better understanding and management of their interdependencies. The focus area on CIP within this H2020 Societal Challenge results from the collaboration of both the General Directorate for Migration and Home Affairs (DG-Home) and the General Directorate for Communications Networks, Content and Technologies (DG-Connect), while the overall management and monitoring of the selected projects as well the organisation of the calls and the evaluations will be performed by the Research Executive Agency (REA) of the EC.

Research on physical and cyber CIP is built-up on the experience already tackled in the Security Research domain of the 7th Framework Programme. More than 50 projects were been awarded between 2008 and 2013 in the areas of energy, transport and communication grids, designing and planning of buildings and urban areas, supply chain and cyber-security for CIP (see catalogue of the projects funded under the Security Research Programme in FP7).

Efficient and effective CIP, a European and global challenge

In the last years we have observed how the disruptions in the operation of our national, regional and local CI may put at risk the efficient functioning of our societies and our economies. Some of these disruptions result from natural, man-made hazards or unexpected accidents but, in other occasions, they are the effect of physical and/or cyber-attacks on installations and systems. Furthermore, the increased interconnection among different installations, the scope of the attack (or hazard), and the need of the operators for having to combine cyber and physical security solutions to protect their CI, have arisen the urgency for deploying comprehensive and holistic approaches.

The final aim would be to ensure an effective and efficient protection of our public and private, connected and interdependent installations. On top of that, and because the current global financial crisis, unprecedented budgetary restrictions have been imposed everywhere. So, innovative security solutions must be more efficient and cost-effective than the ones available up to the moment.

Marina Martínez Garcia

Dr. Martínez-Garcia is in H2020 responsible for the Secure Societies Challenge. She is physicist and H2020 Programme Officer at SOST (Spanish Office for Science and Technology) in Brussels. SOST is the EU branch of CDTI (Centro para el Desarrollo Tecnológico e Industrial), which is the Spanish Funding Agency for Industrial R&I belonging to the Ministry of Economy and Competitiveness.

Dr Martinez is also responsible for the collaboration of SOST with the Spanish regions in Brussels and follows the opportunities for SMEs on European R&D and Innovation programmes. She is the coordinator of the capacity building and strategic positioning programme of CDTI in Brussels.

e-mail: marina.cdti@sost.be
Horizon-2020 Programme Officer at the Spanish Office for Science and Technology (SOST-CDTI)
Spanish Ministry of Economy and Competitiveness

What is funded under the Secure Societies CIP focus area?

Both at the end of March 2016 and 2017, the call on CIP at the Secure Societies H2020 programme will open a call for proposals addressed to fund innovation actions that would cover: Prevention, detection, response, and in case of failure, mitigation of effects and consequences (including novel installation designs) over the life span of the infrastructure. The project would also have the aim for achieving the security and resilience of all functions performed by the installations, and of neighbouring populations and the environment.

It is necessary to address not only all the aspects of both physical (e.g. bombing, plane or drone overflights and crashes, spreading of fires, floods, seismic activity, space radiations, etc.) and cyber threats and incidents, but also systemic security management issues and the combinations of physical and cyber threats and incidents, but also systemic security management issues and the combinations of physical and cyber threats and incidents, their inter-connections, and their cascading effects. Innovative methods should be proposed for sharing information with the public in the vicinity of the installations, and the protection of rescue teams, security teams and monitoring teams as well.

The proposals are expected to lead to developments up to Technology Readiness Level 7 (TRL 7), that is, to have as outcome a system prototype demonstration in operational environment. The installations not covered in the awarded projects within the call-2016 will remain eligible in 2017. Thus, the list of CI and sectors eligible for the call-2017 will be accordingly updated once the results of the evaluations of the first call will be communicated (Winter 2016).

In line with the EU's strategy for international cooperation in research and innovation, international partners and international cooperation is encouraged, as the topic aims a global dimension. In any case, international organisations will be eligible for funding only when the EC considers the participation of those entities as essential for carrying out the action.

The **size of the projects is expected to be up to 8 million Euros of EC contribution, which means an overall budget of the project about 11 and 12 million Euros (approximately),** as innovation actions are 70% funded (except for non-profit public or private legal organisations, which are always funded up to 100%). **About 3 innovation action projects per year** are expected to be funded both in the 2016 and in the 2017 CIP calls.

Projects should focus in the following CI, paying special attention in tackling their interdependencies. Each project should, at least, involve minimum of two CI operators from two different Member States or Associated Countries and, at least, one innovative technological SME within the consortium.

The CI considered are: Utilities such as Water Systems and Energy Infrastructures (i.e., power plants and distribution of electricity, gas, oil, etc.), Transport Infrastructures as well any mean of Transport and mobility at urban, regional, national, cross-border and international level, terrestrial and satellite Communications Infrastructure, Health Services (i.e., hospitals, first aid services) and, finally, Financial Services (banking system, stock exchange, etc.).

Funding rate for the projects is 70% (innovation actions,) with a ceiling of 8 M€ of EC requested.

What is expected of the CIP projects?

At short term, it is expected that projects will make a state-of-the-art analysis of physical and cyber detection technologies and risk scenarios, in the context of a specific CI.
Also, an analysis of both physical and cyber vulnerabilities of a specific CI, including the combination of both real situation awareness and cyber situation awareness within the environment of the infrastructure are expected to be delivered.

In the medium term, the selected projects should:
- Present innovative (novel or improved), integrated, and incremental solutions to prevent, detect, respond and mitigate physical and cyber threats to a specific CI.
- Develop innovative approaches to monitoring the environment, to protecting and communicating with the inhabitants in the vicinity of the CI.
- Perform in situ demonstrations of efficient and cost-effective solutions.
- Provide security risk management plans integrating systemic and both physical and cyber aspects.
- Deploy tools, concepts, and technologies for combatting both physical and cyber threats to a specific CI.
- Where relevant, the project should carry out test beds for industrial automation and control system for CI in Europe, to measure the performance of CI systems, when equipped with cyber and physical security protective measures, against prevailing standards and guidelines.
- Also, the project should test the results and validation of models of a specific CI against physical and cyber threats.

As in all H2020 projects and initiatives, efficient and continuous dissemination activities at European level have to be planned in order to target the relevant user communities. Special attention has to be given by showing specific models of information sharing on incidents, threats and vulnerabilities with respect to both physical and cyber threats.

Also the policy side has to be considered by shaping recommend-dations and contributions to relevant sectorial frameworks and European regulatory initiatives on CI.

The innovation actions granted are expected to contribute, as long term impact, to the safety and security standards, and to the pre-establish-ment of enhanced certification mechanisms in the CI domain.

Some hints about a well-balanced consortium

In addition of the compulsory conditions of the action (at least 2 operators from 2 different countries and at least 1 SME), a good consortium should involve key players at industrial level (i.e., operators and industrial security service providers) but also the most advanced and innovative actors in applied research (i.e., private companies, SMEs, technology and research centres of proven close collaboration, dialogue and transfer with the private sector).

As the standardisation dimension has to be present, the project may include the advice (or, if possible, the participation) of entities, well at national or at European level, which have a specific role in the standardisation and certification process.

The consortium has to take attention to the social side so, local, regional or national authorities and first responder bodies should take part in close cooperation with, for instance, citizenship associations of volunteers which are mobilised in case of large scale incidents of such a kind of installations. A complete and realistic environmental impact should be provided by expert private or public entities.

Finally, given the practical aim of the action, test trials and validation exercises involving not only the internal personnel but also all the actors concerned, should be envisioned within the life-time of the project.

Communication is crucial in these projects so, a complete consortium should involve professional expert communication partners which understand the needs for information of all the chain (from citizens to decision makers, inside workers, etc.) and who would be knowledgeable in information management and information tools.

If you would like to know more about the Secure Societies Challenge in H2020 as well to be updated on the latest news and networking and information events about the calls 2016 and 2017 please visit the EC Participant portal where main information is regularly posted.

What is an "innovation action" in H2020?

An Innovation Action (IA) consist in a collaborative project aiming at producing plans and arrangements or designs for new, altered or improved products, services or processes.
For this purpose the project should consider prototyping, testing, large-scale product validations, demonstration activities, piloting and market replications.
In a "demonstration or pilot" it is expected to validate the technical and economic viability of a new or improved technology, product, process, service or solution in an operational (or near to operational) environment, whether industrial or otherwise, involving, if appropriate, a larger scale prototype or demonstrator.
On the other hand, a "market replication" aims to support the first application or deployment in the market of an innovation that has already been demonstrated but not yet applied/deployed in the market due to market failures/barriers to uptake.
Finally, "Market replication" does not cover multiple applications in the market of an innovation that has already been applied successfully once in the market.
In any case, an "Innovation Action" may include limited research and development activities and it is always funded at 70% except for non-profit legal entities, where a rate of 100% applies).

CIPRNet Master Class on Modelling, Simulation and Analysis of Critical Infrastructures (Edition 2)

Rome, 11th – 13th November 2015

Organised by University Campus Bio-Medico of Rome in coordination with ENEA (Italian National Agency for New Technologies, Energy and Sustainable Economic Development)

Scheme: 1 + 1 + 0.5 days lectures and training (3 optional modules)
Language: English

Description:
The second edition of the Master Class on Modelling, Simulation and Analysis of Critical Infrastructures will be delivered following a "module" approach. In each day an optional module will be delivered:

- Module 1 (11th November 2015): notions and theories regarding Critical Infrastructure modelling, simulation and analysis will be described in details. This module is particularly indicated for researchers and any professional needing a general approach to the topic;
- Module 2 (12th November 2015): Decision Support System and consequence analysis, description of the DSS tool developed by ENEA within the CIPRNet project. This module is particularly indicated for any type of audience, including CI operators;
- Module 3 (13th November 2015, morning): Hands-on exercises on DSS. This module is particularly indicated for technicians and researchers needing to practice with DSS.

Audiences:

- CIP Researchers and experts from different research communities (European and non-European);
- Public/governmental authorities in charge of Critical Infrastructure Protection or Civil Protection matters;
- Stakeholders from Critical Infrastructures' operators.

Please find the registration form and more information regarding the second edition of the CIPRNet Master Class at https://www.ciprnet.eu/endusertraining.html.

IMPROVER: Improved risk evaluation and application of resilience concepts to critical infrastructure

The IMPROVER project is a research and innovation action funded under Horizon 2020. Tasked with operationalising resilience concepts applied to critical infrastructure, the project is aiming for a risk-based approach combining different dimensions of resilience in four living labs.

The exposure of critical infrastructure to different emerging and evolving threats, as well as increasing interdependencies between infrastructures, means that large scale crises are occurring with a growing frequency and having an increasingly significant impact on infrastructure.

To respond to these evolving risks, protection is not always an option, largely because of prohibitive costs and difficulties in implementing technological or other solutions to ensure that critical infrastructure assets or systems are fully protected against a range of threats. There is therefore a paradigm shift taking place not only in technological analysis and system design but also on the political level both here in Europe and abroad - from a focus on the protection of critical infrastructure to the resilience of critical infrastructure.

Despite this change and increasing interdependencies between infrastructures, there is no common European methodology for measuring or implementing resilience, and different countries and sectors employ their own practices. Neither is there a shared, well-developed system-of-systems approach, which would be able to test the effects of dependencies and interdependencies between individual critical infrastructures and sectors. This increases the risk as a result of reliance on critical infrastructures, as well as affects the ability for sharing resources for incident planning due to no common terminology or means of expressing risk.

The IMPROVER project, which started on the 1st of June 2015 and runs for three years, aims at contributing to improving infrastructure resilience through the implementation of resilience concepts to real life examples of pan-European significance, including cross-border examples.

Background

The definition of resilience is a contested one, with different definitions for ecological and engineering resilience and some researchers even extending the definition of resilience so that it encompasses protection as well. In IMPROVER, at least at the initial stage, we have been focusing on the engineering definition of resilience, which closely resembles the UNISDR definition of resilience: "[Resilience is] the ability of a system, community or society exposed to hazards to resist, absorb, accommodate to and recover from the effects of a hazard in a timely and efficient manner, including through the preservation and restoration of essential basic structures and functions".

Naturally, because there are many definitions of resilience from different communities and different sectors, there are many frameworks detailed in research literature and applied in practice focusing on its assessment and implementation. These focus either on communities or the infrastructure, but in any case they rely on combinations of different factors to contribute to the overall resilience of a system or a system-of-systems.

Within IMPROVER, we look at these factors as a kind of a resilience tool-kit which is implemented to manage and to increase the resilience of infrastructure, and the society which is dependent upon it. Resilience is therefore a complex construct which relies upon the interaction between the different tools in the toolkit, and the interaction between the tools and the infrastructure in question.

David Lange

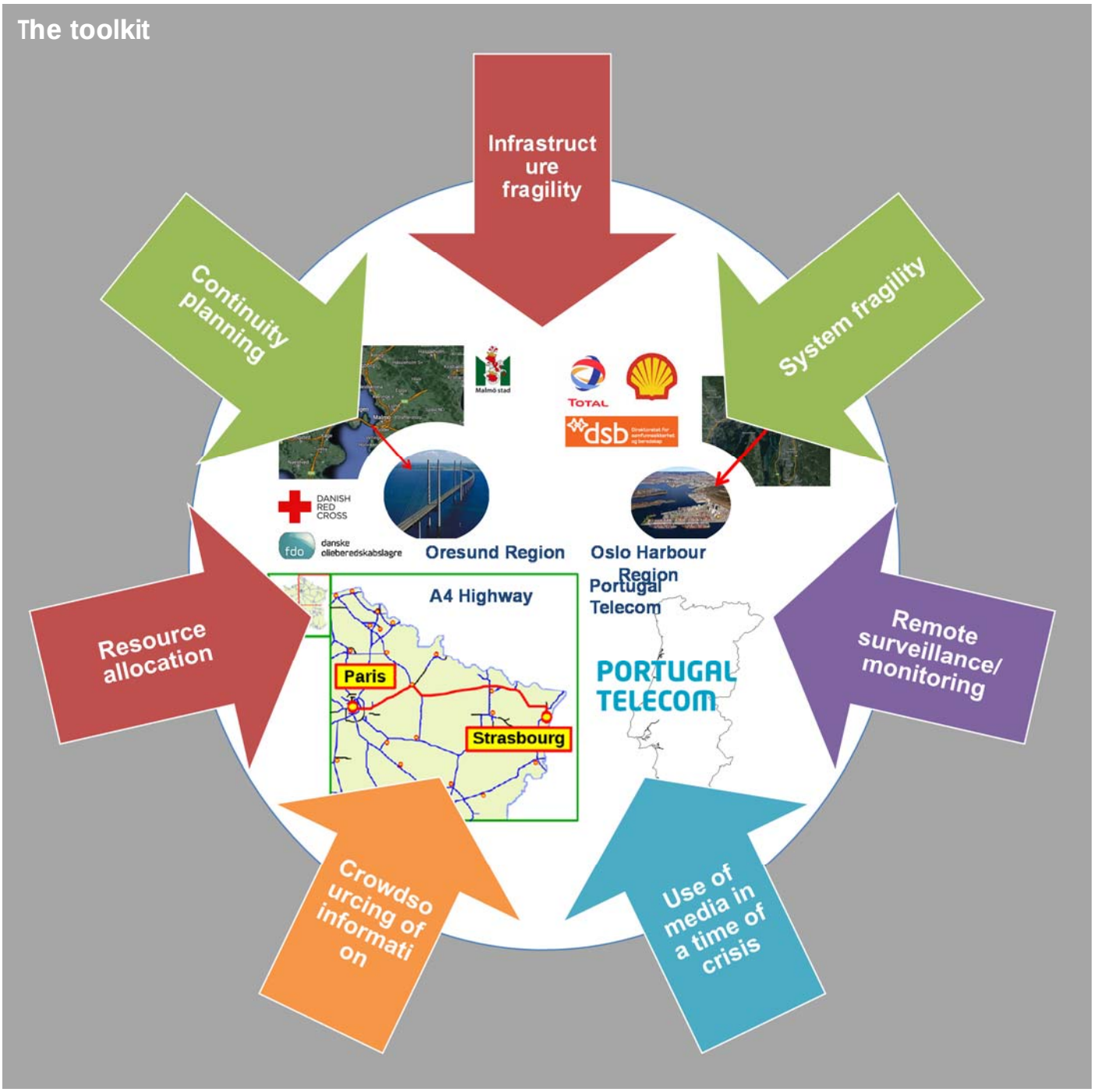
Dr. David Lange is a researcher at SP Fire Research in Borås, Sweden.

e-mail: david.lange@sp.se
SP Technical Research Institute of Sweden, Box 857, 501 15
Sweden

Fanny Guay

Fanny Guay is a project manager at the Danish Institute of Fire and Security.

e-mail: fgu@dbi-net.dk
DBI - Dansk Brand- og sikringsteknisk Institut, Jernholmen 12, 2650 Hvidovre
Denmark



Understanding and operationalising resilience requires a thorough understanding of how these different tools contribute to the fundamental attributes of resilience, such as robustness or recovery of the system in question.

The IMPROVER approach

The project is divided into three stages, which are needed in order to achieve the projects objectives. The first stage is a survey of available approaches for the definition, implementation and evaluation of resilience concepts to critical infrastructure. This will include an extensive literature review, a set of workshops as well as review of ongoing and previous projects both within Europe and globally. The second phase of the project is an evaluation of the available methodologies and the further development of a promising approach to improve its effectiveness, taking account also of existing EU risk assessment guidelines. The final stage is a demonstration of the developed methodology in operation.

In order to properly understand the interaction between resilience concepts which make up the tool-kit and the infrastructure itself we are focussing on 4 'living labs' which represent either clustered infrastructure assets, cross border assets or assets with wide spread geographical dependencies.

In IMPROVER, we will focus on the resilience concepts applied to the infrastructure in these living labs, principally the technological and organisational resilience. In order to assess resilience, it is necessary not only to evaluate the overall resilience of critical infrastructure to threats but also to evaluate the performance and impact of the individual resilience concepts. Working within and across the living labs, the partners in IMPROVER will be able to study resilience concepts acting in isolation and together on the critical infrastructure in order to better

understand the mechanism in which they contribute to resilience. The use of these living labs will also enable us to evaluate and adapt potential existing methodologies for their implementation in critical infrastructure.

This approach using living labs has the advantage of allowing the dependencies, and importantly, the differences between infrastructures to be taken into account when evaluating the different implementations at various stages of the project. This is important when considering that the impact of disasters and crises in Europe is characterised by a highly interconnected society which is increasingly reliant on critical infrastructures providing services which are centralised, if not territorially then contextually. Due to cascading failures through dependencies between critical infrastructure systems, the indirect consequences of natural and man-made disasters may be more severe than expected.

In addition to this focus on resilience of the infrastructure, we will also consider in our overall approach the community resilience, i.e. the combination of societal and economic resilience concepts, through the use of social media and population engagement. The baseline criteria for performance of the infrastructure in times of crises should be based on the response of society to the crisis.

Throughout this work, we will be relying on fields such as resilience, risk assessment, structural engineering (including response of structures to extreme loading), systems analysis, media and communication, crisis management, emergency response, business continuity planning as well as a number of novel and exciting techniques including for example paired comparison, expert elicitation, and crowdsourcing, resulting in improved population engagement.

Next steps

At the time of writing this article, it is just over two months into the projects' three year period. We have been organising our first workshop with different stakeholders and participants in our living labs for the end of September and expect to have a very good attendance from outside of Europe. We have also started our work to evaluate and compare existing approaches for operationalising resilience using the living labs as test cases.

The consortium

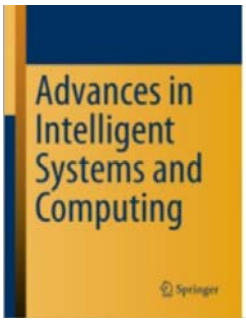
The consortium partners have specific expertise in the different tools which will form our approach. It also includes researchers who are involved in both ERNCIP and the EPCIP programme. The project is coordinated by SP Technical Research Institute of Sweden. The consortium includes 9 additional beneficiaries from throughout Europe including: DBI - Danish Institute of Fire and Security Technology in Denmark, INERIS and the Euro-Mediterranean Seismological Centre in France, the University of Leicester and University College London in the UK, SP Fire Research and the Arctic University in Tromsø in Norway, INOV in Portugal, and the JRC's Institute for the Protection and the Security of the Citizen in Italy.

Acknowledgements

The IMPROVER project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no. 653390

www.improverproject.eu

For updates of the project, follow us on twitter @improverproject and on LinkedIn: IMPROVER – EU Project.



Springer

the language of science

Call for Papers: Advances in Networking Systems: Architectures, Security, and Applications

Aims and Scope:

Modern network systems encompass a wide range of solutions and technologies, including wireless and wired networks, network systems, services and applications. This appears in numerous active research areas with particular attention paid to the architecture and security of network systems. In parallel, novel applications are developed, in some cases strongly linked to rapidly developing network-based data acquisition and processing frameworks. Information security works as a backbone for protecting both user data and electronic transactions in network systems. Protecting the communication and data infrastructure of an increasingly inter-connected world has become vital nowadays. Security has emerged as an important scientific discipline whose many multifaceted complexities deserve the attention and synergy of the computer science, engineering, and information systems communities. This book volume covers a wide range of topics related to networking systems, security, and network applications. The volume will provide comprehensive reviews of cutting–edge state-of-the-art algorithms, technologies, and applications, providing new insights into a range of fundamentally important topics in networking infrastructures and applications. The edited book volume serves as a reference for engineers and scientists by ensemble up-to-date research contributions. Topics of interest include, but are not limited to:

Network Architecture and Systems

- Architecture, scalability and security of network systems
- Service delivery platforms - architecture and applications
- Resource allocation, QoS, and fault tolerance in networks
- Architecture, data allocation and information processing in sensor networks
- The applications of intelligent techniques in network systems
- Software, applications and programming of network systems
- Management, energy and control of Sensor Networks
- Network protocols, algorithms and standards
- Network traffic engineering
- Traffic classification algorithms and techniques
- Wireless communications
- Innovative network applications
- Network-based computing systems
- Network-based data storage systems
- Open data acquisition and exposure systems
- Crowdsourcing systems
- Network systems for large scale data acquisition and processing
- Web services – standards and applications

Security

- Social, organizational and other aspects of information security
- Information security and business continuity management
- Decision support systems for information security
- Digital right management and data protection
- Cyber and physical security infrastructures
- Security and monitoring of sensor networks
- Computer forensic and network security
- Security systems and Surveillance
- Network, cloud and data security
- Misuse and intrusion detection
- Military

Applications

- Social applications
- Environment monitoring
- Transportation & Infrastructure
- Precision agriculture
- Industrial applications
- Home automation
  Entertainment Health-care

Publication Schedule:

The tentative schedule of publication is as follows:

- Deadline for paper submission: **Dec. 01, 2015**
- Author notification: **Feb. 2, 2016**
- Camera-ready submission: **Feb. 15, 2016**
- Publication date: **Q3 / 2016**

More see: http://staff.www.ltu.se/~ismawa/ansasa

RESIN: Resilient Cities and Infrastructures

A new Horizon 2020 project aimed at standardising approaches and delivering decision support tools for cities to support the development of climate change adaptation strategies linking critical infrastructures with other elements of cities.

Background

With most of its population and capital goods concentrated in urban areas, cities are central to a well-functioning European economy and society. However, the concentration of people and assets in cities also renders them extremely vulnerable to the effects of extreme weather events and climate change. When disasters occur in urban areas, they threaten the lives of large numbers of people, critical infrastructure systems, and interregional and global value chains. The combination of increased urbanisation and the increasing consequences of global climate change place an imperative on cities to be proactive in strengthening their resilience to disasters in order to secure their economic competitiveness and to enhance the quality of life for their residents.

City adaptation strategies

Despite this imperative, the development of urban climate change adaptation strategies has been slow. The majority of EU cities are still lagging, and there is a significant north-south divide with cities in southern Europe showing less progress in this regard.

Even where urban adaptation strategies exist, there is a poor integration of different domains, and between critical infrastructures and other city systems. The absence of a standardised approach with regard to the methods for undertaking key tasks such as assessing climate risks and vulnerability, and prioritising between adaptation responses, limits urban adaptation planning. Limited comparability between cities and adaptation options is also a barrier to the provision of national and EU funding for adaptation projects.

And here RESIN comes in:

The RESIN project will develop standardised approaches to help city administrators, the operators of urban infrastructure networks, and related stakeholders to develop their adaptation strategies and ensure that their decisions strengthen the resilience of the whole city. These will be comprehensive by dealing with all elements of the urban system: critical infrastructures, built-up spaces and public spaces, and will cover impact-and-vulnerability assessment and selection of adaptation options. A decision support system will be developed to support decision makers in following a standardised path towards the choice of appropriate and effective adaptation measures into strategies tailored to the particular circumstances of a specific city. RESIN will explore the possibilities and prepare the materials to include adaptation in European standardisation processes.

Project deliverables

To this end, RESIN aims to create a common unifying framework that allows comparing strategies, results and identification of best practices by:

- Creating an urban typology that characterises European cities based on different socio-economic and biophysical variables;
- Delivering standardised methods for assessing climate change impacts, vulnerabilities, and risks;
- Providing an inventory of adaptation measures for critical infrastructures and other urban elements, and developing standardised methods to assess the performance of such adaptation measures;

Peter Bosch

Peter Bosch (MSc) is coordinator of the RESIN project. He works at as senior research scientist at TNO in the Netherlands. In the past years he was involved in the coordination of a large national research project on the adaptation of Dutch cities to Climate change ("Climate Proof Cities"), and other projects supporting cities and the Dutch government in climate change adaptation. He was educated as physical geographer and worked previously for the IPCC and the European Environment Agency.

e-mail: RESIN@tno.nl
TNO
PO box 80015
3508 TA Utrecht
The Netherlands

- Developing an overview of decision support tools in the areas of stakeholder analysis, risk and vulnerability assessment, prioritising between adaptation options and risk reduction strategies, and monitoring and evaluation.
- Collaborating closely with 4 'case cities' for practical applicability and reproducibility;
- Creating a circle of sharing and learning consisting of the core cities together with "Tier 2" cities around them for sharing knowledge and expertise.
- Interacting with European Standardisation organisations to ensure a systematic (standardised) implementation;
- Integrating findings in a coherent framework for the decision making process, with associated methods, tools and datasets.

The consortium consists of researchers with a background in urban climate adaptation (such as the University of Manchester, TNO, Tecnalia) and in risk assessment of critical infrastructures (Fraunhofer, TNO, Siemens). The team includes a large (ARCADIS) and a small (BC3) consultancy experienced in delivering this knowledge to the cities and other customers. Siemens and ITTI are a large and a small business that deliver technical support for managing cities. Four cities from various parts of Europe are a key part of the team. These cities (Bilbao, Manchester, Bratislava, Paris) will serve as a testing ground and are part of the co-creation process to ensure the practical applicability of the research findings. ICLEI, as networking partner, has the capacity to disseminate all outcomes to other cities in Europe. NEN, as member of CEN, the European standardisation body, will take the work forward towards formal standardisation.

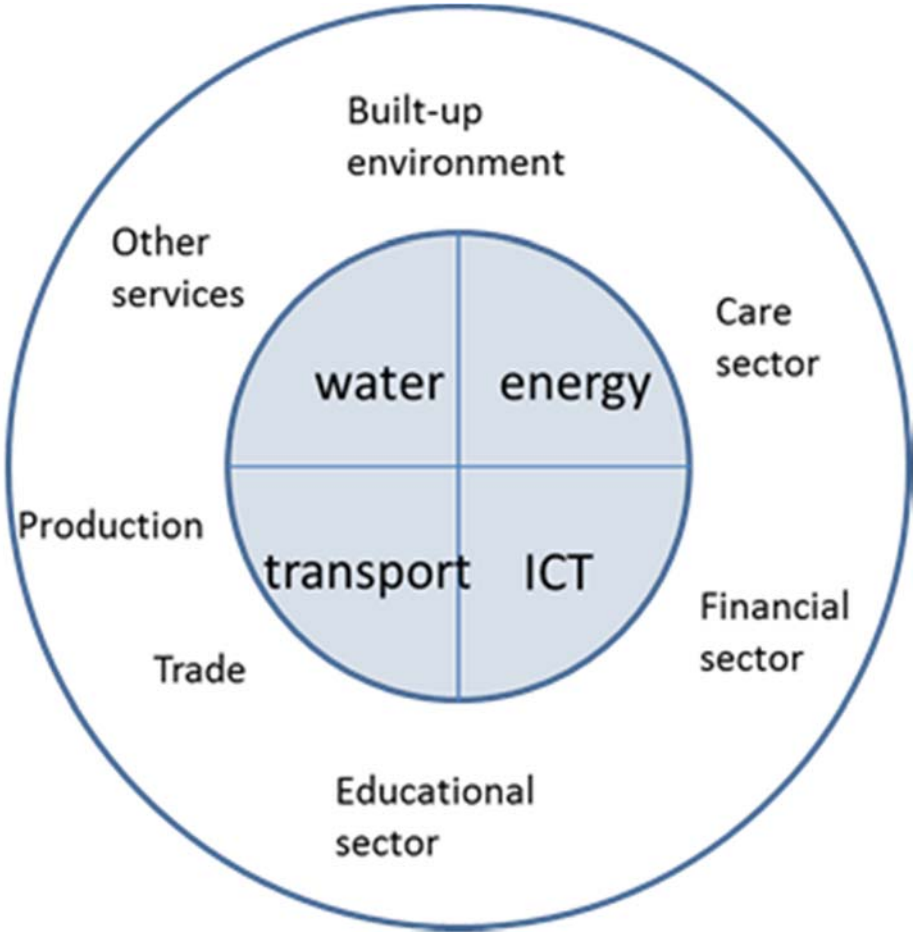


Figure: The cities living and working environment depends on well-functioning infrastructures

RESIN as a project

The RESIN project started in May 2015 and will run for 3.5 years.

UNIRESEARCH will bring project coordination capacities to ensure a successful delivery.

Cooperation will be established with existing European projects dealing with (urban) critical infrastructures and climate change such as INTACT, RAMSES, STREST and PREDICT.

More information

More information about the project can be found already now (and certainly in the near future) on our website: www.resin-cities.eu

Contacts: resin@tno.nl

RESIN has received funding from the European Union's Horizon 2020 programme under grant agreement No. 653522.

RESIN
CLIMATE RESILIENT CITIES AND INFRASTRUCTURES

Poor integration between critical infrastructures and other parts of cities in existing urban climate adaptation strategies formed the starting point of the RESIN project. RESIN will link the existing approaches for climate change adaptation of cities with disaster risk management of critical infrastructures to develop an overall approach for all sectors and elements of the urban system.

Developing a "unifying framework" for the adaptation and disaster risk management process is one of the first steps to be taken in the project.

In developing the subsequent assessment methods and support, we will standardise what can and needs to be standardised.

GRRASP: Geospatial Risk and Resilience Assessment Platform

The development of GRRASP addresses the issue of developing tools for performing analysis of complex networked infrastructure systems.

Critical Infrastructure Protection is getting increased attention as a result of the number of man-made threats (terrorism, malicious attacks, cyber events) and natural disasters. In addition to that, critical infrastructure systems are becoming more and more interconnected with the introduction of ICT technologies and thus isolated events may lead to large-scale or even continent wide disruptions. Interdependencies between critical systems are a key factor that needs to be considered when it comes to the analysis and simulation of critical systems in terms of their resilience. In the US, the NISAC (National Infrastructure Simulation and Analysis Centre) has developed a number of tools for the analysis of CI systems, supply chains, etc. that are tailored for the US reality.

In the aftermath of the terrorist attacks in US and EU the European Commission proposed A European Programme for Critical Infrastructure Protection (EPCIP). The EPCIP was adopted in 2006 and in 2008 the EPCIP Directive was put in force. In 2013 a revised EPCIP was published, clearly mentioning the importance of resilience, interdependencies and impact of CI disruption. JRC responds to this request by developing tools and methodologies. One of them is GRRASP (Geospatial Risk and Resilience Assessment Platform), which aims to bridge the gap of lack of tools for the analysis and simulation of CI at European level. GRRASP is available to be used by CI stakeholders. Furthermore it can be also used for training professionals in the domain of tools for prevention, preparedness and response.

In Europe, most tools are developed responding to national efforts and focus on the specific issues that need to be addressed at national scale. Obviously this approach shows its limitations when it comes to large-scale CI that expand across borders and jurisdictions.

Data sharing is a major issue in the field of CI analysis and this is a parameter that actually hinders development of tools and methodologies for the analysis and simulation of CI.

Collaboration among CI stakeholders is an open issue that is strongly associated with CI analysis and simulation. In order to foster collaborative analysis it is important to make sure that all stakeholders agree on a common terminology and to provide tools enable collaboration while ensuring data security and privacy through the whole analysis cycle.

CI owners and operators have agreed on several occasions the importance of developing tools and methodologies for modelling and simulation in CIP. It is true that in the recent years, an important number of tools have been developed and these can be used for the assessment of a wide number of disruptive scenarios. It seems though that most of such tools lack the features to be used throughout Europe and therefore fail to become standards. In principle, they represent ad-hoc efforts tailored to the needs of a particular region, state or sector. Consequently, often they lack the capability to scale up to international level.

In response to the above-mentioned issues we have developed in JRC the Geospatial Risk and Resilience Assessment Platform - GRRASP.

Georgios Giannopoulos

Dr Georgios Giannopoulos MS Mechanical and Aeronautical Engineering / PhD in Engineering from Vrije Universiteit Brussel / MS Solvay School (Economics & Management).

e-mail:
georgios.giannopoulos@jrc.ec.europa.eu

Luca Galbusera

Luca Galbusera, MSc degree in systems and control engineering / PhD Information Engineering from Politecnico di Milano.

e-mail: luca.galbusera@jrc.ec.europa.eu

Both authors are with:
European Commission
DG Joint Research Centre (JRC / IPSC)
Institute for the protection and security of the citizen
Security Technology Assessment Unit

The main objective is to provide an analysis tool that can be used by MS authorities and operators in order to improve risk and resilience assessment at local, regional, national and international scale. In addition to that we aimed at developing a tool that can be also useful for developing and testing new models as well as for training.

GRRASP tiers and applications

GRRASP can be considered as a hybrid tool that combines the power of GIS systems with mathematical models in order to provide a complete analysis environment with strong visualisation and simulation capabilities. The GIS layer is implemented for data entry (where applicable) and for data/analysis results visualisation as well as for taking advantage of the large amount of available libraries for performing analyses on geospatial data. However, in order to expand GRRASP's capabilities, the computational engine is based on Matlab® developed modules that have been compiled and can be used in stand-alone mode using the Matlab Runtime Compiler (available for download for free). This approach facilitates the interoperability between mathematical models and web based technologies (Apache, Tomcat, etc.).

GRRASP is based on a modular open architecture in order to render the system expandable and scalable to cope with future technology developments (e.g. cloud services). A server-client architecture is implemented in order to facilitate collaboration among users on common projects. Apart from the computational engine, GRRASP is based on a Postgres database where information relevant to models is stored and can be retrieved upon request by the end user. Geoserver, Tomcat, Apache and Drupal technologies (see Figure 1) are used in order to enable to remote users to introduce data, run models and visualise results through their web browser.

As already mentioned GRRASP is developed having in mind the need for a collaborative environment, however, data security is a prerequisite. The architecture implemented in GRRASP strongly considers this element. In addition to that, GRRASP allows (for certain modules) uploading proprietary data, invoking the necessary module, visualising the results and then cancelling all uploaded data. This is an additional level of data security that has been implemented in order to cope with the requirements of the CIP analysis community.

When it comes to the structure of the scientific modules, GRRASP follows a tiered approach (see Figure 2) that facilitates the engagement of actors from various fields and with different expertise.

Tier 1 (sectoral analysis) constitutes the basis of most simulation software for critical infrastructure analysis and obviously there is a reason for this. Research institutes and scientists are often specialised in a particular domain and for this reason there is the tendency to develop detailed engineering models. Typically, such approaches require a high amount of specialised data. On the other hand, these models can provide very detailed descriptions of critical infrastructures and exhibit limited uncertainty, while they often require considerable development time. Further, typically they can only be used by experts in the respective field and the developers have certainly the

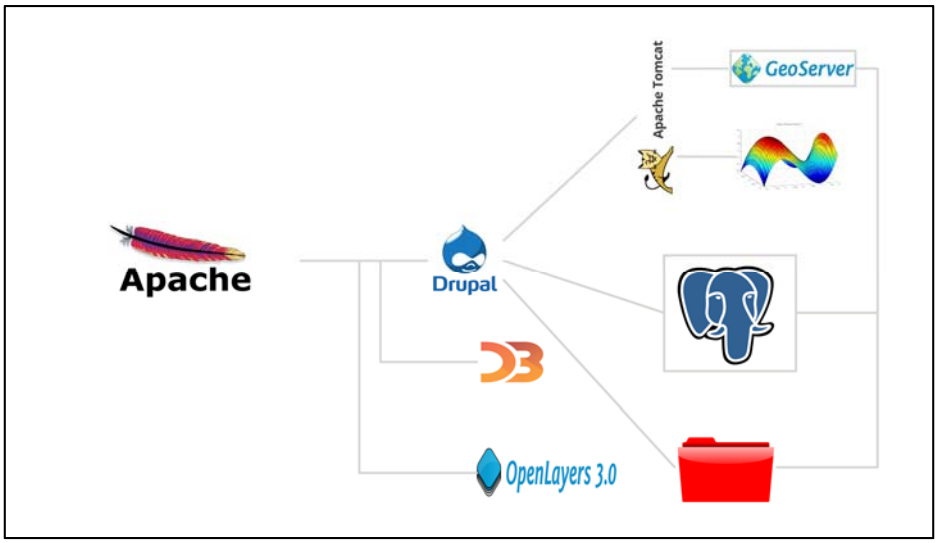


Figure 1: GRRASP architecture

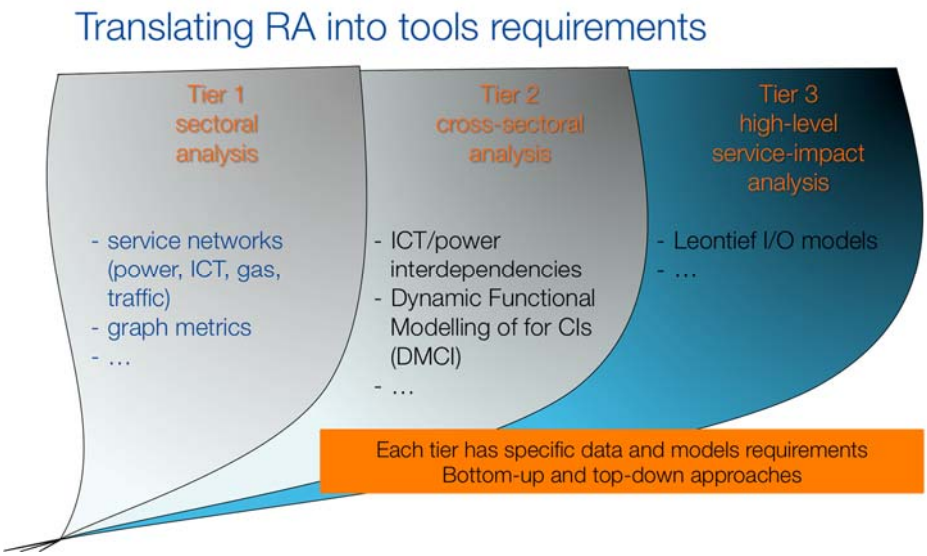


Figure 2: GRRASP tiered approach

primary ownership due to the inherent complexity of such systems. In principle the maturity in this area is high and the vast majority of actors in the field are focused on this particular Tier. In this Tier one may find models that are applicable at all levels (local, regional, national, international), however, their complexity and difficulty rather increases as we scale-up towards national/international level. An example of a model in GRRASP belonging to this tier is the Geomagnetically Induced Current module that evaluates the development of geomagnetically induced currents on power grids due to the variation of earth's magnetic field that follows severe space weather events. Another example is the one of structural analysis of networks (see Figure 3).

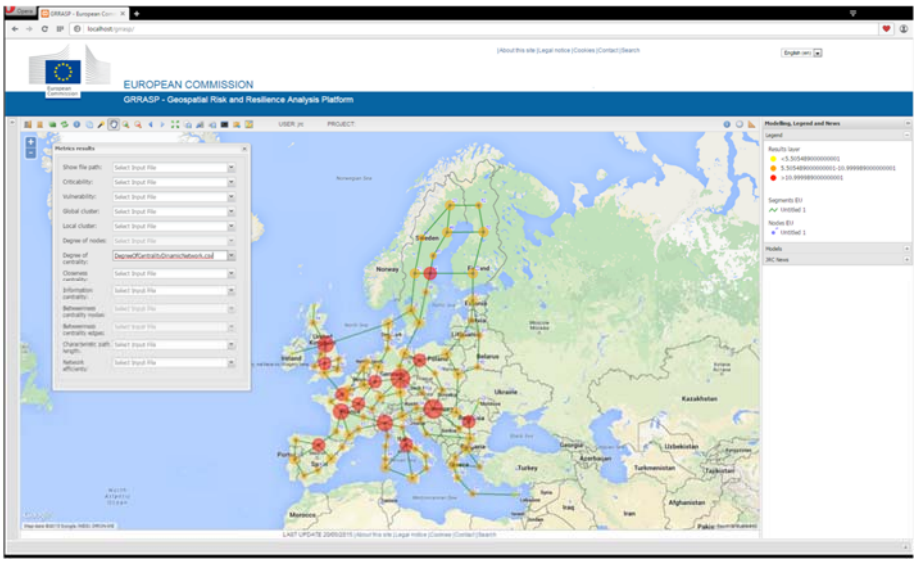


Figure 3: Interface for network metrics in GRRASP

By definition, **Tier 2** (cross-sectoral analysis) includes models that require more knowledge on the interactions between sectors and less specific knowledge on the particular dynamics of a sector. Piecing together models belonging to the first tier while addressing different sectors might lead one to think to obtain an analysis of interdependent systems however, this is not the case. Although this may seem reasonable as a claim, in reality it is strenuous due to the tremendous complexity that this approach would generate and also imply a request for a huge amount of data. So it is necessary to adopt a different approach that focuses on higher-level variables such as demand and delivery of services and in that way interdependent infrastructures can be modelled with less data and also reduced complexity. Here we have much fewer models, although their complexity can be even lower with respect to Tier 1 models. It is important to mention here that Tier 2 models are applicable at all levels but certainly their real strength is shown when it comes to regional and national level. At an international level it is very important to represent large parts of infrastructures with a limited amount of information otherwise there is the risk to go towards first tier models.

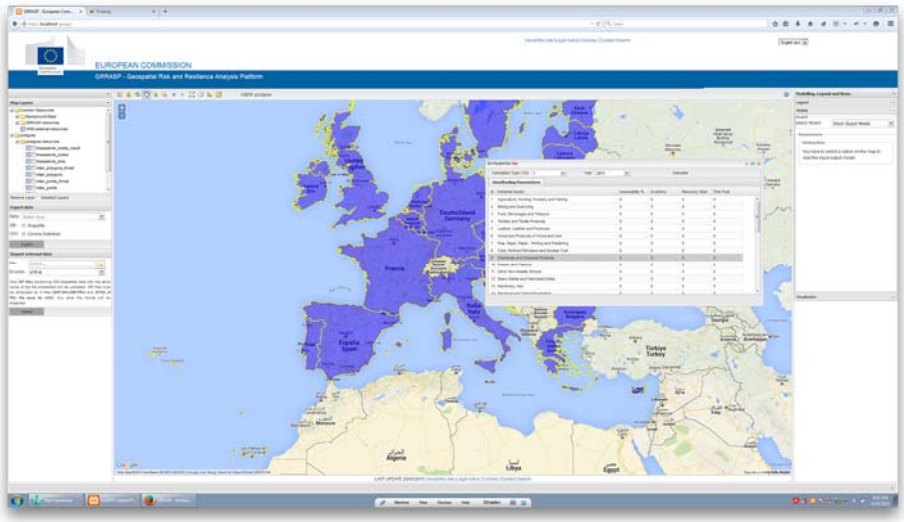


Figure 4: Input-Output model interface

Tier 2 modules are related to the assessment of interdependencies between sectors of critical infrastructures. Interdependencies can be classified as functional, logical, cyber and geographical and certainly a robust interdependencies analysis module should be able to take into account all these types of interdependencies. In order to address this issue we have jointly developed with Polytechnic School of Milan an interdependencies analysis module, the DMCI (Dynamic Functional Modelling of vulnerability and interoperability of CIs)[1] that takes into account the above mentioned types of interdependencies while its modularity enables the end user to define nodes of critical infrastructures on a map and establish cross-sectoral interdependencies among these assets. Among other advantages, this type of tool enables the collaboration of multiple actors in the field thus it facilitates a bottom up approach towards improving the understanding of interdependencies among sectors. Relevant application examples include the impact assessment of power grid disruptions on telecommunications or the effects of a disruption in the rail transports on the road transport network due to the transfer of service demand by the end users.

Tier 3 (high-level service impact analysis) focuses on the assessment of high level impact at regional, national and international level taking input from the modules of Tier 1 and Tier 2, where relevant (see Figure 4). At JRC we have developed an economic impact module that has been introduced in GRRASP and it is based on an inoperability Input/Output

model[3]. This module includes enhanced features in order to describe the dynamics of the recovery process, while taking into account the existence of inventory within certain economic sectors. However, more modules are needed that can address important issues such as regionalisation of the effects of critical events. Although some of these issues this can be addressed, at a first stage, with a Tier 1 module, in that case the output would not be as accurate since high order effects (interdependencies) could be omitted. GRRASP's open architecture allows third party users to enrich the modules portfolio to complement existing capabilities of GRRASP across tiers. Currently the integration of the various modules belonging to different tiers is under development. This will lead to a seamless risk and resilience assessment framework, starting from the assessment of threats at sectoral level leading to estimate interdependencies between sectors and finally reaching the assessment of the total economic impact. The inclusion of further types of impact analysis at Tier 3 is also under development.

In addition to these functionalities, we have equipped GRRASP with the capability to fetch data from remote servers and use them for visualization purposes or for initiating a Risk/Resilience analysis. This functionality enables GRRASP users to set up dynamic and interactive processes for information exchange and sharing of risk maps as well as other geospatially related data. Currently such services are deployed only in a few cases. As an example we provide the case of Italy (see Figure 5) that has set up a portal for this purpose and shares information on risks concerning earthquakes at the level of NUTS 3 areas.

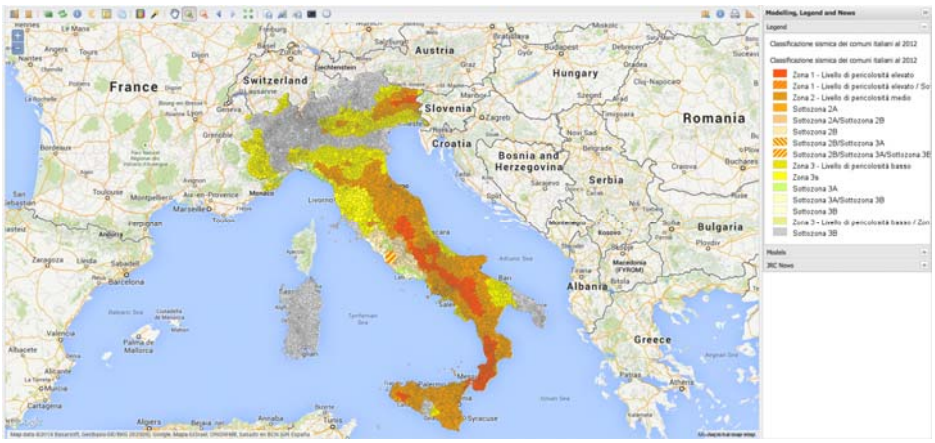


Figure 5: Visualisation of risk maps in the GRRASP environment

Future Work

GRRASP addresses several issues expressed by MS and operators mainly in the domain of tools and methodologies for assessing risks and resilience for CIs. We foresee a further development of GRRASP by introducing more modules, additional applications and a standardised interface in order to include modules by the end users. This will enable the CIP community to expand GRRASP in various directions and render it into a powerful tool for running a series of risk and resilience scenarios for CIs at local, regional, national and international level leveraging the scalability of the system.

In addition to purely Critical Infrastructure related applications, GRRASP enables the analysis also in other domains where the geospatial component is important and where strong modelling capabilities are required coupled with the necessity of a collaborative approach among various stakeholders.

Acknowledgements

GRRASP development has been supported by the "The Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks (CIPS)" Annual Work Programme 2011, 2012 through Administrative Arrangements with JRC. This support is highly appreciated.

References

1. Dynamic functional modeling of vulnerability and interoperability of critical infrastructures, P. Trucco, E. Cagno and M. De Ambroggi, 2012, Reliability Engineering and System Safety, vol. 105, pp. 51-63

2. Identifying groups of critical edges in a realistic electrical network by multi-objective genetic algorithms, E. Zio, L.R. Golea and C.M.S. Rocco, 2012, Reliability Engineering and System Safety, vol. 99, pp. 172-177.

3. Analysing Critical Infrastructure Failure With a Resilience Inoperability Input-Output Model, Olaf Jonkeren and Georgios Giannopoulos, 2014, Economic Systems Research, vol. 26, no. 1, pp. 39-59.

If you would like to know more about GRRASP please visit our website: https://ec.europa.eu/jrc/en/grrasp

Critical Infrastructure Protection: from protection to resilience

A review of critical infrastructure based on uniform criteria and limit values for social disruption that apply to all public, private and semi-private partners in the Netherland

An incident on 27 March 2015 illustrated the dependency of our society on electricity. A power failure left one million households without electricity. Traffic lights stopped working. Trains, metros and trams were out of service and aircraft could no longer land at Schiphol Airport. In the affected area, mobile telephone communications and electronic payment systems were disrupted as well and parts of the businesses came to a standstill.

Guaranteeing the continuity of critical infrastructure is of common interest to both critical (usually private) organisations and to society. Critical infrastructure includes products, services and underlying processes which, should they fail, could cause large-scale social disruption. That is why the government and critical organisations in the Netherlands cooperate in protecting this infrastructure.

Integrated approach

An integrated approach is required, due to the number of parties involved. This is a dynamic and complex domain due to technological developments and interconnectedness of critical processes.

Society has become more dependent on critical infrastructure while the failure of such infrastructure has become less accepted in society. Infrastructure has become more dependent, for example, on IT systems and electricity and has become more vulnerable to (deliberate) cyber incidents.

Moreover, the interconnectedness of critical processes makes it difficult to predict cascade effects. Due to cascading effects the impact can be larger if single processes fail. Critical organisations and the National Government recognise this also on the basis of chain analyses of critical organisations.

Change to a sectorial approach

On behalf of the Dutch Government, the Minister of Security and Justice informed the House of Representatives in 2013 that the policy on the protection of critical infrastructure was to be reviewed. That review has resulted in a new prioritised list of what is considered critical infrastructure in the Netherlands with more focus than before. Instead of a sectorial approach, the relevant processes underlying the products and services are identified. As such, as of 2015, critical infrastructure in the Netherlands is defined in critical processes.

The review has also provided insight into the most important risks, threats, vulnerabilities and the degree of resilience of this infrastructure. Moreover, (more) attention is paid to the implementation of resilience enhancing measures (e.g., security measures). On the national and regional level, businesses, government and scientific institutes work together towards strengthening the identified critical infrastructure processes.

Sven Hamelink

Sven Hamelink (MSc) is program manager at the Dutch Ministry of Security and Justice. He has been working on a variety of topics in the fields of counterterrorism, security and crisis management. He is currently in charge of the national approach for CI resilience.

e-mail: vitaal@nctv.minvenj.nl

Jeroen Mutsaers

Jeroen Mutsaers is a policy officer at the Dutch Ministry of Security and Justice working on (inter)-national security and resilience and climate change adaptation. He is currently involved in the novel national approach for CI and resilience.

Definition of critical infrastructure

A clear definition and identification of critical infrastructure for the Netherlands in 2015 and a suitable policy that ensures and enhances resilience are essential for the national security. For this purpose, the degree of criticality was assessed on the basis of criteria and limit values for social disruption which apply to all public, private and semi-private partners.

Criteria

Criteria were developed based on the National Risk Assessment methodology as used in the National Security Strategy. An integrated impact assessment of the consequences of a failure of the previously identified critical sectors was conducted based on economic, physical and social impact.

Cooperation with partners - Tools and Instruments

In 2015-2018 further action is taken to identify possible new critical processes. Moreover, the aim is to improve accessibility to security tools and, where necessary, develop new instruments for the critical infrastructure. Strategic alliances will be established between businesses, scientific institutes and government.

The review will result in a (more) targeted use of resilience enhancing instruments. For instance, critical infrastructure will be incorporated into the crisis management decision making structures and will be given special attention in the trainings of the National Academy for Crisis Management (NAC). In addition, the National Cyber Security Centre provides its services to businesses in critical processes.

The review has, due to the joint efforts by the relevant public and private partners, resulted in an up-to-date and clear insight into what is critical to our society. The review focusses on the impact on society which resulted into one complete list of critical infrastructure. In future policy and projects, the degree of criticality is used as the guiding principle for programmes and policies.

Categories A & B

A distinction is made between category A and category B in order to reflect the diversity within critical infrastructure, in order to set priorities in case of incidents for example, and in order to allow for individual arrangements if measures are taken that enhance resilience.

New list of Critical Infrastructure

The table on the following page shows the new list of critical infrastructure.

Category A

This includes infrastructure whose disruption, damage or failure will have the type of impact described in at least one of four impact criteria below:

- Economic impact:
  > approx. €50 billion in damage or an approx. 5.0% drop in real income
- Physical consequences:
  more than 10,000 dead, seriously injured or chronically ill
- Societal impact:
  more than 1 million people afflicted by emotional problems or serious problems with basic survival.
- Domino effect:
  failure results in the breakdown of at least two other sectors.

Category B

This category includes infrastructure whose disruption, damage or failure will have the type of impact described at least one of three impact criteria below:

- Economic impact:
  > approx. €5 billion in damage or an approx. 1.0 % drop in real income
- Physical impact:
  more than 1,000 dead, seriously injured or chronically ill
- Societal impact:
  more than 100,000 people afflicted by emotional problems or serious problems with basic survival

NCTV

The National Coordinator for Security and Counterterrorism (NCTV) protects the Netherlands from threats that could disrupt Dutch society. Together with the partners within the government, the research community and the private sector, the NCTV ensures that the Netherlands' critical infrastructure is safe and remains that way.

For any further questions about the protection of critical infrastructure, you can contact the Critical Programme via vitaal@nctv.minvenj.nl .

See next page:
Table on Processes, categories, services, sector and responsible ministry.

Processes	Cat.	Product, service or location	Sector	Ministry
National transport and distribution of electricity	A	Electricity	Energy	Economic Affairs
Regional distribution of electricity	B			
Gas production National transport and distribution of gas	A	Natural gas		
Regional distribution of gas	B			
Oil supply	A	Oil		
Internet access and data traffic	TBD		IT/ Telecom	Economic Affairs
Speech-communication services (mobiles and landlines)				
Satellite				
Time and location services (satellite)				
Drinking water supply	A	Drinking water	Drinking water	Infrastructure and the Environment
Flood defences and water management	A	- primary flood defences - regional flood defences	Water	Infrastructure and the Environment
Air traffic control	B	Schiphol Airport	Transport	Infrastructure and the Environment
Vessel traffic service	B	Port of Rotterdam		
Large-scale production/processing and/or storage of chemicals and petrochemicals	B	Chemical and petrochemical industry	Chemistry	Infrastructure and the Environment
Storage, production and processing of nuclear materials	A	Nuclear Industry	Nuclear	Infrastructure and the Environment
Retail transactions	B	Financial transactions	Financial	Finance
Consumer financial transactions	B			
High-value transactions between banks	B			
Securities trading	B			
Communication with and between emergency services through the 112 emergency number and C2000	B	Maintaining public order and safety	Public Order and Safety	Security and Justice
Police deployment	B			
E-government: the availability of reliable personal and corporate data about individuals and organisations, the ability to share such data, and the availability of data systems which multiple government agencies require in order to function	B	Digital government	Public Administration	The Interior and Kingdom Relations

Swiss Cyber Storm 2015

International IT Security Conference

21st of October 2015
KKL Lucerne, Switzerland

Meet international experts talking about the latest findings, techniques, visions, opinions and lessons learned. With coffee breaks, lunch and apéro riche, the conference provides a lot of room for networking. Thanks to the co-location with the European Cyber Security Challenge, the conference offers an unique opportunity to network with young talents from Austria, Germany, Romania, Spain, Switzerland, and the United Kingdom. All of these countries send a team formed by the winners of their national cyber competition to foster collaboration and to find out who has the best young cyber talents in Europe.

EUROPEAN CYBER SECURITY CHALLENGE
Evil prevails when good humans do nothing!

Featured Talks:

- **Keynote: Why organizations keep getting breached....Still, in 2015**
  Kevin Beaver, Security Consultant, Writer and Professional Speaker, Principle Logic, LLC
- **Flushing Away Preconceptions of Risk**
  Thom Langford, CISO, Publicis Group
- **Threat Intelligence Sharing – Lessons from the Front Lines**
  Patrick Miller, President Emeritus, EnergySec
- **Visibility in the ENISA Threat Landscape**
  Louis Marinos, Senior Expert Risk Management, ENISA

... please check out the full program on our website!

http://www.swisscyberstorm.com

Partners

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für auswärtige Angelegenheiten EDA

Eidgenössisches Finanzdepartement EFD

SATW
Schweizerische Akademie der Technischen Wissenschaften
Académie suisse des sciences techniques
Accademia svizzera delle scienze tecniche
Swiss Academy of Engineering Sciences

Center for Cyber and Information Security and Norwegian Information Security Laboratory

Nations need research support to defend their Cyber Space. Norway reacted early and took coordinated effort.

NISlab

The Norwegian Information Security Laboratory (NISlab) was founded in 2002 and is situated at Gjøvik University College becoming in January 2016 part of NTNU – the Norwegian University of Science and Technology. The group conducts international competitive research in several areas of information and cyber security, supervises Ph.D. research projects in this field and operates study programs in information security at the Ph.D., M.Sc. and B.Sc. level. NISlab leads the national COINS Research School of Computer and Information Security, presenting round about half of Norway's PhD students in the field.

With around 50 affiliated persons, NISlab constitutes one of the larger academic information and cyber security groups in Europe, and has a broad approach to information and cyber security. However, through our focus laboratories, NISlab has a particular focus on biometrics, forensics and information security management.

In Norway, key national cyber security stakeholders have initiated a partnership to establish the Center for Cyber and Information Security (CCIS), a national center for research, training, and education in cyber and information security.

NISlab has in the past five years had more than 80 research publications published in internationally renowned research papers and worked together with around 100 partners worldwide. NISlab hosts and is a member of the Center for Cyber- and Information Security in Gjøvik.

Contact: Dr. Laura Georg
E-Mail: laura.georg@hig.no
www.nislab.no

CCIS

A number of organisations, including the National Police, Industry and Academia, have partnered to create CCIS. CCIS's partners will strengthen the centre's expertise and skills to prevent, detect, respond to, and investigate undesirable and criminal computer based activities. CCIS establishes competence transfer across agencies, companies and sectors. It facilitates research projects that connect industry and government agencies with international research networks, thus helping to build the essential, critical infrastructure to strengthen Europe's cyber and information security. The centre is important because there is a need for extensive international cooperation and long-term research to prepare for tomorrow's challenges.

The CCIS Security of Critical Infrastructures (SCI) group was formed around a long-standing research group at NISlab studying selected aspects of the security and dependability of critical infrastructures at different abstraction levels ranging from national level and supranational dependency and interdependency models to protocols, sensor, and actuator security in process control systems. The SCI group seeks to address these core challenges in close collaboration with national and international partners.

Contact: Sofie Nystom
E-Mail: sofie.nystrom@ccis
https://ccis.no

Laura Georg

Laura is Head of NISlab (PhD in information security, Geneva University) and worked eight years in consulting across various industries. For Deutsche Telekom's consulting unit, she acted as Global Head for IT Risk & Security, before becoming Managing Partner at BaXian AG.
e-mail: laura.georg@hig.no

Sofie Nyrstøm

Sofie is Director of CCIS and a member of the Government new Digital Vulnerability Committee. Previously, she served as Head of Group Security, Telenor Group and Chief information security officer at DNB Bank. Nystrom led the establishment of NorCERT within the National Security Authority.
E-mail: sofie.nystrom@ccis.no

The System Security Lab

Teaching practical security classes requires the existence of lab environments, where students can experience with methods and tools that they learn in theory. This includes attacking techniques that exploit weaknesses and vulnerabilities in computer systems, but also methods and techniques to defend against these attacks.

The goal of the System Security Lab is the creation of a dedicated hybrid network testbed that can be used for educational and research purposes. Hybrid means that the testbed contains both virtualised as well as real hardware components. This lab enables students to conduct cyber security exercises to get hands-on experience and skills in various practical information security topics, e.g., defence and offence mechanisms, incident response processes and security monitoring methods.

The development of the systems Security Lab started in June 2015, and the design of this lab provides:

(1) a high level testing language and a pre-defined catalogue of a wide range of exploits and defence techniques, which ease the design and deployment of the testing topology and infrastructure;
(2) customisable scoring engine that can be used for different types of experiments; and
(3) security monitoring infrastructure that enables the deployment of a wide range of agent sensors that corresponds to the conducted experiment and its associated vulnerabilities.

Besides the educational role of the lab, it provides the underpinning infrastructure for conducting research experiments in different areas of research, e.g., in software security, security testing, security monitoring, and software defined networks.

Contact: Assoc. Prof. Basel Katt
E-Mail: basel.katt@hig.no

The Forensics Group

The CCIS Testimon Forensics Group evolved from an academic research group established in September 2010 to a partnership and close cooperation with Norwegian law enforcement agencies (LEA), including the Norwegian Police Directorate, Norway's National Criminal Investigation Service (KRIPOS), the Norwegian National Authority for Investigation and Prosecution of Economic and Environmental Crime (ØKOKRIM), the Norwegian Police University College (Politihøgskolen), and regional LEAs for instance the Oslo and Vestoppland police disctricts.

CCIS Testimon is an education and research environment, in particular for Digital and Computational Forensics. It is in charge of a Master of Science (MSc) specialisation track on Digital Forensics within the MSc Information Security (i.e. MSc Information Security / Digital Forensics) offered by Gjøvik University College. In addition, CCIS Testimon offers an Experienced-based Master in Digital Forensics and Cybercrime Investigation in cooperation with Politihøgskolen.

CCIS Testimon conducts fundamental research and applied research on behalf of LEAs. Members of the group contribute to forensic casework, expert witnesses, and advisory services in cooperation with partners, e.g. EC3 - Europol Cyber Crime Centre - AG Internet Security, and NRGD - Nederlands Register Gerechtelijk Deskundigen - Ministry of Security and Justice, The Netherlands.

In addition, Testimon members are involved in networking and community-building activities in the computing and digital forensic sciences, e.g., conferences, workshops, tutorials, and invited lectures such as the International Workshop on Computational Forensics (IWCF), and the Technical Committee (TC6) on Computational Forensics under the auspice of the IAPR – International Association of Pattern Recognition.

The current Testimon-research agenda is focusing on three main topics:

- Big-data Forensics and Forensic as a Service using secure computing infrastructure,
- Cloud Forensics and Cybercrime Investigation, and
- Mobile & Embedded Device Forensics (IoT, IoE).

This research agenda is in line with major strategies by the Norwegian police and European cyber-security strategy.

An example of on-going research projects is *ArsForensica*: Computational Forensics for Large-Scale Fraud Detection, Crime Investigation and Prevention. Funded by the IKTPLUSS programme of the Norwegian Research Council. The four-year project involves excellent research environments from Norway and abroad, such as the United Nations Interregional Crime and Justice Research Institute, the University California Santa Cruz, USA, the Kyushu Institute of Technology, Japan, the Netherlands Forensics Institute, the University of Groningen, Netherlands, and the Norwegian Computing Centre.

Contact: Prof. Dr. Katrin Franke
E-Mail: katrin.franke@ccis.no

The Biometrics Lab

Since its inauguration in 2011, the Norwegian Biometrics Laboratory (NBL) has evolved significantly in terms of the number of PhD students and its research activities. It is a fruitful lab to brainstorm and to generate new ideas for projects. NBL is an essential part of NISlab / CCIS and represents an active focus point with currently four ongoing EU research projects under the FP7 framework program. The projects namely *FIDELITY, INGRESS, ORIGINS* and *PIDaaS* deal with biometrics and identity management. Two additional project proposals are under evaluation at this moment. Moreover NBL is serving industry on bilateral research activities and has also established a project relationship with the Nasjonalt ID-senter (NID) and supports with its research and

testing future decisions that are taken. Also on the national level NBL was awarded recently with the *SWAN* project, which will be funded by the Research Council of Norway under the IKTPLUSS program.

NBL's biometric research is covering various physiological and behavioural biometrics including 2D- and 3D-face recognition, iris recognition, fingerprint recognition, finger vein recognition, dental biometrics, ear recognition, signature recognition, gait recognition, keystroke recognition, gesture recognition and mouse dynamics.

Furthermore, the lab focuses on privacy enhancing technologies such as biometric template protection and integration in physical and logical access control.

The Biometrics lab is an active member in the European Association for Biometrics (EAB), and organiser of several international conferences on Biometrics such as the IEEE BIOSIG conference and the EAB-RPC conference.

NBL is also representing Norway in the COST ACTION IC 1106 and was in this role organising the 3rd International Workshop on Biometrics and Forensics (IWBF'15), which took place in Gjøvik on 3-4 March 2015.

It is the intention of NBL to increase the awareness of biometrics in Norway via the Norwegian Biometric Forum (NBF) that is meeting twice a year. The lab also contributes to the international standardisation in the field and have organised the international standardisation conference ISO/IEC JTC1 SC37 in June 2015.

Contact: Prof. Dr. Christoph Busch
E-Mail: christoph.busch@hig.no

The Information Security Management Group

The adage "manage or be managed" when applied to security management can be expanded to read to continually learn to manage yourself and your organisation efficient and effectively with the right incentives or you will end up being managed by your enemies. The Information Security Management Group conducts theoretical, empirical and applied/ clinical research to modelling, measuring and managing information security management problems. The group leverages its academic research into the national arena by collaborating with the Norwegian Center for Information Security (NorSIS) to help organise and arrange the Norwegian Security Roundtable three times an year and participate in the annual national cyber security awareness month. Below is a picture from the 2013 kick-off of the Norwegian Cyber Security Awareness Month where one of the founding members of the ISMG gave a speech to explain "manage or be managed adage of the group. The speech was entitled "Edward Snowden: The Revenge of the Nerd" and outline how the Snowden affair was mainly a problem of poor security management rather than weak or inadequate security technologies.

Professor Kowalski (centre) NORSIS previous Directory Tore Larsen Orderløkken (right) and Nils Kalstad Svendsen (left) the previous leader of NISlab.

The group also has a special responsibility for the information's security management track of the MSc at University College Gjøvik. Consequently its research based teaching methods bring together a broad spectrum of socio-technical systems security research results that cover the social, organisational, psychological, legal, ethical, cultural, political, rhetorical educational and technical aspect of cyber- and information security management.

Contact: Prof. Dr. Stewat Kowalski
E-Mail: stewart.kowalski@hig.no

Critical Infrastructures Lab

The Critical Infrastructure Lab serves to co-ordinate research across the wide spectrum of security and resilience questions in national and supranational critical infrastructures particularly from the tighter integration of infrastructures using information and telecommunication systems, but also the embedding of computational and communication capabilities within the infrastructure elements themselves.

Research hence includes work at higher abstraction levels such as the analysis of dependencies and interdependencies among infrastructures and their dynamic changes, which was initiated by members of the lab in the late 1990s and continuing to evolve along with the infrastructure itself.

Many critical infrastructures also rely on control systems; this has attracted considerable attention in recent years. Research in the lab has focused on novel attacks and resilience mechanisms against the observability and controllability of control systems, particularly in areas where stability and timeliness is of importance such as in electrical power networks including smart grid environments, and continues to investigate attacks specific to such cyber-physical systems where in-depth modelling yields important insights. Whilst also applicable to general industrial control systems, the main emphasis is on the energy sector as the application domain, however, with a number of European and national projects providing support.

Given the complexity of the problem space, understanding risks and vulnerabilities cannot be achieved exhaustively, nor can all possible contingencies be considered; both the construction of scenarios and systematic attack models, as well as incident response mechanisms also have their place within the confines of the laboratory; given the frequent need to co-ordinate among entities and dependencies among not just the information technology but also the physical infrastructure, these

challenges are distinct from those encountered in a purely ICT-based environment; it is also at the same time more difficult to clearly identify the threat sources and actors as these are known to have a wide range of capabilities ranging from individuals to nation state actors.

Collaboration with partners from government including national security authorities and emergency services, but also the defence sector is important in understanding the scope of challenges and contributing not only to advancing the scientific and mathematical knowledge but also to contribute to the resilience of society to faults and attacks; similarly, close collaboration with industry is crucial in understanding present and future challenges in infrastructure security as well as providing the ability to collaboratively approach such challenges. Cooperation with national critical infrastructure operators such as Telenor, Statnett, and Statkraft as well as other infrastructure providers ensures timely and relevant research.

Contact:
Prof. Sokratis Katsikas
E-Mail: sokratis.katsikas@ccis.no /
Prof. Stephen Wolthusen
E-Mail: stephen.wolthusen@hig.no

European Projects

The areas of research that occupy NISlab's focus groups have already been mentioned with some details above. NISlab and CCIS comprise a large number of researchers in the various topics of cyber security; it is a dynamic and motivated group of young but seasoned academics and researcher with ample research background and with a strong international network. The researchers continuously engage in identifying project opportunities and developing high quality national and international consortia. For years, NISlab has been at the very top of the list of institutions in Norway with the largest EU-funding per researcher. For several years now researchers at NISlab have been well acquainted with responding to EU calls for proposals and with obtaining research funding from the various schemes and EU programmes.

NISlab's research interests are well aligned with the focus areas and themes in the European Commission's Horizon 2020 programme under the so-called pillars on Excellent Sciences, Societal Challenges and Industrial Leadership. NISlab has taken on various roles, including as participating partner, as coordinator, or as individual researcher through the MSCA programme.

The Research Council of Norway has played a key role in providing support to the research strategy and activities at NISlab by financing research through their funding schemes --most recently three important projects have been granted funded under its ICT-Pluss programme. But also RCN has contributed importantly with NISLab by making funds available to support the proposal development stage in responding to major EU calls.

Florissa Abreu
E-Mail: florissa.abreu@ccis.no

National Cyber Defence: Preparedness handling attacks on all level

Cyber act of war, Espionage, sabotage subversion: How to organise and prepare against it? See Norwegian approach below.

Thomas Rid states that there will be no war only in cyber, and he divide the threat into espionage, sabotage and subversion (Rid, 2011). This grouping of the threat is partly supported by Director of National Intelligence (DNI). But he only has two groupings, espionage and cyberattack (Clapper, 2013, p. 1). By studying the past, what kind of hostile activities have we seen so far, and would any of these activities lead to war. In the end how to organise to face this challenges.

Cyber act of war

The threshold of a cyberattack being an act of war is hard to find. NATO states in the latest strategic concept that cyberattacks may reach a threshold that threatens national and Euro-Atlantic prosperity, security and stability (NATO, 2010). This is in line with Article 4 of NATO's founding treaty regulating consultation among the parties. USA has made an International Strategy for Cyberspace (The White House Office, 2011). This one states the right of self-defence, and it also states that cyberattacks may be faced with all necessary means. In Norway a cyberattack is linked to serious injury or death for personnel or material damage (Forsvarets høgskole/Forsvarets stabsskole, 2013, p. 190). This could lead to war. Stating war is a though a political decision, but linked to the criteria. These three examples show there is a possibility of a cyber act of war. But the aggression of the act is not defined.

Then a closer looks upon the three different groups of cyberattacks, and the severity which they may inflict to a nation.

Espionage

First we have espionage. Espionage in cyber is common to espionage in real life. Most of the states have an intelligence service trying to get as much information as possible on potential advisories. If a spy is cough in his activities on foreign ground, the case would be as a criminal act and handled by the police or the security services. In cyber it is hard to discover the person or organisation behind while the activity is underway. Cyberspace is borderless and the digital activity takes place on a different physical place than the location of the person or organisation behind. Even though there is an attribution problem there may be possible to point at someone doing espionage. USA has accused Russia on spying on the White House mail system[1]. In the early stages of the Sony hacking case in 2014 there had to be an espionage activity in order to find and exploit the data in the servers. Espionage is a large threat both to a nation or a company. Both the Director of the National Security Agency (NSA) and Richard Clarke have raised the issue. And they name the flow of vital information as "death by a thousand cuts"[2] (Rosenbaum, 2012). By this they state that the information stolen by espionage may threaten a nation's political or economic future. A company may lose their patents or business strategies, and thereby weaken their marked position in the years to come. In the end these activities are only criminal activities, which have to be faced by taking those behind to court or by inflicting sanctions on those supporting the activity.

Nils Gaute Prestmo

LtCol Nils Gaute Prestmo is a Army Signals officer and has more than 25 years of service. He currently serves in the staff of the Norwegian Cyber Defence in the operations branch. Last year he was a student at the Norwegian Defence Command and Staff College. This spring he delivered a master thesis on Cyber Security.

e-mail : nprestmo@cyfor.mil.no
Norwegian Cyber Defence
N-2617 Lillehammer
Norway

[1] Source http://edition.cnn.com/2015/04/07/politics/how-russians-hacked-the-wh/, 10th. August 2015

[2] "Alexander referred to the growing number of hacking incidents targeting US technology and corporate trade secrets as 'death by a thousand cuts." Source http://www.hstoday.us/focused-topics/cybersecurity/single-article-page/us-facing-death-by-a-

Sabotage

Secondly there is sabotage. Sabotage in cyberspace is inflicting something through the digital world (Von Solms & Van Niekerk, 2013). Known sabotage actions are the STUXNET attack on Iranian nuclear facility and operation Orchard [3] on Syrian air defence system. The first one is against a governmental research facility and was executed by introducing malicious malware on offline systems (Rid, 2011, p. 17). The second one was targeting Syrian air defence systems making it possible for Israeli fighters to enter Syrian airspace undetected (Rid, 2011, p. 16) . Both were targeting the nation's ability to build nuclear weapons. Only the last caused effects outside the systems. The fighters targeted facilities and thereby probably both inflicted personal death and material destruction. Critical infrastructure is vulnerable to cyberattacks. In most of the nations around the world they are owned by private companies. The energy sector is often mentioned. In Brasil in 2007 there was a large blackout which was initially blamed on cyberattack [4]. It was later revealed that poor and lacking maintenance was the cause. In 2014 there was a large national outage in Turkey. Some media speculated on a large cyber-attack, but this was not confirmed (Senel, Hirsti, & Bruland, 2015). The indirect consequences of a power outage may be serious, and may lead to deaths among the population. The director of NSA, Admiral Mike Rogers, has stated that the energy sector is Americas Achilles heel [5]. To modern armed forces sabotage in cyberspace may hamper military operations, or even stopping them. Operation Orchard demonstrating what could be done to sensors. The Sony hacking case demonstrates the possibility to delete servers and making information unavailable.

Subversion

In the end there is subversion. Subversion is about changing the perception on subjects. It ranges from both defacing webpages and false twitter messages to large scale information operations. A false twitter message from Fox stating the death of president Obama, made the values on the stock exchange to drop [6]. Today we see large subversion attacks as a part of information operations in Ukraine. The pro-Russian fighters are controlling the electronic communication (ECOM) infrastructure in eastern Ukraine (Franke, 2015). By controlling the ECOM infrastructure there are multiple ways to perform hostile acts. Physical access to the net is vital for performing various cyberattacks. Controlling the network gives the possibility to deny access for certain users. All this together adds up to a favourable position to effectuate information operations. Few or none news agencies have formalised a cooperation regarding cyber security. In Norway the former national radio and Television Company, Norsk Rikskringkasting (NRK), has a formalised cooperation with NorCERT. During the process the journalists raised their voice and opposed the cooperation. They didn't want to lose their independence [7]. On the other side NRK didn't want to get in such a position where advanced cyberattacks could misuse their servers for hostile acts.

Sabotage is so far the only act in cyber which may lead to war. And the seriousness is judged on physical effects by the politicians. Espionage is influencing the power balance in advance and during war. Finally subversion are inflicting political decisions prior to and during war. Even though it's hard to find and prove quantitative effects caused by cyberattacks, there are some examples where a nation has responded by offensive means. According to the media USA blocked North-Korean internet access as a response to the Sony hacking case (Fackler, 2014). There are also articles on USA starting offensive actions as a response to several attributed cases over the last years [8].

How to organise

As describes in the previous text ownership of critical infrastructure (CI) is mostly private companies. They are exposed to sabotage, but the nations will be those who face the consequences. When looking into how to organise for handling the threat from cyberattacks there may be preferable to discuss two approaches. One approach is only focusing on the public part of the nation, while the other approach focuses on both the public and the private dimension of the nation.

Common to both approaches are the various Computer Emergency Response Teams (CERT) and Computer Security Incident Response Teams (CSIRT). These are related to the various sectors such as finance, energy, health etc. They are linked together both nationally and international, and they share information on threats and handling of these. Nationally there is often a national CERT on top level coordinating the information flow and reporting the government. Internationally there are organisations like European Union Agency for Network and Information Security (ENISA), Forum of Incident Response Teams (FIRST) and Fi-ISAC. They all share a function of sharing information and best practice. In case of cyberattacks the various national sectorial CERT and CSIRT are the entities to handle it on tactical level. There are no other response structures or incident handling organisations in cyberspace ready to respond and support. This is neither nationally or internationally. The only exception is NATO rapid reaction team [9]. The team is a part of the NATO Computer Incident Response Capability (NCIRC).

---

thousand-cuts-in-cyberspace/4ac6f26957f17cafb8611b6fa5899622.html , 7th. May 2015

[3] Source http://en.wikipedia.org/wiki/Operation_Orchard, 8th. May 2015

[4] Source www.wired.com, "Brazilian blaxckout Traced to Sooty Insulators, not hachers", 9th August 2015

[5] Source https://www.nsa.gov/public_info/_files/speeches_testimonies/ADM.ROGERS.Hill.20.Nov.pdf, 5th May 2015

[6] Source http://www.theguardian.com/news/blog/2011/jul/04/fox-news-hacked-twitter-obama-dead , 5th May 2015

[7] Source http://www.klassekampen.no/article/20150113/ARTICLE/150119981, 5th. Mai 2015

[8] Source http://www.reuters.com/article/2015/09/01/us-usa-cybersecurity-russia-exclusive-idUSKCN0R12FE20150901 ,20th September 2015

[9] Source http://www.nato.int/cps/en/natolive/news_85161.htm

The first approach has focus on governmental structures and public systems. On one side the formalised command relations between decision makers and execute level is positive for prioritisation. In case of crisis or war the resources may be stretched, and the need for prioritisation is urgent. When focusing on public systems and having a large cyber capacity it's possible to focus on hostile states and state sponsored actors. On the other side this may narrow the focus area. The USA has several public organisations dealing with cyber security. The American model is criticized by Ricard Clarke (Clarke, 2009). He states that there is too much focus on offensive capacities. And the defensive capability is only focusing on governmental and public systems. In his article he is not discussing whatever the large offensive capability would deter potential adversaries. As the threat to public services is mostly espionage, there has to be a system of collaborating with private actors on handling sabotage and subversion. CERT and CSIRT, even in private sector, are mostly reporting incidents and handling incidents. They are not prioritising among each other. Laws and regulations on private ownership in Critical Infrastructure may not be enough to engage these actors in a cooperative venture to increase national cyber security.

The second approach and another way to organise are to have a stronger focus on public private cooperation. On one side this approach tries to establish a common interest in national cyber security. In the Dutch Cybersecurity strategy they describe cooperation between public and private entities (National Coordinator for Security and Counterterrorism, 2013, p. 24). In the first version of the strategy they described a process of coordination. This showing there is a development in making preparations to handle the threat in cyberspace. Thereby shifting wording from coordinate to cooperate. On the other side this approach challenges some areas of historical and sectorial responsibility. In many nations there are constitutional responsibilities linked to the different sectors. The energy sector is run by the Department of Energy, the telecom may be run by the Department of Transportation and so on. When responding to large crisis or war this "stow pipe organized" sectors need to cooperate in order to face the intra sectorial threats such as the cyber threat. A model of colocation could provide better information sharing in such a system. Instead of the information following organisational structures to the government, a colocation of assets on operational level may better the information sharing and the building of a common situational awareness. The link down to the different CERT and CSIRT could also benefit from such collaboration. Colocation of the assets does not remove the constitutional responsibility given to the sectors, but it may shorten the time for making the proper counter measures when facing cyberattacks of various kinds.

Preparedness

In the end declaring war is a political decision even in cyberspace. But the politicians need the facts and figures from the various national entities. Even though nations face harassing cyberattacks they may not be on the level of starting a war. These attacks may call for other counter actions than offensive military operations. In order to face the threat in cyberspace there need to be a good public private cooperation. Sabotage by cyberattacks against private owned systems such as energy critical infrastructure or electronic communications critical infrastructure may have severe consequences on a nation. These attacks could inflict death and material damage making it an act of war due to the consequences. Subversion as part of information operations in cyberspace may shift public opinion and hamper political decisions. The cooperation between public and private actors need to be formalised and organised in a way to speed up the response of various types of cyberattacks, and thereby gathering the nation's resources in a joint venture to counter the attacks. Colocation of resources on operational level could be a way of creating a common ground for cooperation.

Bibliography

Clapper, J. R. (2013). US Intelligence Community Worldwide Threat Assessment. US Senate Select Committee on Intelligence.

Clarke, R. (2009). War From cyberspace. National Interest.

Fackler, M. (2014, Dec 28). North Korea Accuses U.S. of Staging Internet Failure, New York Times. Hentet fra http://search.proquest.com/docview/1640597714?accountid=8017

Forsvarets høgskole/Forsvarets stabsskole. (2013). Manual i krigens folkerett. Oslo: Forsvarssjefen.

Franke, U. (2015). War by non-military means.

National Coordinator for Security and Counterterrorism. (2013). National Cyber Security Strategy 2 - From awareness to capability. NCSC Hentet fra https://http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/NCSS2Engelseversie.pdf.

NATO. (2010). Strategic Concept For the Defence and Security of The Members of the North Atlantic Treaty Organisation. Lisbon.

Rid, T. (2011). Cyber War Will Not Take Place. Journal of Strategic Studies, 35(1), 5-32.

Rosenbaum, R. (2012). Richard Clarke on Who Was Behind the Stuxnet Attack. Smithsonian Magazine.

Senel, E., Hirsti, K., & Bruland, R. S. (2015). Strømmen tilbake i Istanbul, NRK.no.

The White House Office. (2011). International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World: White House.

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. computers & security, 38, 97-102.

The 49th ESReDA Seminar on:

Innovation through Human Factors in Risk Assessment and Maintenance

October 29-30, 2015, Clos Chapelle-aux-Champs, B-1200, Brussels, Belgium

www.esreda.org

Several research projects and programs on system safety engineering and Quantitative Risk Analysis in the last 40 years offered very strong evidence of the crucial role that human and organizational factors (HOFs) play in major accidents. According to this increasing concern toward the relevance of HOFs in limiting safety performance of complex socio-technical systems, considerable research effort has been spent worldwide in the last couple of decades. Rich literature covering areas from theoretical bases, to accident investigation methods and application to major disasters, to very sophisticated modelling approaches and techniques of HOFs in Quantitative Risk Analysis.

Contributions of the senior researchers involved in the Marie Curie Project InnHF **www.innhf.eu** address for instance the challenges described above. Addressing these challenges is carried on through the formalization of theoretical and applied approaches able to integrate the current and to develop advanced assessment methods. The integrating approaches should comply with the recommendations and requirements expressed by recognized industrial standards and methodologies. Required approaches should be easy to use but and completely integrating human factors and comprehensive system health management approaches.

The aim of the seminar is thus to share within a wider scientific and technical community, to discuss and to compare the results of the proposed approaches, demonstrating how they can be translated into a factual design improvement initiatives for new or existing plants, machinery and critical infrastructures. Seminar's conclusions should be able to provide leverages to achieve competitive and safe performances of complex systems (maximum availability, minimum unscheduled shutdowns of production incident and accident, economic maintenance and increased resilience etc.

Topics include (but are not limited to):

- Risk assessment and management techniques
- Human and organisational factors assessments
- Resilience Modelling and Simulation
- Decision Support Systems (DSS)
- Data collection, expertise & treatment
- Reliability and maintenance
- Prognostic, health monitoring & management
- Maintenance modelling and planning
- Maintenance effectiveness: indicators and measures
- Maintenance & incidents/accidents occurrence
- Maintenance: standards and specifications

Contact:

Michala Demichela micaela.demichela@polito.it
Politecnico di Torino (Italy)

Mohamed Eid mohamed.eid@cea.fr
CEA (France)

Seminar Place:

https://www.uclouvain.be/66833.html

RICS: Research Centre on Resilient Information and Control Systems

The Swedish approach to secure Critical Infrastructures' IT

Introduction

In September 2015 a Swedish research centre on Resilient Information and Control Systems (RICS) was launched to address societal critical functions in several critical infrastructure domains. RICS will be financed by the Swedish Civil Contingencies agency (MSB) over a period of five years totalling 20 MSEK (roughly 2.1 M€). The project leader Professor Simin Nadjm-Tehrani at Linköping University is happy to find this important topic on the agenda for Swedish research and development and presents the goals and motivations for the centre as follows.

Parallel with the growing role of information technology (IT) in business and society we see an alarming wave of computer-based failures leading to breaches of availability and integrity. Industrial control systems (ICS) are among applications with the highest availability and performance requirements. In this project we address the security threats against those ICS on which the critical infrastructures (CI) in society depend, among them power distribution networks, water and heat management systems, and other applications for which we find actively interested stakeholders during five years of the project. One of the main challenges in this sector is the blurring of the borders of the technical system, so far run as an isolated application with proprietary components and protocols, and the business IT, potentially connected with every day communication platforms. Another challenge is the complex nature of these systems which makes understanding of the functional and security related operational modes difficult, even for the most experienced operators. The absence of investments in research and competence building in the area of security-safety in ICS in Sweden has resulted in shortage of competence in terms of young workforce and researchers trained with the right mind set. Our project proposes to strengthen the security of ICS in CI (ICS-CI) using three connected pillars of research:

A) Data generation

Through collaboration with the defence research establishment, FOI, and relevant stakeholders in society we develop methods for creation of realistic datasets based on operational data or meaningful emulations of systems. The generated data using these methods will be a foundation for experimental research through the capability to replay on the current NCS3 test bed at FOI, and encompasses both normal and abnormal (subject to attack or benign failure) modes of operation.

B) Attack modelling and risk analysis

We develop techniques to create reusable models of attacks and malfunctions, and through exposing the simulated or emulated test networks (with extended capability compared to NCS3) characterise the vulnerabilities and concretise the risks to a CI, including the ensuing safety risks.

C) Real-time detection

We develop methods and tools to perform real-time monitoring of systems of comparable complexity to today's ICS-CI, based on adaptations of the concept of anomaly detection. This will include identifying the specific characteristics of the domains under study so that false positive rates are at acceptable levels, and mapping the verdict of the monitoring system to meaningful messages understandable for the operators, thereby enhancing their reaction and mitigation capability.

The first ingredient (A) above is in itself a valuable contribution to international research, provided that open data sets based on the collected or generated data can be created (this

Simin Nadjm-Tehrani

Prof. Nadjm-Tehrani is the coordinator of RICS, and leads the Real-time Systems Laboratory at Dept. of Computer and Information Science at Linköping University, Sweden. She has recently led a national project as a pre-study in the area of Internet of Things and security within the area of critical infrastructures, and for the past four years acted as a member of the scientific advisory board at the Swedish Civil Contingencies Agency.

e-mail: simin.nadjm-tehrani@liu.se

will obviously be subject to clearance by stakeholders). We plan to participate in exercises run by FOI together with a range of relevant stakeholders. Among the main stakeholders we expect the Swedish national grid (Svenska Kraftnät). The data thus collected will be used as an input when designing the platform that can be used for repeatable replay of (insensitive, cleaned) data streams. This improves the ability to develop relevant tools that can be adopted by industry, and increases the understanding about these systems among stakeholders. The data emulation layer thus created as an interface to the underlying test bed will be of a generic nature, so the applicability of the method in new sectors within ICS-CI is also a major contribution.

The second ingredient (B) above is a means to strengthening the societal functions in terms of preventative measures. Today's CI operators have several functions outsourced to external cloud services and their understanding of the risks and potential attack vectors is dependent on proactive analysis built within the operational environments. Given adequate inputs from stakeholders, from (A) above, RICS demonstrations of the methods for identifying weaknesses and vulnerabilities will be built on case studies recognisable by the stakeholders. Extending attack models in RICS will thereby include dealing with issues of scale and complexity that arises in networks with heterogeneous (and cloud-provided) services. Efficiency of the methods will be based on reusability, and their relevance based on combined safety and security analysis.

The third ingredient (C) brings an improvement on today's ability to react to and deal with adverse events by more precise and timely detection of these in the context of ICS-CI. A main part of detecting adverse events in real-time consists of identifying the features of the systems to be monitored. To monitor the vital IT processes in a SCADA environment, irrespective of which borders the data transgresses and where certain services are delivered, is a challenge in today's networked environments and RICS will address it as follows. The characterisation of the network structure, vulnerabilities, and potential attack vectors in part (B) above will create the relevant inputs to selection of features to be monitored. The created data sets in collaboration with our stakeholders in part (A) above, form a base for validation of our real-time anomaly detection algorithms in realistic scenarios. The attack models obtained based on work in (B) above will be used to test and verify the real-time adverse event detection in part (C) and used in demonstrative case studies in presentations to stakeholders.

RICS will operate as a national research centre with contributions from three strong research teams. The two teams that collaborate with the Real-time Systems Laboratory at Dept. of Computer and Information Science at Linköping University are the groups led by Dr. Magnus Almgren at Dept. of Computer Science and Engineering at Chalmers, and Professor Mathias Ekstedt at Industrial Information and Control Systems at the Royal Institute of Technology (KTH).

LINKÖPING UNIVERSITY

CHALMERS UNIVERSITY OF TECHNOLOGY

KTH VETENSKAP OCH KONST

Collaborating partner:

Swedish Defence Research Establishment (FOI)

Active Stakeholder: Swedish National Grid

Funded by: Swedish Civil Contingencies agency (MSB)

MSB Myndigheten för samhällsskydd och beredskap

Watch this space: www.rics.se

Elevating identity and access management to the digital era

Identity and access management is no exception to the digitisation of everything. The use of biometric features, behavioral aspects and physiological technologies is just around the corner, bringing new authentication and authorisation methods to the market.
Another wave of technology disruption or an actual business need?

Era of digitalisation and disruptive technology

The unprecedented explosion of technology disruption and innovation, the velocity of change and the tremendous impact on businesses are ultimately forcing a large number of industries to increase the pace at which they do business and transform technology.

At the same time, the need for increased data and information protection cannot be overstated.

> "The new digital ecosystem of connected entities, people and data requires an integral identity and access management, beyond the purpose of regulatory and security compliance."

The recent Ashley Madison hack (stolen personal information from a website dedicated to matching up people who want to engage in extramarital affairs) is prime evidence that the management of identities and accesses goes beyond the purpose of regulatory and security compliance.

It impacts the society as a whole and plays an important role in today's cyber ecosystem.

Cyber threats

Identity and access management must be re-aligned with today's digital and cyber ecosystem.

With the digitisation of everything, the classical perimeter of an organisation is disappearing, leading to an increased and complex exposure to potential cyber threats.

The range of the perimeter now includes the authentication and authorisation to and from the corporate organisation or the multiple types of users (e.g., employees, customers, business partners, third parties and suppliers) through multiple channels.

Customer-centric and resilient to cyber identity fraud

Traditionally, organisations have managed their identities and accesses primarily by focusing on the internal employees accessing corporate-wide internal applications. For many organisations, this remains an actual challenge, which requires continuous funding and available skills to maintain a sustainable state.

It is therefore not surprising that identity and access management continues to be a key priority on the agenda of information security.[10]

With the new reality of a digital and cyber ecosystem, organisations have no other choice but to extend the scope of identity and access management with the additional two aspects

1) customer-centric (especially for the external types of users who are accessing their trusted organisations) and

2) resilient to cyber identity fraud.

Maurice Bollag

Maurice works as a Senior Manager at EY (former Ernst & Young AG) in EMEIA Financial Services Advisory, IT Risk and Assurance & IT Advisory. He is a FINTECH advisor specialised in Cyber, IT and Information Security, IT Risk and IT Service Management.

e-mail:
maurice.bollag@ch.ey.com

[10] EY Global Information Security Survey 2014 "Get ahead of cybercrime", October 2014.

1. Customer-centric

Customer behaviour is changing in many ways. The following two examples highlight the reasons why a customer-centric identity and access management is key to building and retaining customer trust in the organisation they are working with:

a) End user acceptance and usability of usernames and passwords

In the digital ecosystem, customers have to manage multiple intercommnected identities.

This makes it very challenging to use the traditional management of usernames and passwords.

Customers are getting tired of and increasingly frustrated with the tedious and inconvenient processes involved in managing those identities.
The Millennial Generation (also known as Gen Y) might have been used to it, but the subsequent Generation Z will certainly not accept it.

Can we image how Gen Z would feel about accepting the use of indefinite usernames and passwords to enable their access to a web service? Will Gen Z accept having to prove who they are instead of being recognised automatically (authentication based on who they are, not what they remember)?

b) Increased customer awareness of security reliability

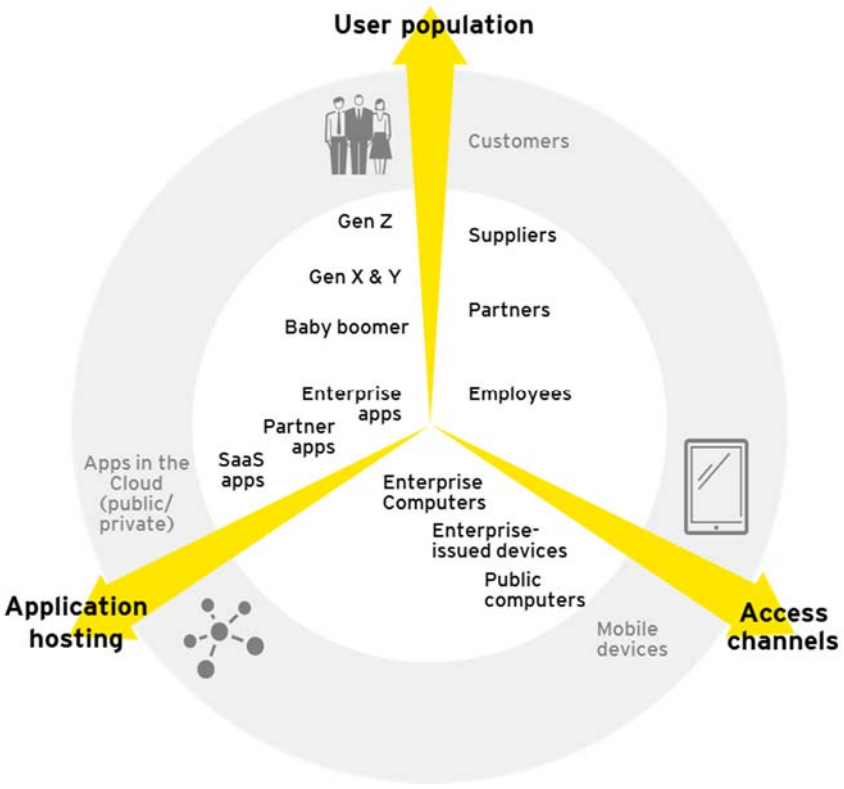
Society has become more aware of the risks related to information security. Customers are feeling less secure about the reliability of usernames and passwords to protect their personal data.

Even good habits and best practices of password management (e.g., different and strong passwords for each used service) are no longer secure and effective enough to protect from identity fraud and theft. Analysis of root cause for identity fraud and theft incidents often includes a flawed authentication method.

Therefore, providing customer-centric identity and access management will become a key factor in ensuring customer satisfaction and trust.

2. Resilient to cyber identity fraud

Indeed, breaches have been occurring for a long time, but their impacts have never been so severe. Incidents which are directly or indirectly related to weak management of identities and accesses are becoming a persistent business operational risk (e.g., damage to reputation, intellectual property, ability to serve customers, financial impact).



Regulations around the world are imposing rules, enforcing mandatory public disclosure of any breach (and even attempted breaches) that compromised personal or financial information and notification of affected consumers within a pre-defined timeline. Non-compliance will be subject to increased fines.

The recent Ashley Madison hack could not have been a better wake-up call. It impacts the society and can have consequences far worse than any financial impact.

Customers will no longer accept and trust companies who cannot demonstrate their ability to protect personal data and privacy.

Innovative solutions for authentication and authorisation methods are emerging to disrupt current practice, but their success will depend on whether they arrive on the market with a pre-installed system for protecting data privacy. (see figure next page Identity and Access Management)

Technology trends

A possible way to address this challenge is to deploy innovative authentication and authorisation methods.

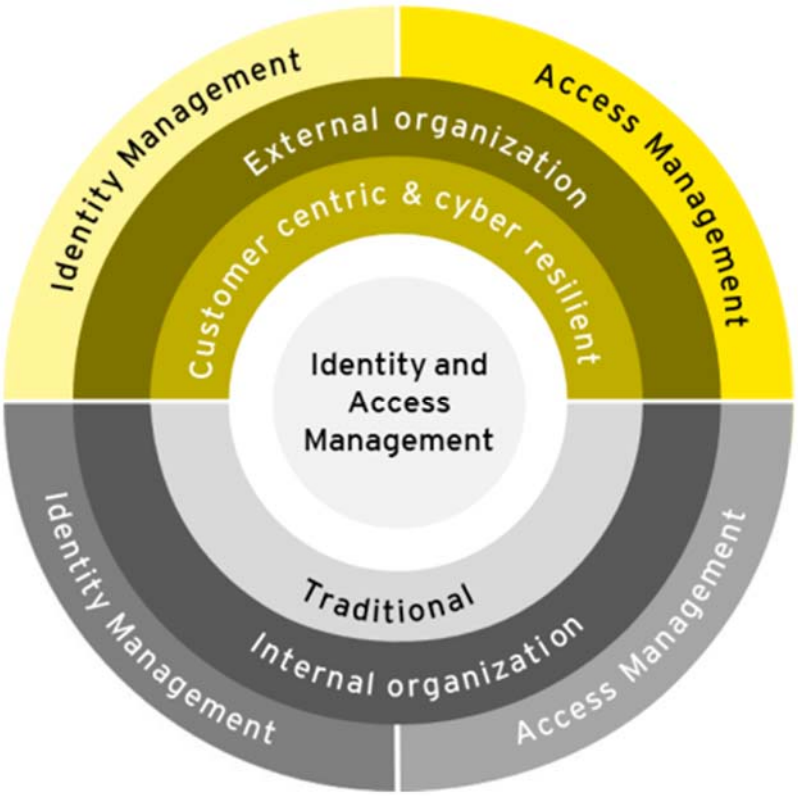
Research has been conducted to predict the key developments and roadmap of current and future identity and access management technologies.

At the end of the day, consumer perception of confidence and trust will play a key role in the success of each technology.

The following list is an overview of the new methods:

Context-based

Authentication and authorisation are driven by a risk context, taking into account criteria such as geographical location, physical device, time and duration of a user's request to access a service. The measures of authentication and level of authorisation dynamically change according to the actual contextual information and risk level.



Biometrics

Authentication and authorisation are based on digitalised biometrics from a human being such as fingerprint, facial or voice recognition – methods that have actually been in place for many years. The latest biometric frequency, vein, palm, iris, DNA, handwriting and even tattoos. technologies include other physical human elements such as heartbeat.

Behavioral

Authentication and authorisation are based on personalised gestures such as hand-eye coordination, keystroke dynamics or cursor movements. Algorithms and patterns of interaction might be combined to set the behavioural criteria.

Which technology will ultimately succeed is difficult to predict. A combination of different technologies might become the future best practice. The new technologies will have to prove their advantages before passwords become obsolete in the near future and assert themselves against emerging and future trends in password security (Password 2.0). However, what certainly can be predicted is that the cultural, geographical and industrial differences are going to play a key role. Offering choices of authentication methods for different locations and user populations might lead to a greater appeal and acceptance.

Cultural and geographical tendency

A global organisation will have to consider the cultural differences in the region they operate in and its online customer base. We have seen countries which have emerged and directly embraced new technologies. Others, however, have adapted their technology, but face challenges due to a lack of user acceptance.

Industry tendency

The question is "how" rather than "which" specific industry will be impacted. The following examples from three industries highlight the differences relating to the "how": the banking industry, which has been dealing with identity and access management for a while, the automobile industry and the smart home industry. The last two are becoming increasingly relevant to our private lives.

Banking

The strongly regulated financial industry has improved its capabilities of managing its identities and accesses over the last couple of years. Nonetheless, a digital banking business model requires massive adaption to its identity and access management methods to support upcoming digital banking services. Mobile and peer-to-peer payments, crowd funding as well as trading and lending functions need to be customer-centric and resilient to cyber identity fraud.

Automobile

Connected cars have to offer simple and secured authentication and authorisation methods. For example, access to the car could be provided based on biometric data such as fingerprints. Car owners might need to think about authentication and authorisation in the future, but car producers definitely must start to integrate secure and easy to use security functions.

The question is "how" rather than "which" specific industry will be impacted.

Smart home

Last but not least, society will have to start thinking about authentication and authorisation of their digitised home rooms, devices and furniture.

Three actions to be taken today

The industries and organisations need to start extending the scope of their current identity and access management model and elevating it to the digital era by:

- Assessing the current state and evaluating its current digital transformation journey to include adapted identity and access management methods.

- Assessing their ability to detect identity fraud and threats and readiness to respond to potential incidents.
- Reviewing the current technology, operating model and governance to effectively and efficiently include integral identity and access management beyond the purpose of regulatory and security compliance.

Conclusion

The new authentication and authorisation technologies have tremendous potential.

It is a business and a customer need. A business need for a robust resilience against identity fraud and cyber threats.

A customer need for a more convenient and trusted method of authentication and authorisation.

With the speed at which the digitalisation process is taking place, it will not be long until we find out which emerging technology will assert itself.

However, the challenge remains to introduce these new technologies with a watertight protection of data privacy.

Asset Management and Critical Infrastructures: Differences and synergies

Micheline W.A. Hounjet,

Micheline is a creative and strong connector between various fields of delta technology. With her background as an engineering geologist, she is not only active in the cross-over between technical disciplines, but also focuses on the link between technology and people. She is keen to find innovative solutions to help people manage flood risks, increase stakeholder participation for urban development and gain insight in integral critical infrastructure impacts in Delta regions. Serious gaming, information tools and visualisation techniques for crisis management are her main interests.

e-mail: micheline.hounjet@deltares.nl

J.M. IJmker - van Gent

Janneke is a communicative team player who translates her work into impacts for the natural system and stakeholders. As a physical geographer she has an eye for the "will" of the natural system itself, which results in more effective measures. To stakeholders, she expresses the results of her work into recognisable units, for example the task for dike enforcement in The Netherlands in euros and the uncertainty in hydraulic heads in 2050 in a bandwidth of costs. Her main interest is to accommodate decision-making with clear, unambiguous, fit-for-purpose information. Combined with her organisational skills, this has led to her present role in implementation of asset management in civil engineering.

e-mail: janneke.ijmker@deltares.nl

At Deltares there is a team of researchers on Asset Management and a team of researchers on Critical Infrastructures. Both focus on infrastructure networks, however their approaches seem to be different. What do these teams have in common and what are the differences between both research subjects? Janneke IJmker van Gent from the Asset Management team and Micheline Hounjet from the Critical Infrastructures team met to discuss these points (see figure 1).

Propositions

For this discussion several propositions and questions were raised:

- In many research calls, the Critical Infrastructures topic is linked to natural and man-made hazards. Has the Asset Management topic the same approach to hazards?
- Asset Management has its stakeholders at the maintenance and risk management departments of asset owners. Critical Infrastructures has its stakeholders at the risk management and crisis management departments of these asset owners. Is there overlap?
- For Critical Infrastructures interdependencies are very important. Does Asset Management take interdependencies into account?
- What types of data do both groups use?
- How do the different teams communicate with the end-product users and their stakeholders?

Hazards

Critical infrastructures research usually takes severe disruptions into account. These disruptions can be caused due to natural hazards or human errors. Sometimes Critical infrastructures are mentioned in combination with climate change, but usually heavy rainfall, storm surges, etc. are meant. For Asset Management long-term maintenance planning is important and climate change is certainly a topic that is mentioned. For instance in the Netherlands most assets are aging and efficient asset management has high priority. But it is not only the aging effects that need to be considered. Climate change effects are added threats for these assets.

In general Critical Infrastructures handles "what happens after a disruption, what are the impacts" while Asset Management handles "how to optimise performance and minimise failure and nuisance in the future". For each network the focus is a bit different: A dike system built to retain water is designed to perform during rare, extreme occasions, but some other networks are built for optimal performance in daily life situations under less extreme conditions.

Stakeholders

The Critical Infrastructures Team is mostly in contact with crisis managers from network owners, industries, governmental bodies and crisis organisations. It is quite easy to talk to crisis managers about extreme events. For example, when the team talked to risk managers from the same organisations, discussion quickly turned to chances of occurrence. However, it was difficult to get them interested in events that have an occurrence of less than 1 every 100 years.

The Asset Management Team approaches risk managers, network owners and governmental bodies. Risk assessments are a substantial part of the work related to Asset Management. These risk managers are involved in decision-making when daily performance is concerned. Their approach is much more detailed as they monitor performance constantly and they are trained to solve issues and outages as quickly as possible.

Deltares recently set up a new national research group with different Asset Management stakeholders. It is called ROBAMCI. The goal of this research initiative is to initiate projects where industry and research partners team-up. Until now, three projects on water management related assets have been launched.

These projects help Deltares to understand the needs of different organisation levels: Strategic, Operational and Tactical. They need different levels of detail and deal with different time intervals for disruptions and consequently handle decision making for future measures differently. It is essential that the outcome of this research exactly match to the needs of the end-users.

Figure 2: Different organisational levels within asset owners

(Inter)dependencies

Currently, the most important research questions for Critical Infrastructures at Deltares evolve around cascading effects between networks and the simulation and visualisation of them. The challenge is to look at a region or a city as a system of systems.

In contrast, the focus of Asset Management is on single networks and long-term adaptation strategies for climate change effects.

Both teams are now exploring whether knowledge on interdependdencies could be beneficial for Asset Management and how detailed Asset Management knowledge could be used for cascading effects simulations and impact models.

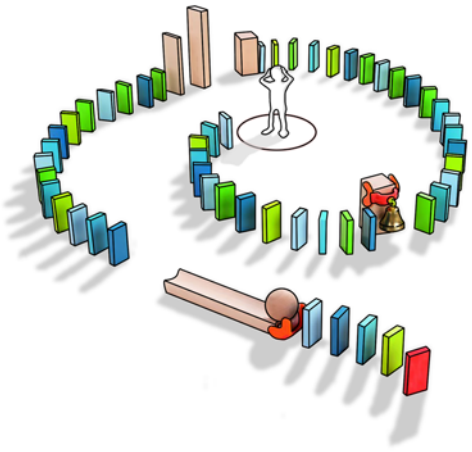


Figure 3: Stakeholder participation workshop for Critical Infrastructures

Data

As mentioned above, for Asset Management detailed risk management is necessary and sometimes available as well. But still there is a need to include knowledge and experiences from the different stakeholders as well (see table 1). It is therefore vital that these different parties work together.

	Data	Experience	Knowledge	
Government				
Industry				
Knowledge Institutes				

Table 1: Overview of parties with data, knowledge and experience for Asset Management.

For Critical Infrastructures it is difficult to receive detailed network data from stakeholders as it is classified. Deltares developed a method that is based on the use of open data combined with expert knowledge and experiences. The idea is that when different network owners discuss consequences with each other and share the knowledge of their own network, there is enough knowledge to evaluate cascading effects after a disruption. This method is called CIrcle and uses an interactive

Figure 1: Janneke IJmker-van Gent (l) of the Asset Management Team and Micheline Hounjet (r)of the Critical Infrastructures Team discuss research and overlap of these topics.

tool for data-mining during the discussion and visualisation techniques to simulate the results of this discussion.

Communication

For Asset management it is vital to communicate research results exactly on the right level of their end-users. ROBAMCI also pays attention to this aspect in their case studies and research projects. The third year of the program is especially designed for communication of results.
For Critical Infrastructures and cascading effects it was difficult to get stakeholders thinking about interdependencies. It seemed too complicated and many assumed everything would just fail at once. Deltares noticed that when the issues were visualised in a simple and understandable way, stakeholders were eager to think about it and

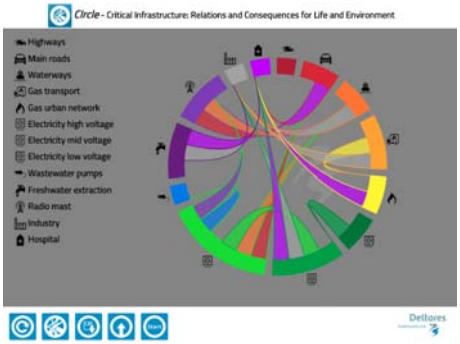


Figure 3: CIrcle tool.

share their knowledge. The level of detail that can be reached with open data can be enough to raise awareness and discuss these issues together. With the discussion results and sometimes more detailed data that is donated after a workshop session, cascading effects evaluations are carried out.
One of the workshops that were organised was for a Water Board. For the celebration of a flood that occurred in 1916 within their area, they wanted to have a visualisation that would show the difference in effects when the same flood would occur in 2016, as civilisation is now more dependent on networks as it was 100 years ago. This simulation will be used by the Water Board to raise awareness on cascading effects.

Example research projects

The research goal for Critical infrastructures focusses on cascading effects at the moment and interactive ways to visualise them and to discuss protective measures. The city of Jakarta is used as a case study. Open data was gathered and a workshop was organised with CIrcle to collect more local information.
For this case study Deltares is now developing a 3D, interactive environment in which cascading effects are visible and will change for different flood scenarios or when for instance the level of a vulnerable object is modified. The accuracy level of this project is at the moment lower than it is required for an Asset management projects.

For the ROBAMCI project in the Beemster polder, performance of important assets of the local water board, such as roads, dikes and pumps, has to be optimised for future situations, under climate change effects, increasing need for transparency and reducing funds. To identify every asset's contribution to risk reduction, a failure mode and effect analysis (FMEA) was carried out. The study is used to identify to what function it is best spending one Euro, so where one Euro creates the largest risk reduction. The method was shown for the Beemster polder, but to achieve reliable results, highly detailed data is required.

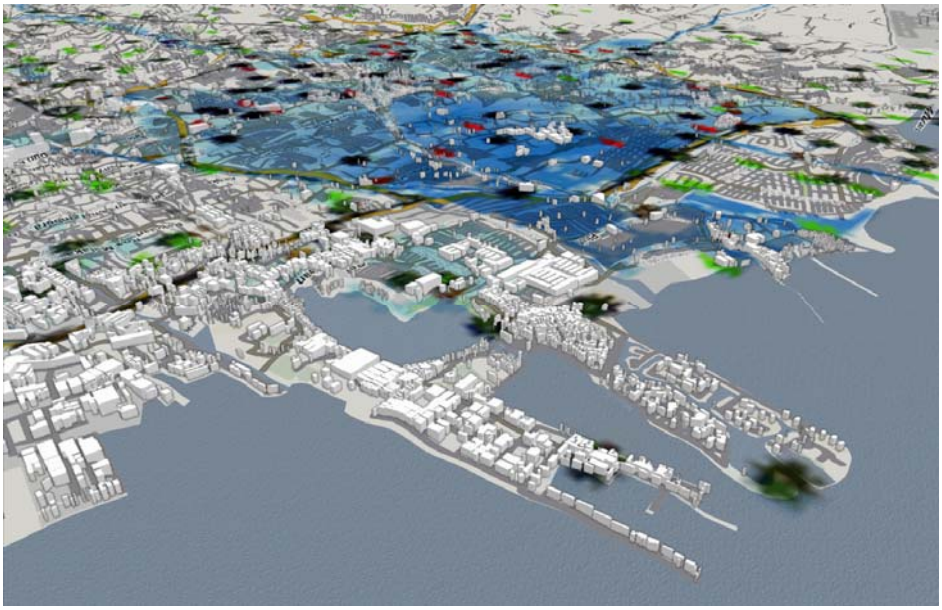


Figure 4: 3D, interactive environment for Jakarta

Furthermore, it should not be forgotten that decisions are often based on subjective arguments rather than objective ones, such as acceptability of risk in different sectors.

Both teams are now cooperating to realise a research project within ROBAMCI that benefits both research lines.

This page is intentionally left blank.

Teaching Homeland Security

Teaching Homeland Security is a hard challenge and a great opportunity to develop innovative curricula. The comparison between two training courses, in Italy and USA, shows a variegated scenario reflecting different HLS approaches.

Although a universal consensus does not exist for the definition of both domestic and international Homeland Security (HLS), it is still feasible to reach an agreement on its key features; one of the most established definitions, for instance, is that provided by the National Research Council (U.S.A.): "Any area of inquiry whose improved understanding could make U.S. (and International) people safer from extreme, unanticipated threats" [1].

According to the Quadrennial Homeland Security Review Report of the DHS, Homeland Security can be defined as: "intersection of evolving threats and hazards with traditional governmental and civic responsibilities for civil defence, emergency response, law enforcement, customs, border patrol, and immigration" [7].

The key word in this particular definition is evolving. Hence the scope of HLS has graduated from National Security to Emergency Personnel to Critical Infrastructure Protection, to Private Security (both cyber and physical aspects) and subsequently setting a tone of blind acceptance for nearly all threats to be categorised under the wide umbrella of HLS. Another element that emerges from the above definitions is that the cornerstone is the safety of people (and goods) in spite of the source of the threats. In other words, actual HLS is adopting, especially after hurricane Katrina, an All Hazards approach.

The lack of a universally adopted definition of HLS is reflected by the operative choices of the different National and International governments and Institutions.

For example, although the United States continues to focus on a wholesale approach to domestic security and border protection issues, European countries have largely preferred to work within their existing institutional architectures to combat terrorism and respond to other security challenges and disasters, both natural and man-made [3].

Such a diversity has indubitably a deep echo in the way Homeland Security is taught across different countries and institutions; at least in terms of intended audience, contents, occupation of trainees, etc.

To date, quite a bit of research has been conducted on how to teach Homeland Security. In [6] the need for the coexistence of HLS and Emergency Management (EM) in the same program is stressed. In [16] a comparison of the US and EU approaches to homeland security teaching is carried out, pointing out that, while US has continued to focus on centralising and unifying HLS efforts, EU governments tend to maintain the existing institutional settings, and (unlike the US) do not have a dedicated Department of HLS in many European countries; thus, the responsibilities are often delegated to several ministries, law enforcement and intelligence agencies.

In Europe, a myriad of threats have led to the dilution of a singular definition (of particular note is the prioritisation of elements compared to the U.S.). For example, while 'terrorism' is a top priority for the United States, the European Union might be more focused on immigration and Critical Infrastructure Protection (CIP); these differing approaches obviously impact a HLS curriculum.

This work aims at assigning a core curriculum for a HLS program, following three main strategies: comparative analysis, prioritisation of threats and an understanding of the ethical playground one is attempting to navigate.

Further, we compare the experience acquired in managing HLS training program by the University Campus Bio-Medico of Rome, Italy (UCBM, www.MasterHomelandSecurity.eu) and the Naval Postgraduate School, USA (NPS, www.nps.edu/). These institutions have, through independent strategic approaches, constructed working HLS graduate programs. Ultimately, we aim to provide a loose framework (predicated upon the "lessons learned" from our two case studies) for building a strong HLS program.

Roberto Setola

Roberto Setola is professor at University Bio-Medico, Rome and head COSERITY Lab (Complex Systems & Security Lab) and director of the Post Graduate program in Homeland Security.
Email: r.setola@unicampus.it

Maria Carla De Maggio

She belongs to the Complex Systems and Security Laboratory of the University Campus Bio-Medico of Rome since 2009. She holds a Master Degree in Biomedical Engineering (2007) and a PGP in Homeland Security (2011).
Email: m.demaggio@unicampus.it

Teaching Homeland Security: the recipe for success

Teaching Homeland Security is, simultaneously, a hard challenge and a great opportunity to develop innovative curricula capable of quickly responding to the needs of a specific country [8]. In fact, unlike other disciplines (e.g. Medicine, Accounting), no standard baseline for academia exists for the Homeland Security arena; subsequently, "Homeland Security Experts" graduate into the field with no oversight or guarantee that the appropriate knowledge base was explored.

No matter how one interprets the skills of a Homeland Security graduate, one variable is certain: there is no recipe to follow, and thus no accurate prediction in the outcome of a HLS graduate. Indeed, the academic context of homeland security could be stretched to include almost every discipline and topic area imaginable (e.g. public health, military history, international diplomacy, the psychological-sociological examinations of other cultures, comparative government systems, etc.), with "homeland security" serving more as a target for the application of such studies, rather than as a descriptor of the studies themselves [1].

Consequently, constructing a boundary-spanning interdisciplinary educational strategy remains a utopia, and has arguably become the victim of benign neglect [2].

While no two programs are identical, every HLS program contains particular "planks" which ensure that the most vulnerable "gaps" are covered; at least in theory. When starting to analyse particular HLS building blocks, one quickly deduces that the area of focus is not molded by the needs of the international community per se; rather, it is shaped through personal opinion and local or domestic trends. This desire to stay within the "box" of HLS, albeit a large and ever-expanding box, can potentially limit the student's exposure to areas of interest. According to the Federal Emergency Management Association (FEMA), there are currently 25 Universities offering Graduate level Homeland Security programs within the United States (2013) [10]. However, it is important to keep in mind that this number is skewed by the language; there are many other programs operating in the United States that could be categorised under the HLS umbrella but do not contain the specific label "Homeland Security" in their respective course. Further, when one applies the "Homeland Security Graduate Degree" search parameters into the NPS Center for Defense and Security website, the results yield seventy-nine Universities currently offering Homeland Security Graduate programs (2013) [11]. This is a classic example of why it has become so difficult to understand the exact role of homeland security experts. The inability to obtain a consensus (even within the confines of DHS- of which both FEMA and the NPS are members) has propelled many within the community to incessantly expand their HLS definition; hence, the Homeland Security "bubble" becomes ever more inflated and complex.

"Neither the U.S. Department of Homeland Security, the Federal Emergency Management Agency (DHS and FEMA), nor the several professional associations have agreed upon and articulated a common benchmark standard for collegiate education in these related fields" [3]. In addition to the differing external (between universities and agencies) Homeland Security program paradigms, many of the classes internally (within a university or institution) continue to be controversial. So, even within their respective institutions, it remains a point of contention amongst instructors on which classes to expose their students to in order gain an appropriate scope of relevant topics. The discontent between colleagues is also fuelled by physical location: even though globalisation continues to interconnect every facet of our lives, physical locality can still steer the curriculum.

And this physical location is not limited to mere approaches; along with a certain environment comes a specific type of lexicon.

ELEMENTS OF A HLS PROGRAM – USA	***ELEMENTS OF A HLS PROGRAM – ITALY***
Protection of critical infrastructure	Protection of critical information
Cyber security (crime and political attacks)	Cyber security
Border security and global threats	Risk analysis
Intelligence and strategic analysis	Strategy and intelligence
Disaster management and all hazard approach	Security legislation and standards
Mass transportation safety and security (ground, air, and maritime transportation)	Crisis management and disaster recovery
Interagency cooperation (including information sharing and safeguarding)	Security management
Political violence and terrorism	System engineering
Technology applied to security	Technology applied to security
Ethical dilemmas and civil rights	Ethics and privacy

All of these contrasted approaches inherently drive respective syllabi. However, it should be noted that the United States and Europe, of late, are applying a much wider purview in their HLS teachings (as deduced from the inclusion of globalisation and diplomacy courses). Several areas are generally addressed in an upper-level Homeland Security program for the United States. Such areas are summarised in the Table.

Comparative analysis

The NPS Master of Arts in Homeland Security program and the UCBM post-graduated level Homeland Security program were chosen for comparative analysis because they present differing styles in their respective teaching approach to HLS. The biggest difference is their intended audience.

The NPS program is geared towards personnel already vested in U.S. government service; this prerequisite for government experience provides a unique classroom atmosphere and is critical to highlight because, as with any upper-level education, the professor serves more as a facilitator than a direct educationalist. Subsequently, it behoves the program to have an experienced cadre of students who, in addition to analysing the static curriculum, provide personal experience and

opinions. During the last three cohorts of the NPS HLS program, ninety students have graduated with an average age of 45 and a career level of mid to senior; thus, they encompassed the capability to implement change within their respective agencies [9].

According to the Director of Academic Programs at the NPS Center for Homeland Defense and Security: "The students are oriented more to practice than to theory, to applied knowledge rather than analysis…Our approach is to assume the students are participants in the course rather than an audience for what we have to deliver" [5]. However, limiting the applicant pool can inadvertently impact a program.

Uninfluenced by their respective government agency, a "fresh" and open-minded student may prove just as valuable as their professionally developed counterpart. In this respect, the University Campus Bio-Medico has the ability to produce students that are directly shaped through their studies, not their potential biases commonplace amongst differing government agencies. The subsequent graphs (Figures 1 & 2) illustrate the relative experience of the UCBM student cadre for the past three sessions editions.

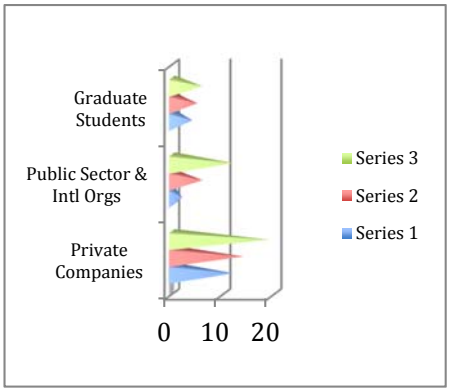


Figure 1 UCBM breakdown of student history for the past three editions.

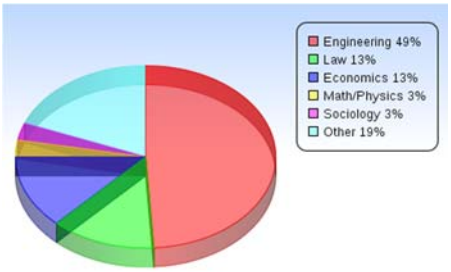


Figure 2 More background information regarding UCBM students for the past three editions.

Notice the high level of private company participants; although these companies irrefutably impact the HS community, there interests are most likely specified. Subsequently, the lessons learned in the program may not be applied on a global level. Although this is speculative, it is worth noting due to the known global impact of the NPS graduates. However, it is also worth mentioning that the lack of a target audience affords the student an ability to focus on their respective area of expertise. Additionally, the majority of participants in the UCBM HS program are 38-45 years old (see Figure 3); this statistic is extremely relevant because it highlights the fact that most participants in upper level programs are already entrenched within their career, thus we can assume that their respective opinions have already been influenced and subsequently formed.

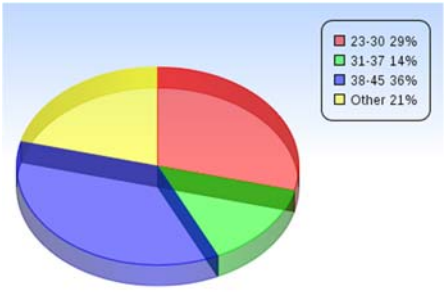


Figure 3 Age level of UCBM students for the past three editions.

Along with age, experience and background, the amount of time invested into each program is a critical element to examine. The NPS program is 18 months in duration while the UCBM is 12 months long (thus, the overall number of in-class hours invested by each student annually is more for those participating in the UCBM program). In this framework the NPS program incorporates also web-based coursework is a fundamental difference. While the online forum provides an extra level of interaction with the students, it is arguably an insufficient substitute for in-class instruction.

Yet another differing element is the inclusion of a thesis or capstone project. NPS requires a standard thesis project, while UCBM requires their students to complete an internship (minimum 2 months) within one of their sponsoring companies or a pre-approved public agency.

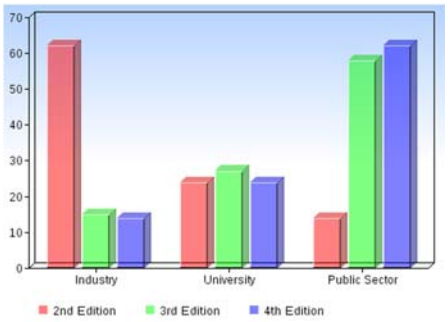


Figure 4 Background of the faculty for the past three editions for UCBM.

Because the NPS students are already entrenched within their government careers, students are required to construct a thesis within the confines of their relative agency. Thus, they develop their HLS skills within the very domain they impact; this practical approach behoves the U.S. government as much as the student. However, this also limits the student's ability to address issues outside of their immediate realm.

The graph of Figure 4 illustrates the teacher origins for UCBM; in the last 3 editions there was an evident inversion of tendency from a situation where the majority of teachers were from the Industry sector, to a situation where most of the instructors stemmed from the Public sector (including international organisations). The UCBM cadre of professors provides the students with a unique blend of Industry, Academia and Homeland Security experts.

Like the UCBM approach, the NPS program also incorporates a multidisciplinary cadre of professors whose wide ranging background provide the students with differing perspectives and subsequent teaching techniques.

In regards to outside the classroom experiences, both universities understand the value of gathering data first-hand and offer opportunities as such. For example, the UCBM program encompasses several field trips to some of the most relevant military, public and private homeland security agencies. These included: the Italian flight agency control room, the Italian civil protection control room, the virtual shooting polygon at Selex Elsag Spa, a power plant control room in Civitavecchia (near Rome) and the crisis unit of the Italian foreign office (U.S. State Department equivalent). When queried about field trips at NPS, Heather Issvoran (the Director of Strategic Communications at NPS) stated "as opportunities arise, we take advantage of them" [9].

Lessons Learned

How does one prioritise threats? Is it truly rational to place emphasis on one disaster over another? Should we focus more on the domestic or international front? Should an HLS program be tailored to counter a specific threat (i.e. cyber-security, industrial, private, transportation, emergency planning, natural disasters, etc.) or should it be a more all-encompassing approach? All of these questions present realistic challenges in molding an appropriate curriculum. And, once again, we believe that oversight is the answer. The real challenge lies in balancing probability, vulnerability and, most importantly, consequence. A curriculum focused on these elements, with the heaviest emphasis on consequence, is a sound recipe for success. This is based upon the mind-set of "when, not if". Operating under this umbrella of brutal realism, we can better prepare ourselves. Consider this: if the majority of resources are pumped into probability and vulnerability protection, then we can assume that the smallest amount of resources are allocated towards consequences. Further, is it possible to plan for EVERY threat? Ultimately, a new threat of a different variation will appear: this is fact. Therefore, it behooves the security mindset to accept a realistic outlook and form curriculum accordingly (i.e. providing a consequence-heavy focused syllabus).

Beyond student surveys, oversight of a program is necessary. With the Homeland Security field being such a fluid concept, wouldn't it make sense to overhaul program curriculum on an annual basis? For example, the Department of Defense promoted yhe presence of a Board of Visitors (BoV), comprised of Congressional members and civilians, into their program which role is to visit, examine and, ultimately, provide their findings to the Secretary of Defense and Congress. Although the power of the BoV is limited to an advisory capacity, the input provided has proven to be a valuable tool for the school. "In practicality, it has had impact on curriculum in two ways: 1) The Congressional members see specific needs or changes that can be made by legislation, and get those done and, 2) the knowledge and expertise of the civilians who have served (many lawyers, professors, former ambassadors) allow them to make practical suggestions that can be implemented right here" [4].

Understanding the ethical playground is another element which must be considered. As former U.S. Attorney General John Ashcroft wisely commented following September 11, 2001: "We always have to be careful that the rights which America stands for are protected, but we also have to understand that in order for those rights to be enjoyed, they have to be protected" [13].

At what point are civil liberties willingly sacrificed under the authority of 'homeland security'? In this regard, it is critical that a HLS program incorporate ethics and law into their respective syllabi. Nowhere is the moral playground murkier than in the field of technology. Simultaneously, the HLS field has been tasked with extending their technological capabilities and developing guidelines for their use. For example, "if precision weaponry is assumed to be inherently ethical, it may grant policymakers and strategists the chance to conflate the description of tactics with the prescription of normative judgments" [12]. Constrained only by the human element, technology itself neither answers nor ignores ethical questions; it is only the particular use of these technologies by practitioners that will either distract us from, or make us well attuned to, particular ethical questions concerning the rights and safety of citizenry [12].

Acknowledgement

Authors would to thank Gregory Fink for his support and to provide valuable information about US and NPS initiatives.

References

[1] Frameworks for Higher Education in Homeland Security Committee on Educational Paradigms for Homeland Security, National Research Council ISBN: 0-309-54511-0, 78 pages, 6x9, (2005)

[2] Journal of Homeland Security and Emergency Management; Volume 6, Issue 1 2009; Article 34, Educational Challenges in Homeland Security and Emergency Management. Robert McCreight; George Washington University, Copyright 2009, The Berkeley Electronic Press

[3] European Approaches to Homeland Security and Counterterrorism. Congressional Research Service: Report For Congress; July 24, 2006, Kristin Archick, Coordinator; Carl Ek, Paul Gallis, Francis T. Miko, and Steven Woehrel Foreign Affairs, Defense, and Trade Division

[4] Rials, Lee A. (lee.a.rials.civ@mail.mil). (2012, April 16). Interview results. Email to authors.

[5] Bellavita, Christopher; Gordon, Ellen M. "Homeland Security Affairs"; Volume II, Issue I, Article I (2006); Changing Homeland Security: Teaching the Core.

[6] Kiltz, L. The benefits and challenges of integrating emergency management and homeland security into a new program. Journal of Homeland Security Education, 1(2), 6-28. (2012). Retrieved from www.journalhse.org/vli2-kiltz.html

[7] U.S. Department of Homeland Security. (February, 2010). Quadrennial homeland security review: A strategic framework for a secure homeland. Retrieved from http://www.dhs.gov

[8] Pelfrey, W., Sr. & Pelfry, W., Jr. (2009). Curriculum evaluation and revision in a nascent field: The utility of the retrospective pretest-posttest model in a homeland security program of study. Evaluation Review, 33(1), 54-82.

[9] Issvoran, Heather. (hissvora@nps.edu) (2013, February 6). Interview results. Email to authors.

[10] FEMA homepage, retrieved from www.fema.gov

[11] NPS Center for Defense and Security website; retrieved from www.chds.us

[12] Another Question Concerning Technology: The Ethical Implications of Homeland Defence and Security Technologies John Jacob Kaag

[13] Cited in CSIS Briefing, "Strengthening Law Enforcement Capabilities to Combat Terrorism", October 2003.

[14] M. C. De Maggio, M. Mastrapasqua and R. Setola, "The professional figure of the Security Liaison Officer in the Council Directive 2008/114/EC", 10th International Conference on Critical Information Infrastructures Security (CRITIS 2015), Berlin, 2015

Links

ECN home page	www.ciprnet.eu
ECN registration page	www.ciip-newsletter.org: Please register free of charge
CIPedia©	www.cipedia.eu the new CIP reference point

Forthcoming conferences and workshops

TIEMS 2015 Annual Conference	http://tiems.info/tiems-2015-annual-conference.html	Sept. 30 - Oct. 2, 2015, Rome.
10th CRITIS Conference	www.critis2015.org	Call for Participation, Oct 5-7, 2015, Berlin
Cyber Storm	www.swisscyberstorm.com	Oct. 21, 2015
49th ESReDA Seminar	www.esreda.org	Clos Chapelle-aux-Champs, Belgium 29/30 Oct. 2015
CIPRNet Master Class	www.ciprnet.eu/endusertraining.html	Rome, 11th – 13th November 2015
16th IEE El.Tech Conference	http://melecon2016.org	Call for Participation
ACM CPSS'16	http://icsd.i2r.a-star.edu.sg/cpss16	Call for Paper, Xi'an, China – May 30, 2016
New book	http://staff.www.ltu.se/~ismawa/ansasa	Call for Paper
6th IDRC Davos 2016	www.grforum.org	August 28 - Sept. 01, 2016

Institutions

National and European Information Sharing & Alerting System	www.neisas.eu

Project home pages

FP7 CIPRNet	www.ciprnet.eu
H2020 IMPROVER	www.improverproject.eu
H2020 RESIN	www.resin-cities.eu
JRC GRRASP	https://ec.europa.eu/jrc/en/grrasp
Ernest & Young	http://www.ey.com/GL/en/Services/Advisory/EY-global-information-security-survey-2014

and Deltares Brochure:
https://www.deltares.nl/en/projects/climate-change-risk-assessments-and-adaptation-for-roads-the-roadapt-project/

Interesting Downloads

European Network and Information Security Agency www.ENISA.eu publishes reports and other material on "Resilience of Networks and Services and Critical Information Infrastructure Protection" I this issue e.g.:

ENISA	www.enisa.europa.eu/activities/Resilience-and-CIIP
ICS Certification ENISA	https://resilience.enisa.europa.eu/ics-security
Network Information Security Platform	https://resilience.enisa.europa.eu/nis-platform

Websites of Contributors

Acris	www.acris.ch
Center for Cyber & Information Security NO	https://ccis.no
Cyfor	https://www.dfs.no/Skytterlagssider/opplandskretsen/gudbrandsdal/cyberforsvaretcistg
Deltares	www.deltares.nl/en
EC Joint Research Centre	https://ec.europa.eu/jrc
EY	www.ey.com/CH/de/Home
Fire and Security DK	www.dbi-net.dk/
H2020	http://ec.europa.eu/programmes/horizon2020
Linköping University	www.liu.se/?l=en
Network Security Lab NO	www.nislab.no
RISC SE	www.rics.se
SP research Sweden	www.sp.se/sv/Sidor/default.aspx
Campus Bio-Medico di Roma	www.unicampus.it

www.cipedia.eu

Let's grow CIPedia©

An online community service by the CIPRNet Project.

Derived from the EU FP7 Network of Excellence project **CIPRNet**, CIPedia© aims to be a **Wikipedia-like online community service** that will be a vital component of the CIPRNet's VCCC (Virtual Centre of Competence and expertise in CIP) web portal, to be hosted on the web server of the CIPRNet project.

It is a multinational, multidisciplinary and cross-sector web collaboration tool for information sharing on Critical Infrastructure (CI)-related matters. It promotes communication between CIP-related stakeholders, including policy-makers, competent authorities, CI operators and owners, manufacturers, CIP-related facilities and laboratories, and the public at large.

CIPedia© needs you in order to become a common reference of CIP concepts.

CIP terminology varies significantly due to contextual or sector differences, which combined with the lack of standardization, create an unclear landscape of concepts and terms. CIPedia© tries to serve as a point of **disambiguation** where various meanings and definitions are listed, together with additional information to relevant sources.

In its current stage of development, CIPedia© is a collection of pages – one page for each **concept** with key **definitions** from various sources. It is supplemented by: a list of CIP **conferences**, several sector-specific **glossaries**, CIP-related **bibliography**.

In future stages it will include discussion topics on each concept, links to useful information, important references, disambiguation notes, and more. The full articles will eventually grow into a form very different from dictionary entries and related concepts can be combined in one page. CIPedia© does not try to reach consensus about which term or which definition is optimum, but it records any differences in opinion or approach.

The CIPedia© service aims to establish itself as a **common reference point for CIP concepts and definitions**. It gathers information from various CIP-related sources and combines them in order to collect and present knowledge on the CIP knowledge domain.

Your contribution is essential for putting value in the CIPedia© effort.

Marianthi Theocharidou

Marianthi Theocharidou is a Research Fellow at the European Commission's DG Joint Research Centre (JRC), working for the CIPRNet, IMPROVER and ERNCIP projects.

marianthi.theocharidou@jrc.ec.europa.eu

Expression of Interest

CIPedia© now welcomes **CIP experts** to actively **contribute**:

- ✓ Add definitions and references!
- ✓ Create a new topic!
- ✓ Start a discussion!
- ✓ Moderate!

If you are interested to become an active contributor, please contact Dr. Theocharidou for information.