CIPRE 2016
2-3 March 2016
Netherlands

critical infrastructure PROTECTION AND RESILIENCE EUROPE 2-3 MAR 2016 The Hague Netherlands

Tuesday 1 March

2.30pm - 5.00pm **CIPRE Roundtable Workshop hosted by IET**

Wednesday 2 March

9am

Opening Keynote

Chair: John Donlon

Ard van der Steur, Minister of Security & Justice, The Netherlands

Olivier Luyckx, Head of Unit HOME.D.1 (Terrorism and Crisis Management), DG HOME, European Commission

Liviu Muresan, Executive President of EURISC Foundation - European Institute for Risk, Security and Communication Management, Romania

Deputy Mayor Ingrid van Engelshoven, Municipality of The Hague, The Netherlands

10.30am Networking coffee break

11.00am

Plenary Session

Collaborative Approach to CIP and CIIP

As the lines and responsibilities between CIP and CIIP become increasingly blurred in many areas, a holistic approach to protection of CNI, from both physical and cyber security perspectives is increasingly important. To this nature the collaboration between agencies and CNI operators, and individual departments, becomes increasingly important. How can we work better together for common purpose, resource sharing and intelligence gathering to deliver better value for the tax payer and greater success in delivering security & resilience to our Critical National Infrastructure, and improving disaster risk reduction.

Chair: John Donlon

Evangelos Ouzounis, Head of Unit - Secure Infrastructure and Services, European Union Agency for Network and Information Security - ENISA

Critical Infrastructure Protection Interdependency Analysis and the impact from Cyber - Fred Ruonavar, Chief of the Contingency Operations and DoD Information Network (DoDIN) Critical Infrastructure Protection (CIP) Branch, Operations Directorate, Defense Information Systems Agency (DISA), USA

Andrew Wright, Head of Industrial Resources and Communications Services Group , NATO

Netherlands national testbed for protecting critical infrastructures - HSD and TNO

IET Round Table Review - IET

12.30pm Networking lunch

2pm

CIP Break out 1

Emerging & Future Threats Detection & Management

The ever changing nature of threats, whether natural, through climate change, or man-made through terrorism activities, means the need to continually review and update policies, practices and technologies to meet these growing demands. But what are those emerging threats and how can we detect, prevent, monitor and manage their levels of potential damage?

Chair: Roger Gomm, ICPEM

Paul Minnebo, Senior Representative, EUROPOL

CIRAS (Critical Infrastructure Risk Assessment Support) Project - Jaime Martin Perez, Project Coordinator, ATOS

Critical Infrastructure: Emerging Threats, Their Identification and Management - Ian Betts, Global Head, Risk Analysis, G4S Risk Consulting Ltd

CIIP breakout 1

Cyber Security Standards and Law

With the increasing cyber threats and changing nature of attacks, standards in cyber security and law have to develop to keep pace and operators of critical infrastructure are under increasing pressure to meet progressive challenges. With current variations of standards across the EU in reporting and handling of critical incidents, harmonising these standards would benefit the region. How can government and operators better collaborate and share information and contribute towards better standards fit for pan-European infrastructure?

Chair: Evangelos Ouzounis, Head of Unit - Secure Infrastructure and Services, European Union Agency for Network and Information Security - ENISA

Dutch Cyber Security Council (invited) - Martin Bobeldijk, communication advisor

Elena Ragazzi, Project Coordinator ESSENCE, Italy

Cyber(Security)HUB-E - Florian Haacke, CSO / Head of Group Security, RWE, Germany

3.15pm Networking coffee break

4pm

CIP Break out 2

Enhancing Preparedness and Response through Modelling and Simulation

Enabling government, operators and industry policy makers and managers to optimise security and disaster planning by identifying and predicting the opportunities for improvement. Ensuring organisations develop a more robust integrated risk-based defence posture, through modelling and simulation techniques could assist the industry in enhancing CNI protection and resilience.

Chair:

IMPROVER - David Lange, Project Coordinator IMPROVER, SP Fire Research, University of Sweden

CIIP breakout 2

Convergence in Cyber Security and CIIP

All parts of infrastructure are interconnected which, despite being convenient and efficient, can leave the complete system extremely vulnerable to attack. Convergence of cyber security, incidence response and crisis management can enhance the integrity of the infrastructure and help exceed minimum security requirements.

Chair: TBC

Improving security by converging cyber security incidence response and crisis management - Bharat Thakrar, Cyber Resilience & Advanced Threat Defence, BT Security Enterprise, BT GS, UK

	PREparing for the Domino effect In Crisis SiTuations on critical infrastructures (PREDICT) - Dr. Y.Barbarin the scientific coordinator, CEA, France	**Security for remote control and switching – not only in energy distribution systems** - Dietmar Gollnick, CEO, e*Message W.I.S. Deutschland GmbH, Germany
	FORTRESS - Robert Pelzer, Research Associate Technische, FORTRESS, Germany	**Open innovation strategies for IT security of critical infrastructures** - Dr. Albrecht Fritzsche, Researcher, University Erlangen-Nürnberg & Joerg Dreger, Managing Partner, Dreger Group, Germany
	Protecting infrastructure & communities – the UK case study on developing world class resilience through a tested model - Sean Glynn, Chief Executive, Chief Fire Officers Association National Resilience Ltd (CNR Ltd), UK & William Drysdale, Head of Strategy and Business Development, Babcock International Group	**PRE-EMPTIVE** - Giorgio Sinibaldi,B U Government & Industries System Engineering & Business Development, Vitrociset, Italy
5.30pm	Networking Reception	

Thursday 3 March

9am	CIP Breakout 3 **The PPP Role in CIP** *With many critical infrastructures in the hands of private organisations, how does the responsibility of security and resilience lie between government, with public accountability to keep them safe, secure and operational 24/7, and the private operator, with additional responsibilities towards shareholders? How can improving the communication between the public sector and private sector enhance protection and can incentives be employed to better engage private owners into PPP?* Chair: John Donlon Paul Gelton, Director of Resilience, Ministry of Security & Justice, The Netherlands **The PPP in Lombardy Region** - Cinzia Secchi, Manager of Integrated Prevention System Unit, Lombardy Region – G.D. Safety, Civil Protection and Immigration, Italy **Protecting CI: Challenges for PPP in time of new types of security threats** - Ms. Lina Kolesnikova, Fellow, Institute of Civil Protection and Emergency Management (ICPEM)	CIIP breakout 3 **Protecting the 'Smart CII'** *In the age of smart cars, smart airport, smart hospitals, smart grids, for enhancing economic development, social mobility and efficiencies, actually how smart are we or are we sleep walking into a future catastrophe? The interconnected 'smart' society leaves critical information, data and systems exposed and vulnerable to cyber attack that could create chaos or potential disasters and threat to human life. How do we best plan and secure our smart systems and how do the different stakeholders ensure the integrity of the systems?* Chair: Anjos Nijk, Managing Director, European Network for Cyber Security (ENCS), Netherlands **The Connected Car** - Bharat Thakrar, Cyber Resilience & Advanced Threat Defence, BT Security Enterprise, BT GS **Hacking Critical Infrastructure becomes easier and easier every day. Is there a defense to the attack?** - Elaine Mullen, PT Security - abstract
10.30am	Networking coffee break	
11.15am	CIP Breakout 4 **Technologies to Detect & Protect** *Technologies greatly assist in surveillance, detection and protection of CNI and are becoming increasingly important in their application due to heightened threats. What are some of the latest innovations and future technologies, from ground surveillance to space based technology, to predict or detect potential threats to CNI, whether natural or terrorist related.* Chair: Tony Kingham, Editor, World Security Report DRiving InnoVation in crisis management for European Resilience (DRIVER Project) - Jaime Martin Perez, Project Manager, Homeland Security and Defence Sector, Research & Innovation, ATOS **Towards categorizing the level of protection that GNSS Receivers provide in adverse environments** - Guy Buesnel, Spirent Communications	CIIP breakout 4 **Cyber Analysis, Monitoring and Defence** *The ability to monitor the cyber threats to CNI can greatly assist the operators and agencies better prepare their defences against cyber attacks on systems and information/data. What is the latest strategic perspective on cyber monitoring and cyber defences for enhancing CIIP?* Chair: Critical Infrastructures and Cloud Computing (CI2C) - Maria Cristina Brugnoli, ICT4People Research Unit, University of Rome, Italy **Cyber monitoring and response management in critical infrastructures** - Douglas Wiemer, Rhea Group **Emerging Best Practice for ICS Perimeter Cyber Security** - Dimitry Shvartsman, Director of Industrial Security, Waterfall Security Solutions, Israel Ministry of Security, The Netherlands (tbc)
12.30pm	Networking lunch	
2pm	Plenary Session and Round Up **Critical Infrastructure Security and Resilience : Approaches and Case Studies from Transport, Energy & Telecomms Sectors** *Transport, power and telecommunications continue to be the crucial economic lifeblood of any modern industrial economy, which have all been tested in the past year with threats from cyber attacks, terrorism and man-made threats, as well as the changing weather patterns delivering more unpredictable systems and risk of flooding. Communications infrastructure becomes key during any threat scenario to which many fail when severely damaged, limiting coordinated efforts and potentially causing damage to the economy far in excess of any physical damage they may incur. The problem for the authorities, operators and agencies is to ensure the right balance of security, safety and resilience in facilities that are widely dispersed and subject to diverse ranges of threats.* Chair: Ms. Lina Kolesnikova, Fellow, Institute of Civil Protection and Emergency Management (ICPEM) **All-Hazard Guide for Transport Infrastructure** - Selcuk Nisancioglu, Senior Researcher, Federal Highways Research Institute, Germany **EUSTO (European Surface Transport Operators Forum)** - Ilias GKotsis, Associate Researcher, Center for Security Studies- KEMEA **Securing and Providing Resilient National Critical Communication Services in case of national disasters or major threat incidents** - Norbert Elferink, Senior Business Consultant Manager, Group 2000 **Monitoring and Assessing Risks in a Complex Global Environment** - Tobias Larsson, Director and Head of DHL Resilience360, Deutsche Post DHL Group	
4pm	Conference close by John Donlon	