

COMMISSION OF THE EUROPEAN COMMUNITIES

Brussels, 20.10.2004
COM(2004) 702 final

COMMUNICATION FROM THE COMMISSION TO THE COUNCIL AND THE EUROPEAN PARLIAMENT

Critical Infrastructure Protection in the fight against terrorism

TABLE OF CONTENTS

1. INTRODUCTION 3

2. THE THREAT 3

3. EUROPE'S CRITICAL INFRASTRUCTURES 3

3.1. What is critical infrastructure 3

3.2. Security Management 5

4. Progress so far in protection of critical infrastructure at Community level 6

5. ENHANCING EU'S CRITICAL INFRASTRUCTURE PROTECTION CAPABILITY 7

5.1. A European Programme for Critical Infrastructure Protection 7

5.2. Implementing EPCIP 8

5.3. EPCIP objectives and progress indicators 9

TECHNICAL ANNEX 10

1. INTRODUCTION

The European Council of June 2004 asked the Commission and the High Representative to prepare an overall strategy to protect critical infrastructure.

The present Communication gives an overview of the actions that the Commission is currently taking on protection of critical infrastructure and proposes additional measures to strengthen existing instruments and to meet the mandates given by the European Council.

2. THE THREAT

The potential for catastrophic terrorist attacks that affect critical infrastructures is increasing. The consequences of an attack on the industrial control systems of critical infrastructure could vary widely. It is commonly assumed that a successful cyber attack would cause few, if any, casualties, but might result in loss of vital infrastructure service. For example, a successful cyber-attack on the public telephone switching network might deprive customers of telephone service while technicians reset and repaired the switching network. An attack on a chemical or liquid natural gas facility's control systems might lead to more widespread loss of lives as well as significant physical damage.

Another type of catastrophic infrastructure failure might be when one part of the infrastructure leads to the failure of other parts, causing widespread cascade effect. Such failure might occur due to the synergistic effect of infrastructure industries on each other. A simple example might be an attack on electrical utilities where electricity distribution was disrupted; sewage treatment plants and waterworks could also fail, as the turbines and other electrical apparatuses in these facilities might shut down.

Cascade events can be very damaging too, causing widespread utility outages. The blackouts in North-America and Europe during the last two years have put in evidence the vulnerability of energy infrastructures and consequently the need to find effective measures to prevent/or to mitigate the consequences derived from a major supply disruption. This use of cyber-terrorism could also result in an amplification of the physical attack's effects. An example of this might be a conventional bombing attack on a building combined with a temporary denial of electrical or telephone service. The resulting degradation of emergency response, until back-up electrical or communication systems can be brought into place and used, could increase the number of casualties and public panic.

3. EUROPE'S CRITICAL INFRASTRUCTURES

3.1. What is critical infrastructure

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 in the Member States. 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. Some critical elements

in these sectors are not strictly speaking 'infrastructure', but are in fact, networks or supply chains that support the delivery of an essential product or service. For example the supply of food or water to our major urban areas is dependent on some key facilities, but also a complex network of producers, processors, manufacturers, distributors and retailers.

Critical infrastructures include:

- Energy installations and networks (e.g. electrical power, oil and gas production, storage facilities and refineries, transmission and distribution system).

- Communications and Information Technology (e.g. telecommunications, broadcasting systems, software, hardware and networks including the Internet)

- Finance (e.g. banking, securities and investment)

- Health Care (e.g. hospitals, health care and blood supply facilities, laboratories and pharmaceuticals, search and rescue, emergency services)

- Food (e.g. safety, production means, wholesale distribution and food industry)

- Water (e.g. dams, storage, treatment and networks)

- Transport (e.g. airports, ports, intermodal facilities, railway and mass transit networks, traffic control systems)

- Production, storage and transport of dangerous goods (e.g. chemical, biological, radiological and nuclear materials)

- Government (e.g. critical services, facilities, information networks, assets and key national sites and monuments)

These infrastructures are owned or operated by both the public and the private sector. However, in its Communication 574/2001 of 10 October 2001, the Commission has declared: "The reinforcement of certain security measures by the public authorities in the wake of attacks directed against society as a whole and not at the industry players must be borne by the State". The public sector has therefore a fundamental role to play.

Critical infrastructures must be defined at Member States' level and at European level and such lists should be established by the end of 2005.

Europe's critical infrastructures are highly connected and highly interdependent. Corporate consolidation, industry rationalization, efficient business practices such as just-in-time manufacturing and population concentration in urban areas have all contributed to this situation. Europe's critical infrastructures have become more dependent on common information technologies, including the internet and space-based radio-navigation and communication. Problems can cascade through these interdependent infrastructures, causing unexpected and increasingly more serious failures of essential services. Interconnectedness and interdependence make these infrastructures more vulnerable to disruption or destruction.

The criteria for determining the factors that make a particular infrastructure or element of an infrastructure critical need to be studied. These selection criteria should also be based on a sectoral and collective expertise. Three factors might be suggested for identifying potential critical infrastructure:

- Scope - The loss of a critical infrastructure element is rated by the extent of the geographic area which could be affected by its loss or unavailability - international, national, provincial/territorial or local.

- Magnitude - The degree of the impact or loss can be assessed as None, Minimal, Moderate or Major. Among the criteria which could be used to assess potential magnitude are:

    (a) Public impact (amount of population affected, loss of life, medical illness, serious injury, evacuation);

    (b) Economic (GDP effect, significance of economic loss and/or degradation of products or services);

    (c) Environmental (impact on the public and surrounding location); and

    (d) Interdependency (between other critical infrastructure elements).

    (e) Political (confidence in the ability of government);

- Effects of time - This criteria ascertains at what point the loss of an element could have a serious impact (i.e. immediate, 24-48 hours, one week, other).

However, in many cases, psychological effects may escalate otherwise minor events.

Current critical infrastructure protection developments are documented in technical annex which provides a sector based overview of Commission achievements accomplished so far. They show that the Commission has acquired considerable experience in this field.

3.2. Security Management

Information from a number of sources is needed to conduct threat, incident and vulnerability analysis of Member States critical infrastructure elements and their dependencies. Each sector and Member State will need to identify infrastructure critical to them, within their respective jurisdictions according to a EU harmonised formula and the organisations or persons in charge of security.

Not all infrastructures can be protected from all threats. For example, electricity transmission networks are too large to fence or guard. By applying risk management techniques, attention can be focused on areas of greatest risk, taking into account the threat, relative criticality, the existing level of protective security and the effectiveness of available mitigation strategies for business continuity.

Security Management is a deliberate process of understanding risk and deciding upon and implementing actions to reduce risk to a defined level, which is an acceptable level of risk at an acceptable cost. This approach is characterized by identifying, measuring, and controlling risks to a level commensurate with an assigned level.

Critical infrastructure protection (CIP) requires a consistent, cooperative partnership between the owners and operators of critical infrastructure and Member States authorities. The responsibility for managing risk within physical facilities, supply chains, information technologies and communication networks primarily rests with the owners and operators.

Alerts, advisories and information notes must be issued to help public and private sector stakeholders protect key infrastructure systems. From time to time specific risks or threats of a terrorist attack may emerge that require an immediate response. On these occasions a well coordinated operationally focused response will be required from Member States Governments and industry. In these circumstances the EU should coordinate the necessary political responses, and on that basis detailed supporting arrangements will be agreed with stakeholders on a case-by-case basis.

Even the best security management plans and legislation which compel to their enforcement are worthless without proper implementation. Experience proves that independent Commission security inspections of their implementation are the only efficient instrument to guarantee the correct implementation of security requirements.

4. PROGRESS SO FAR IN PROTECTION OF CRITICAL INFRASTRUCTURE AT COMMUNITY LEVEL

Europeans expect critical infrastructures to continue to function, regardless of which organisations own or operate the component parts. They expect the Member State governments and the EU to play a leadership role in ensuring that this happens. They expect all levels of government and private sector owners and operators to cooperate to assure the continuity of the services on which Europeans depend.

As a complement to the measures which have been taken at national level, the European Union has already undertaken a number of legislative measures setting minimum standards for infrastructure protection in the framework of its different EU policies. It is notably the case in the transport, communication, energy, occupational health and safety, and public health sectors. Activities have been boosted after the recent assaults in America and Europe. They will lead to a further improvement or an extension of existing measures.

For decades, inspections have been conducted in the framework of the EURATOM Treaty to control the proper use of nuclear materials. In the radiation protection field, there is a considerable number of legislation that applies to the risks related to the operation of facilities and the use of sources involving radioactive substances.

In the field of international transport, the European Union adopted legislation implementing or reinforcing the agreements reached by the international ruling bodies in the aviation and maritime sectors. The European Union will continue to promote and actively participate in their activities at international level. It will encourage Third Countries which have economic relations with the EU to implement these Agreements. It has provided some assistance to some of them, with a view to reach a homogeneous and constant level of security within and beyond EU borders.

A further step is being made with the creation of agencies, such as the European Network and Information Security Agency (ENISA) for communication security. In addition, in sectors like aviation and maritime security, inspection services have been created within the Commission

to inspect the implementation of security legislation by the Member States. These inspections are producing the necessary benchmark which ensures an equal implementing level in the Union.

Current critical infrastructure protection developments are documented in technical annex which provides a sector based overview of Commission achievements accomplished so far. They show that the Commission has acquired considerable experience in this field.

5. ENHANCING EU'S CRITICAL INFRASTRUCTURE PROTECTION CAPABILITY

5.1. A European Programme for Critical Infrastructure Protection

Bearing in mind the great number of potential critical infrastructures and their own particularities, it is impossible to protect them all by European level measures. By applying the subsidiarity principle, Europe must concentrate its efforts on the protection of infrastructures having a transboundary effect and let the others under the sole responsibility of the Member States but under a common framework.

Numerous Directives and Regulations already exist, which impose means for the detection of accidents, the establishment of intervention plans in cooperation with Civil Defence, regular exercises and clear links between the different intervention levels, public powers, central organisations and urgency services. On the other end, a lot remains to be done on the protection of energy installations other than nuclear. As showed in technical annex, a Community acquis exists in critical infrastructures protection at a variable level of development.

In most of the domains mentioned above, work is going on and cooperation with Member States' experts and the concerned economical sectors is established to identify the possible shortcomings and the corrective measures to apply (legal or others). Many networks and security committees have been established.

The Commission will report progress to the other institutions each calendar year in a Communication. It will analyse for each sector the developments of community work in the field of risk evaluation, development of protection techniques, or ongoing/envisaged legal actions in order to collect their advice. The Commission will further propose in this Communication, if necessary, updates and horizontal organisational measures for which there is a need for harmonisation, coordination or cooperation. This Communication integrating all the sectoral analyses and measures shall constitute the base of a European Programme for Critical Infrastructure Protection (EPCIP).

Such a programme will seek to assist industry and Member States Governments at all levels in the EU, while respecting individual mandates and accountabilities. The Commission is of the opinion that a network assembling EU Member States CIP specialists could assist the Commission in drawing up the programme – this Critical Infrastructure Warning Information Network (CIWIN) should be set up as soon as possible in 2005.

The setting up of the network should assist mainly in stimulating an exchange of information on shared threats and vulnerabilities and appropriate measures and strategies to mitigate risk in support of critical infrastructure protection. Member States would therefore in turn make

sure that the relevant information is passed to all relevant governmental departments and agencies, including emergency services organisations, informing relevant industry sector bodies so that they in turn will inform affected owners and operators of critical infrastructure through a network of contacts established within the Member States.

EPCIP would promote an ongoing forum where the constraints of competition, liability and information sensitivity can be balanced with the benefits of a more secure critical infrastructure. Industry will be closely consulted in this process. It will help provide more information to partners on specific threat situations that will allow them to take actions to deal with their potential consequences. The responsibility and accountability of owners and operators to make their own decisions and plans for protecting their own assets should not change.

When sectoral standards do not exist or where international norms have not yet been established, the European Committee for Standardization (CEN) and other relevant standardisation organisations could assist the network and propose uniform security sectoral and adapted standards for all the various branches and sectors interested. Such standards should be also proposed at an international level through ISO in order to establish a proper level playing field in this respect.

Care must be taken when referring to national security threats to critical infrastructure, including terrorism, so as to avoid undue concern in the EU domestically as well as for potential tourists and investors. Terrorism is a constant threat but it is the task of policy makers to encourage all to carry on their lives as undisturbed as possible. Care must also be taken to ensure respect of privacy rights, both inside and outside the Union. Consumers and operators must have confidence that information will be handled accurately, confidentially and reliably. It is necessary to have in place an appropriate framework to ensure that classified information is properly managed and protected from unauthorised use or disclosure.

Much of both EU and Member State critical infrastructure steps across the borders of the EU. Pipelines stretch across continents, cables vital to information technology services are buried deep on ocean floor beds etc. This means that international cooperation is an important component in establishing ongoing, dynamic national and international partnerships among critical infrastructure owners/operators and third country governments, in particular direct suppliers of energy products to the Union.

5.2. Implementing EPCIP

Critical infrastructure protection requires the active participation of the owners and operators of infrastructure, regulators, professional bodies and industry associations and Member States and the Commission. Based on the information supplied by Member States interfaces and the network, the objectives of the EPCIP will be to continue to identify critical infrastructure, analyse vulnerability and interdependence, and come forward with solutions to protect from, and prepare for, all hazards. This would include assisting industry sectors with understanding the threat and consequence variables in their risk assessments. Member States law enforcement agencies and the civil protection mechanism should ensure that EPCIP is an integral part of their planning and awareness raising.

In close coordination with the network, the Commission services will develop further actions which should consist in the adoption of legislation and/or dissemination of information. The Task Force of the Chiefs of Police and Europol would have a role to play in disseminating the

relevant security levels and intelligence information to the Member States' law enforcement agencies, who in their turn should advise and liaise with critical infrastructure owners and operators on relevant threat information, assist in the provision of protective security advice and development of protective security strategies to counter terrorism.

Member States Governments will continue and/or develop and maintain databases of nationally significant critical infrastructure and would be responsible for the development, validation and audit of relevant plans and so ensure continuity of services under their jurisdictions When laying down the EPCIP the Commission would put forward suggestions as to what should be the minimum content and format of such databases and how they should be inter-connected.

The Member States Governments would in turn continue to inform the owners and operators of critical infrastructure (as well as other Member States, if appropriate) relevant intelligence and alerts as well as the agreed type of response expected for each level of threat/alert to stakeholders.

Owners and operators of critical infrastructure would provide adequate security of their assets by actively implementing their security plans and conducting regular inspections, exercises, assessments and plans. Member States should control the overall process while the Commission should ensure an equal implementation throughout the Union with adequate inspection systems.

5.3. EPCIP objectives and progress indicators

The goal of EPCIP and the duty of the Commission would be to ensure that there are adequate and equal levels of protective security on critical infrastructure, minimal single points of failure and rapid, tested recovery arrangements throughout the Union. EPCIP would be an ongoing process and regular review will be required to keep abreast of the issues and concerns within the community.

Success shall be measured by:

- The Member States governments' identification and establishment of inventories of critical infrastructures in their jurisdictions according to the EPCIP drawn up priorities;

- Businesses collaborating within sectors and with government to share information, and reduce the likelihood of incidents causing widespread or lengthy disruption to critical infrastructures;

- The European Community resolves to establish a common approach to tackling the security of critical infrastructures through cooperation of all public and private actors.

TECHNICAL ANNEX

GLOSSARY

Critical Infrastructure (CI)

Those physical resources; services; and information technology facilities, networks and assets which, if disrupted or destroyed, would have a serious impact on the health, safety, security or economic well-being of Europeans or the effective functioning of the EU or its Member States governments.

Critical infrastructure Warning Information Network (CIWIN)

A EU network to assist Member States, EU Institutions, owners and operators of critical infrastructure to exchange information on shared threats, vulnerabilities and appropriate measures and strategies to mitigate risk in support of critical infrastructure protection.

Critical Infrastructure Protection (CIP)

The programs, activities and interactions used by owners and operators to protect their critical infrastructure.

CIP capability

The ability to prepare for, protect against, mitigate, respond to, and recover from critical infrastructure disruptions or destruction.

European programme for Critical Infrastructure Protection (EPCIP)

A programme to provide enhanced security for critical infrastructure as an ongoing, dynamic, national partnership among EU institutions, critical infrastructure owner/operators and EU Member States to assure the continued functioning of Europe's critical infrastructure

Infrastructure

The framework of interdependent networks and systems comprising identifiable industries, institutions (including people and procedures), and distribution capabilities that provide a reliable flow of products and services, the smooth functioning of governments at all levels, and society as a whole.

Risk

The possibility of loss, damage or injury. The level of risk is a condition of two factors: (1) the value placed on the asset by its owner/operator and the impact of loss or change to the asset, and (2) the likelihood that a specific vulnerability will be exploited by a particular threat.

Risk Assessment

A process of evaluating threats to the vulnerabilities of an asset to give an expert opinion on the probability of loss or damage and its impact, as a guide to taking action.

Risk Management

A deliberate process of understanding risk and deciding upon and implementing actions to reduce risk to a defined level, which is an acceptable level of risk at an acceptable cost. This approach is characterized by identifying, measuring, and controlling risks to a level commensurate with an assigned level.

Threat

Any event that has the potential to disrupt or destroy critical infrastructure, or any element thereof. An all-hazards approach to threat includes accidents, natural hazards as well as deliberate attacks.

Threat Assessment

A standardized and reliable manner to evaluate threats to infrastructure.

Vulnerability

A characteristic of an element of the critical infrastructure's design, implementation, or operation that renders it susceptible to destruction or incapacitation by a threat.