

A CEPS TASK FORCE ON

“CRITICAL INFRASTRUCTURE PROTECTION IN THE EU”

Chair: **Prof. Dr. Bernard Haemmerli**, Vice-President ISSS
Information Security Society Switzerland

Rapporteur: **Andrea Renda**, Senior Research Fellow, CEPS

PROSPECTUS

Over the past few years, the attention of policymakers and industry players towards the protection of critical infrastructure has grown remarkably. In the era of networks, citizens and businesses have become increasingly dependent on a large set of infrastructures encompassing energy networks, the banking sector, telecommunications, the Internet etc. In the US, a national programme to protect critical infrastructure was launched in 1998, under the Clinton administration, and was confirmed and updated under the Bush administration in 2003. At EU level, the European Council of June 2004 called on the European Commission to prepare an overall strategy to protect critical infrastructure (CI). The Commission adopted on 20 October 2004 a Communication on Critical Infrastructure Protection (CIP) in the Fight against Terrorism which put forward suggestions on what would enhance European prevention, preparedness and response to terrorist attacks involving Critical Infrastructures.

The CI debate continued with the Council conclusions on “Prevention, Preparedness and Response to Terrorist Attacks” and the “EU Solidarity Programme on the Consequences of Terrorist Threats and Attacks” in December 2004, which endorsed the intention of the Commission to propose a European Programme for Critical Infrastructure Protection (EPCIP) and agreed to the setting up by the Commission of a Critical Infrastructure Warning Information Network (CIWIN). After a Green Paper adopted in November 2005 and the December 2005 Justice and Home Affairs (JHA) Council Conclusions on Critical Infrastructure Protection, the Commission finally adopted a Communication, which designated European critical infrastructure as those ones that, in case of fault, incident or

attack, could impact both the country where it is hosted and at least one other European Member State.

In 2005, the Commission defined critical infrastructure as “those physical resources, services, information technology facilities, networks and infrastructure assets, which, if disrupted or destroyed would have a serious impact on the health, safety, security, economic or social well-being” of citizens and member states. This definition was kept deliberately broad to enable a horizontal, multi-sectoral policy approach. Critical infrastructure is further separated into two categories: (i) a general critical infrastructure (CI) which is comprised of the actual physical resources and services that have a serious impact of the functioning of society – such as energy grids and financial services; and (ii) critical information infrastructure (CII), which is defined as including all of the ICT systems that are “critical infrastructures [in] themselves or that are essential for the operation of critical infrastructures (telecommunications, computers/software, Internet, satellites, etc.)”.

It is increasingly accepted that both CI and CII face potential threats; an attack on either would result in significant economic costs. For example, The World Economic Forum estimated in 2008 that there is a 10 to 20% probability of a major CII breakdown in the next 10 years, with a potential global economic cost of approximately \$250 billion. Similarly, The US Business Roundtable in 2007 suggested that the economic costs of a month-long internet disruption to the United States alone could be more than \$200 billion, while the OECD estimates the annual losses to United States businesses caused by malware to be \$67.2 billion.

The figures above suggest a number of considerations.

- First, the risk of a significant disruption in critical infrastructure is serious enough that it warrants attention from both the public and private sector.
- Second, the high dependence of critical infrastructures in the EU and United States mean that any disruptions would result in large economic costs.
- Third, as the EU and United States are affected by similar issues there is a need to discuss CIP from a transatlantic perspective.

As the European society becomes more interconnected and advanced, its dependence on critical infrastructure is inevitably heightened. Despite its increasing importance, many European businesses and citizens still seem to underestimate the risks to which critical infrastructures are exposed. In addition to this, many businesses feel they cannot justify the private return on investment associated with increasing security. Accordingly, there is often an underprocurement of protection of critical infrastructures by businesses in the EU.

In response to this challenge, both officials and the private sector have made calls to establish a public-private partnership (PPP) with a twofold ambition: (i) to find the appropriate level of public support for protecting critical infrastructures supplied by private firms, by ensuring that any public support offered will improve security without causing externalities such as market distortions, or unfair

competitive advantages for certain firms or industries; and (ii) to facilitate information exchange between governments and firms, as well as among firms, on best practices for protecting critical infrastructures.

The future PPP on critical infrastructure protection is meant to establish a dialogue that is as informative as possible, while recognizing the need for firms to protect their intellectual property. The structure and functioning of this PPP are however still to be defined with precision: what will be the role of the public and private sector in securing enhanced resilience and network security in the years to come? How will private players be rewarded, and with what consequences for IP protection and competition? Despite heavy work being undertaken in EU institutions such as the European Commission and ENISA and growing collaboration with key players in a number of fields, many of these questions still await a precise answer.

Against this background, considering the challenges faced by firms and government in protecting critical infrastructures, and the need to establish a functional and effective PPP, CEPS proposes to launch a new “Task Force on Critical Infrastructure Protection”. The purpose of this Task Force will be to discuss the challenges and opportunities that will arise from a future PPP, as well as how a PPP could operate at the European level between firms and government, and whether the current institutional setting at the EU level is appropriate. In addition to discussing CIP in the EU, the task force will offer a venue to examine CIP from a transatlantic perspective to explore potential synergies and avenues for collaboration, also within the Transatlantic Economic Council (TEC).

The ultimate goal of this CEPS Task Force is to provide policymakers and field practitioners with an updated and independent view of current developments on CIP (with an emphasis on CIIP) and PPP, while at the same time representing in an objective way the needs and problems identified by industry players and authoritative scholars in the field. In addition, our CEPS Task Force on critical infrastructure protection will seek to provide a unique forum for cooperation between public and private players, as testified by the success of our first seminar in this field, held in May 2009, which saw the participation of representatives from the European Commission, ENISA and several industry players.

Below, we briefly introduce each of the topics that will be addressed in the Task Force meetings, as well as a proposed time schedule for completion of the Task Force.

DESCRIPTION OF PROPOSED TOPICS

We propose to structure the discussion in the form of an impact assessment of a future policy initiative. Accordingly, our proposed list of topics broadly follows the structure of Commission's impact assessments. We start from the identification of the problem and the corresponding need to act (and act at EU level), and then explore a number of potential policy alternatives, in order to identify the pros and cons of each policy option. We also explore options to set up a suitable governance system for enhanced CIP and CIIP, and the potential for transatlantic cooperation on CIP-related issues.

Note: topics for Discussion may be adapted based on the ideas and concerns of Task Force members.

- ***Problem definition***

- *Defining critical infrastructure: a long-term perspective.*
- *What does the evidence tell us? The risk of disruption in CI and CII today and in the future.*
- *Assessing potential benefits from enhanced protection of CI and CII.*
- *Existing programmes to foster network resilience and security in the EU: national programmes and the EU action plan.*
- *What is missing? An agenda on CIP and CIIP for the years to come.*

- ***Defining policy options***

- *The need to act*
- *The need to act at EU level*
- *Acting through enhanced information*
- *Acting through enhanced cooperation between institutions (EU and member states)*
- *Strengthening EU institutions (e.g. the role and powers of ENISA and other sectoral regulators)*
- *Involving the private sector: the PPP*
- *A single policy for all CIs? Peculiar needs of individual sectors (energy and utilities, transport, water, telecoms, ICT, health care, safety, chemicals, government, manufacturing, etc.).*
- *The need for a "holistic", cross-sectoral approach.*

- ***Shaping a public-private partnership: opportunities and challenges.***
 - *The public side I: the role of the European Commission, the role of ENISA, the role of sectoral agencies.*
 - *The public side II: the role of national administrations and their interaction with the EU level.*
 - *The private side I: what role and responsibility should private players have?*
 - *The private side II: the role of standardization in a PPP and its impact on CIP and CIIP*
 - *The private side III: effects of a PPP on competition and IP protection.*

- ***CI and CII: a Transatlantic perspective***
 - *Initiatives and guidelines in the US*
 - *Areas for collaboration, synergies, interrelations*
 - *Integrating CIP and CIIP in the Transatlantic Economic Council.*

- ***Risk assessment and CIP and CIIP-related issues in EU policymaking***
 - *How to integrate risk assessment and CIP and CIIP in EU policymaking;*
 - *Methods and features of a EU (cyber)risk assessment model.*
 - *Monitoring and evaluation: choosing governance structures and performance indicators.*

SUMMARY OF PROPOSED TOPICS

Meeting 1 (launch meeting)

- Introduction of the issues, goals, output in the Task Force
- Defining CIP, CIIP and proposed PPP
- Who are the actors?

Meeting 2 - THE EU, INDUSTRY AND CIP

- What is the EU's jurisdiction regarding CIP and CIIP
- What is the current role of Industry in CIP and CIIP
- The role of ENISA

Meeting 3 – THE PUBLIC PRIVATE PARTNERSHIP

- How is it envisioned by Industry/Government
- Are there existing models for PPP and an opportunity for co-ompetition? (British example?)
- Examples in practice: Financial Services, ICT, Energy?

Meeting 4 – A TRANSATLANTIC PERSPECTIVE FOR CIP, CIIP AND PPP

- Looking at European approaches in a global context
- What is being done in the United States? How can cooperation be facilitated?

Meeting 5 – REFLECTION AND WRAP-UP

- Examination and comments on the Preliminary Task Force Report
- Finalization of the Task Force Report

THE CEPS TASK FORCE: ORGANISATION AND GOVERNANCE

In organizational terms, we propose to structure the debate over 5 meetings, including an initial launch meeting to introduce the issues. The organisation of a launch meeting has proven very important in previous CEPS Task Forces to fine-tune the topics to be addressed and bring them closer to the interests of industry players and regulators.

We propose to host the launch meeting on November 3rd. On that occasion, representatives from industry, academia and government will be invited to comment on the proposed Task Force agenda and indicate topics that may be added/dismissed. Following the launch meeting, we plan to host four additional meetings in 2009 and 2010, completing the Final Report by summer 2010.

As stated, the Chair of the Task Force will be Bernard Haemmerli, Vice-President ISSS Information Security Society Switzerland. The Rapporteur will be Andrea Renda, Senior Fellow, CEPS.

WHY A CEPS TASK FORCE AND HOW DOES IT WORK?

The CEPS Task Force will constitute a unique forum of representatives from the European Commission, Members of the European Parliament, officials from member states, business and industry, NGOs and other stakeholders to discuss highly topical issues in a multi-stakeholder setting. The objective of a task force is i) to create a process where issues can be analysed in an open but structured discussion and ii) to publish an authoritative analysis including policy recommendations. CEPS will produce an (operational) synthesis report for each meeting. At the end of the Task Force, CEPS will publish and circulate among EU and member state policy recommendations together with a background report, which will be also formally published in the CEPS Task Force Report publication Series. The Background Report will be based on discussion in the meetings supplemented by research carried out by the Rapporteurs.

CONDITIONS FOR PARTICIPATION

The CEPS Task Force is principally designed for CEPS Corporate Members but participation is open to non-members as well, at a higher fee.

The fee covers participation in all workshops, documentation, lunches and three copies of all reports produced. If participants wish, CEPS will mail additional copies of the final report to persons identified by participants.

Fee Structure

Participation fee for:

CEPS Corporate Members: EUR 1,000

Non-members: EUR 7,000

To register, please use the Registration Form in the Appendix of this document.

About CEPS

The Centre for European Policy Studies, based in Brussels, was launched as an independent research institute in 1983 to encourage the study and discussion of public affairs in Europe. It aims:

- to provide decision-makers, inside and outside government, with authoritative and independent analysis of European affairs;
- to contribute to the public debate about European institutions and policies through sound research and judgement; and,
- to create a network of leaders and thoughtful individuals who are committed to working together to enhance the development of European integration and co-operation.

CEPS is funded by corporations, public bodies, membership fees and income from activities.

If you have any questions regarding the Task Force, please contact:

Staffan Jerneck

Director & Director of Corporate Relations

Tel: (32.2) 229 39 10

GSM: (32) 475 903 924

Fax: (32.2) 22939 22

e-mail: Staffan.Jerneck@ceps.be



REGISTRATION FORM

CEPS Task Force **“CRITICAL INFRASTRUCTURE PROTECTION IN THE EU”**

First meeting at CEPS - 1, Place du Congrès - Brussels

Date: November 3rd 2009

A participation fee for the task force including all task force meetings of €1,000 applies for CEPS Corporate Members, while €7,000 applies for non-members.

Name	
First name	
Position	
Company	
Address	
Telephone	
Fax	
Email	

Please tick correct box:

<input type="checkbox"/>	My company is a corporate member of CEPS and pays €1,000 (+21% VAT).
<input type="checkbox"/>	My company is not a corporate member of CEPS and pays €7.000 (+21% VAT).
<input type="checkbox"/>	My company is interested in becoming a member of CEPS. Please send additional information.

Return to:

Staffan Jerneck,

Director and Director Corporate Relations, CEPS

Fax: +32 2 229 39 22

Email: staffan.jerneck@ceps.eu

(Tel: +32 2 229 39 10 –GSM +32 (0)475 903924)