



CONSORTIUM ON SECURITY AND TECHNOLOGY

*Building Public-Private Partnerships for more effective protection
of people, economies and infrastructure against international terrorism
and organized crime*

March 2006 | No.3

Cluster on

Critical Infrastructure Protection

Report of the meeting held on January 19th, 2006

The public and private sectors are coming together to improve the protection of citizens, economies and infrastructure against international terrorism and organized crime and also by focusing on the role that technology can play in this process. On January 19th, 2006, the EastWest Institute organized a public-private roundtable discussion on the topic of critical infrastructure protection in Europe. Public sector officials, owners and operators of critical infrastructure, and technology providers participated in the discussion which provided input into the development of a European Programme for Critical Infrastructure Protection (EPCIP).

Executive Summary

The EastWest Institute Consortium on Security and Technology organized a roundtable discussion on January 19th, 2006, on the topic of critical infrastructure protection in Europe. The objective of the roundtable discussion was to provide feedback on the European Commission's recently published *Green Paper on a European Programme for Critical Infrastructure Protection*¹. Over 30 public sector officials, owners and operators of critical infrastructure, and technology providers participated in the discussion. The discussion resulted in the following key conclusions:

- ❑ Because a voluntary approach to critical infrastructure protection might not result in increased security standards, there should be a legislative, common framework around the basic principles of EPCIP, without going beyond the principle of subsidiarity.
- ❑ EPCIP should guarantee the confidentiality of sensitive information. The best way to do this is to have the sharing of data on specific infrastructure be the responsibility of Member States.
- ❑ Another key principle should be proportionality. Protection strategies and measures should be proportionate to the level of risk involved. Protection measures should be defined on a sector by sector basis.
- ❑ Critical infrastructure operators should ensure an adequate level of security through the deployment of security plans. Member States should analyse the threat and threat levels and audit the deployment of security plans at the national level.
- ❑ The European Commission should provide an overview of the effectiveness of Member States' policies. The Commission should have a coordinating role whenever a disruption of critical infrastructure has transnational consequences.
- ❑ Cooperation between the EU and NATO on the issue of critical infrastructure protection should be improved.
- ❑ New measures and standards adopted at the EU level should not result in barriers hampering the possible use of effective non-European technology.

¹ [COM\(2005\) 576 final](#), 17 November 2005.

Background

Critical infrastructures consist of those physical and information technology facilities, networks, services and assets which, if disrupted or destroyed, would have a serious impact on the health, safety, security or economic well being of citizens or the effective functioning of governments. Critical infrastructures extend across many sectors of the economy, including banking and finance, transport and distribution, energy, utilities, health, food supply and communications, as well as key government services. Changes on the international scene have shifted attention to new security threats.

Critical infrastructure protection (CIP) has become particularly important in this context. Since the mid 1990s, the governments of many western countries have recognized the importance of critical infrastructure to their foreign and security policy. In 2004, given the nature of the threat and the fact that Europe's critical infrastructures are highly connected and highly interdependent the CIP debate was brought up on to the European level.

In June 2004, the European Council asked the Commission to prepare an overall strategy to enhance the protection of critical infrastructures. In response, the European Commission transmitted a Communication in October 2004 entitled *Critical Infrastructure Protection in the Fight against Terrorism*² which put forward suggestions to enhance European prevention, preparedness and response to terrorist attacks involving critical infrastructures. The Commission's intention to propose a European Programme for Critical Infrastructure Protection (EPCIP) and a Critical Infrastructure Warning Information Network (CIWIN) was accepted by the December 2004 European Council in its conclusions on prevention, preparedness and response to terrorist attacks and in the Solidarity Programme, both of which were adopted by the Council on December 2nd, 2004.

The Green Paper on EPCIP

Throughout 2005, intensive work was done on the elaboration of EPCIP. An inter-service group on critical infrastructure protection was created to discuss which areas should be focused on. Nominated contact persons from all the relevant Directorates General of the Commission participate herein to coordinate and prioritize. The Commission has contact points within the ministries of the EU Member States as well as Bulgaria, Norway, Romania and Switzerland, to

communicate on issues that concern the Member States and to bring the process further.

The complex nature of the topic and the importance of political and substantial engagement into a public-private dialogue with all concerned stakeholders including the Member State authorities, made the European Commission re-evaluate their original approach and instead issue a Green Paper. In so doing, the Commission wished to highlight difficulties and questions from a principle framework point of view. Two European seminars on critical infrastructure protection and a number of informal meetings were held bringing together experts from all the EU Member States. This work culminated in the adoption by the Commission in November 2005 of the *Green Paper on a European Programme for Critical Infrastructure Protection*.

EPCIP Approaches

Should there be a legislative framework approach, or a voluntary approach towards the establishment of EPCIP? Previous experience had shown that taking a voluntary approach to critical infrastructure protection might not result in increased security standards. The best approach seemed to be to have a legislative, common framework around the basic principles of EPCIP, but not towards each sector or to go beyond the principle of subsidiarity.

The question whether there should be an 'all-hazards approach' regarding critical infrastructure protection, or a special focus on the particular threat of deliberate attack, i.e. terrorism, had already been decided upon when the Council adopted several conclusions on EPCIP³ in December 2005. While recognising the threat from terrorism as a priority, the Council agreed that the protection of critical infrastructure should be based on an all-hazards approach. What should be taken into account, however, was the possible overlap of such an approach with the current legislative framework such as the EU directives on security of supply, the Seveso directive⁴, and others.

CIWIN

The Commission developed a number of rapid alert systems allowing for the concrete, coordinated and effective response in case of emergencies, including those of a terrorist origin. In October 2004, it announced the creation of a

² [COM\(2004\) 702 final](#), 20 October 2004.

³ [2696th Council Meeting, Justice and Home Affairs](#), 1-2 December 2005.

⁴ Following an industrial accident, [Council Directive 82/501/EEC](#) was adopted.

central network in the Commission ensuring rapid information flows between all rapid alert systems and concerned Commission services (ARGUS).

The Commission has suggested creating CIWIN to stimulate the development of appropriate protection measures by facilitating an exchange of best practices in a secure manner as well as being a vehicle for transmission of immediate threats and alerts. The system would ensure that the right people have the right information at the right time. In this way, the Commission could communicate directly with the owners and operators of critical infrastructure. In early March 2006, a tender for a study on the creation of CIWIN⁵ had been launched.

Key Principles for EPCIP

One of the key principles of EPCIP should be confidentiality. There is a need to guarantee the confidentiality of sensitive information. The best way to do this was to have the sharing of data on specific infrastructure be the responsibility of Member States. The mapping of the EU's critical infrastructure would not be appropriate if confidentiality could not be ensured because this list would be a liability in itself. The information provided by Member States to the Commission should therefore be limited to statistical information, trends and the level of compliance.

Another key principle should be proportionality. Protection strategies and measures should be proportionate to the level of risk involved. Protection measures should be defined on a sector by sector basis. Not all areas of critical infrastructure could be protected from all risks, because risk levels differed from one country or region to another.

Energy operators should ensure an adequate level of security through the deployment of security plans. Because the Commission could only go so far as setting up a network onto the Member State level, Member States should analyse the external threat, define the threat levels, and audit the deployment of security plans at the national level. The Commission should provide an overview of the effectiveness of the Member States in auditing the security plans, and it could also have a coordinating role whenever a disruption would have transnational consequences.

The protection of critical infrastructure was not only a European issue but also a global issue. The installations and features of critical infrastructure

protection had impact beyond the EU's borders, i.e. with regard to oil and gas pipeline security. There should be sufficient communication with the appropriate departments in the Commission whether critical infrastructure protection measures could also be considered in an external context. Even though funding for critical infrastructure protection was not possible outside of EU borders, cooperation agreements could be considered in the framework of the European Neighbourhood Instrument. Also, coordination could be envisioned with the European Investment Bank on loans to the private sector that take into account critical infrastructure protection investments.

Cooperation between the EU and NATO on the issue of critical infrastructure protection was not always easy. There were different roles and responsibilities. Cooperation was needed however to avoid duplication. Within NATO, in the EAPC format, critical infrastructure protection and civil emergency planning has been discussed. Regarding critical infrastructure protection, NATO worked with Russia, Ukraine, countries in the Caucasus, and countries in Central Asia.

European efforts to enhance critical infrastructure protection should take into account experiences in other parts of the world. New measures and standards adopted at the EU level should not result in barriers hampering the possible use of effective non-European technology. If the ultimate goal was to provide protection for EU citizens, the technologies and products that best could serve this purpose should be used, irrespective of their origins.

⁵ [Study on EU Cross-border alert networks used by police authorities and the creation of a Critical Infrastructure Warning Information Network \(CIWIN\)](#), 4 March 2006.

Additional Information

For more information about the EastWest Institute *Consortium on Security and Technology*, please contact:

Daniel Bautista

Program Manager
Global Security Program
Tel +32-2 743.46.28
Mob +32-47 348.25.90
Fax +32-2 743.46.39
Email dbautista@ewi.info

Erol Spencer Hofmans

Project Manager
Global Security Program
Tel +32-2 743.46.28
Mob +32-47 554.85.56
Fax +32-2 743.46.39
Email ehofmans@ewi.info