# Protecting Europe's Critical Infrastructures: Problems and Prospects

**Åsa Fritzon*, Kristin Ljungkvist*, Arjen Boin** and Mark Rhinard***

*Swedish Institute of International Affairs, Stockholm, Sweden. E-mail: asa.fritzon@ui.se, kristin.ljungkvist@ui.se, mark.rhinard@ui.se
**Leiden University Crisis Research Center, Department of Public Administration, Leiden, The Netherlands. E-mail: boin@fsw.leidenuniv.nl

**The European Union has become increasingly involved with protecting the security and safety of European citizens. The latest addition to this new policy space is critical infrastructure protection (CIP) at the EU level. A central role for the EU in guarding against infrastructural breakdowns and preparing for failures may seem self-evident. In reality, the precise nature of such a role remains unclear. Moreover, enthusiastic rhetoric is not always matched by firm action. This article surveys what the EU has in place in terms of CIP and identifies outstanding issues for debate.**

## Introduction: Protecting Europe and its Citizens

The European Union (EU), typically associated with economic cooperation, has become increasingly involved with protecting the security and safety of European citizens. From pandemic preparedness to food safety, and from disaster response to counter-terrorism initiatives, the EU institutions and agencies now play a role. Those efforts signal a qualitatively new type of cooperation in the EU, and the emergence of a 'European protection policy space' (Boin, Ekengren and Rhinard, 2006).

The latest addition to this new policy space is CIP at the EU level. The interconnectedness of European critical infrastructures (CIs), hastened through the drive towards a single market, has brought unprecedented efficiency and prosperity across the continent. That same interconnectedness, however, increases the potential for cross-border crises when infrastructures fail. This increased vulnerability was borne out by the power cuts that swept across ten European countries during the first weekend of November 2006 (Strauss, 2006).

Because CIs span many national borders in Europe, a role for the EU in guarding against breakdowns and preparing for failures seems evident. The precise nature of such a role, however, is unclear. Although the EU has announced plans for a European Programme for Critical Infrastructure Protection (EPCIP), it has only recently sought to identify what infrastructures are 'European' in operation and effect. Practical work on how to protect those infrastructures and how to manage breakdowns is in a nascent stage. Meanwhile, private firms and national governments have reacted with no small degree of scepticism regarding the role of European institutions. Despite these uncertainties, the EU institutions are pressing on. The EPCIP discussion paper has given way to a proposal for legislation, followed by sectoral approaches to protecting specific infrastructures.

This article argues that enthusiastic rhetoric about EU CIP should be tempered by a more forthright appraisal of the key challenges to cooperation. We

begin the article by briefly sketching the backdrop for discussion, including the growing role of the EU in 'protection' issues and the rise of CIP on the EU agenda as part of that trend. We then survey a select set of CIs, documenting EU initiatives to protect those infrastructures from breakdowns. The subsequent section identifies some basic questions that remain unanswered in the EU's approach to CIP. The conclusion summarizes the discussion and sets out the importance of clarifying uncertainties before the EU proceeds in this 'high stakes' policy area.

## The Rise of CIP on the EU Agenda

The emergence of CIP programs at the European level represents a growing trend. Across a number of issue areas, EU Member States have opted for crisis management cooperation through supranational institutions. In some areas, cooperation amounts to information sharing and the spreading of best practices. In other areas, cooperation goes further to include binding legislation and a commitment to speak as one voice. Despite differing degrees to which Europe 'matters' across the issue spectrum, the EU's efforts share a common focus on the protection of people, vital systems, and core societal values from dangerous threats.

This development reflects a qualitatively new role for the EU beyond economic management. A 'European protection policy space' is emerging (Boin, Ekengren and Rhinard, 2006). This protection space cuts across policy sectors and EU institutions, comprising all activities, mechanisms, resources and other means to deal with transboundary crises.[1]

In the area of public health, for instance, EU governments have agreed to create common surveillance programs and guidelines for pandemic preparedness and continuity planning, alongside the creation of a new agency for disease prevention and control. In the area of food safety, European cooperation aims to ensure the integrity of food supplies, from animal health inspections to food processing standards and rapid alert systems that can flag potential crises. Moreover, the EU is increasingly coordinating counter-terrorism programs through such institutions as Europol and Eurojust. National governments have delegated authority to the EU level to organize resource sharing in the event of transboundary disasters. A Monitoring and Information Centre alerts EU governments to impending crises, and signals when cooperative action might be required. Protection activities extend into the external domain: the European Security and Defence Policy (ESDP) improves the Union's capacity to deal with crises and disasters that occur outside its territorial boundaries (Duke and Ojanen, 2006).

The EU may engage in a wide array of protection activities, but the intensity of cooperation differs dramatically between sectors. Different laws determine the extent to which a sector is subject to 'Community competence' and thus to formal decision-making and participation by supranational institutions. When considering EU policy making, these particular features must be taken into account. The EU comes with its own set of institutions, policy dynamics, and autonomous drivers that shape and constrain developments (Hix, 2005).

### *CIP as a global policy problem*

CIP is a new addition to the EU's protection policy space, but is not a new issue at national and global levels. The reliance of modern societies on infrastructures has been exposed through a number of incidents. The threat of the 'Y2K' bug, although never fully materialized, led to widespread concern about the robustness of vital infrastructures. Hurricane Katrina demonstrated the panic and destruction that occurs when vital services fail. And a spate of recent terror attacks, from 9/11 to the 2005 London bombings, refocused attention on protecting the systems that enable societies to function. Often, the indispensable nature of these CIs becomes apparent only when an actual disruption occurs.

In both academic and practitioner circles, it is widely perceived that large-scale systems have become increasingly vulnerable to catastrophic breakdowns (Perrow, 1999; De Bruijne and Van Eeten, 2007). As critical systems become increasingly complex and integrated across geographic and functional borders, relatively small disturbances can rapidly cascade into multifaceted crises.

As a result, CI vulnerabilities have garnered high-level political attention in recent years. The Clinton administration began to work with the CIP concept during the aftermath of the Oklahoma bombings (Executive Order, 1996). The administration realized that the breakdown of certain infrastructures could have a devastating impact on US security and began to consider ways to protect these infrastructures from breakdown. The Clinton initiative adapted an approach used in conventional wartime planning – the protection of strategic targets vital for national interests – to modern developments and threats.

The emergence of CIP as a concept, however, has done nothing to clarify the many uncertainties associated with it (see Egan, this issue). For one, defining 'critical infrastructure' is problematic, considering that many vital systems crosscut and rely upon one another. This can explain the tendency to focus on Critical *Information* Infrastructure Protection (CIIP) as much

as, or even more so than, CIP itself. The threat of the Y2K bug focused minds on CIIP, which refers to the protection of systems such as telecommunications, computer hardware and software, internet, satellites, and fibre optics. These infrastructures are essential for the proper functioning of most other CIs and are a crucial tool for managing risk factors and returning infrastructures to order after a breakdown occurs (Metzger, 2004).

### *European developments in CIP*

In June 2004, three months after the Madrid train bombings, the European Council asked the European Commission to prepare an overall strategy to protect the Union's CIs. In response, the Commission published a Communication (a pre-legislative proposal) entitled 'Critical Infrastructure Protection in the Fight Against Terrorism'. In the Communication, the Commission defines CI as consisting 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' (Commission, 2004: 3).

This Communication can be seen as the first European step towards protecting European CIs. Not surprisingly, the EU focused initially on terrorism as the source of disruption. It was soon acknowledged, however, that other forces – such as natural disasters, managerial negligence, criminal activity or sabotage – could also cause CIs to break down. Over time, the EU policy on CI has evolved into an all-hazards approach.

In December 2004, European ministers endorsed the idea of a more detailed program for CIP. Knowing the considerable complexities associated with CIP, the Commission responded in 2005 with a 'Green Paper' on EPCIP rather than with legislation. The Green Paper sought to propose questions, present ideas, and gather input from relevant stakeholders. Since then, discussions and consultations have taken place with CI operators, national authorities, private firms, and other interested parties with a view to eventually formulating more specific legislation.

The Green Paper suggests an ambitious goal for EPCIP: to ensure adequate levels of protection and rapid recovery arrangements within the Union. The Green Paper adopts the principle of subsidiarity, whereby Member States remain responsible for national CIP under a common framework. The EU would concentrate only on aspects of CIP with cross-border effects. The common European framework could be mandatory, voluntary or a mixture of the two, but according to the Commission, only a legally binding framework can provide a strong and enforceable basis for protecting European CIs.

The Green Paper adopts a sweeping definition of CI, which would include a wide variety of sectors and services. At the same time, the Green Paper definitions are underspecified in terms of functions, products and services delivered. The definition of what constitutes a *European* CI would be determined by its cross-border effect. Discussion remains whether cross-border effects must apply to at least two or three Member States (the Commission seems to prefer the former definition).

The Green Paper suggests a common EPCIP framework that would define the competence and responsibilities of all CIP stakeholders and lay the foundations for sector specific approaches. The proposed framework would include common principles, common codes and standards, common definitions of CI sectors and CIP priority areas, a formal description of stakeholder responsibilities, benchmarks, and a common methodology. The Green Paper also states that EPCIP should complement sectoral measures already in place in Brussels and in the Member States.

The Commission has moved ahead preparing an overarching legislative package in November 2006. The package, if approved as planned, includes a proposal for a decision (a binding legislative instrument) on EPCIP, along with sectoral proposals (Commission, 2006b). In regards to the latter, several Commission DGs are formulating sector-specific ideas for CIP. DG Transport and Energy (DG TREN), for instance, will present a Communication including ideas for a comprehensive approach to energy infrastructure protection. This confirms a more general move in the EU toward developing CIP principles on a sector-by-sector basis. Such a strategy allows for CIP to be tailored to different CI needs and varying legal competences for CIP across the policy spectrum.

## Sector Policies Related to EU CIP

A deeper understanding of the EU's CIP efforts requires us to focus not just on the general, horizontal EPCIP program. In addition, we must examine specific policy sectors and consider the CI issues in those sectors. In this section, we survey several policy sectors that relate to the provision of critical services and thus raise CIP issues. In these sectors, many policies have been put in place as the result of the drive to a single market; their effects on CI are equally important.

It should be noted that this survey is not comprehensive. For a full listing of CI issues deemed relevant by

the EU, one should consult the Green Paper discussed above. This section offers a sampling of the key issues confronting several sectors of CIP in the EU.

## Energy

The EU has discussed various aspects of energy safety since the end of the 1960s. For example, the EU prescribed minimum storage levels of oil and other petroleum products (Eriksson and Barck-Holst, 2005). The European Commission has assumed a coordinating function for ensuring maintenance of emergency stocks; this task includes gathering and publishing regular oil stocks data from Member States.[2] However, there is no European legislation in the energy area that protects energy distribution systems against accidents, except in the nuclear field (discussed below). The Member States remain responsible for ensuring the safety of energy supplies and energy systems (Jönsson and Jarlsvik, 2005).

In 1996, the European Council adopted guidelines for the development of the trans-European energy network (TEN-E). This project is part of the European Union's overall energy policy, which aims to increase competitiveness in the electricity and gas markets and to enhance the security of supply (as well as the protection of the environment).[3]

In 2003, the Commission introduced measures to safeguard security of electricity supply and infrastructure investment (Commission, 2003). The resulting regulatory framework directs Member States to develop strategies for safeguarding energy supply and to make sure the systems live up to certain security standards related to transfer capacity, information provision and network modelling. The Member States must ensure that their distribution systems hold sufficient capacity for cross-border interconnections. The Commission has formulated measures to secure Europe's gas supply, to improve gas transmission networks and to develop the internal gas market. Protection of hardware such as pipes and pumps is less of an issue, since most gas infrastructure is underground.

On 8 March 2006 the European Commission published a Green Paper on developing a common, coherent European Energy Policy (Commission, 2006). This Green Paper posits a new and problematic global energy era in which Europe has an urgent need to invest in aging energy infrastructures and to plan for increasing energy demand and import dependency.

The security of energy in the EU was placed in sharp focus after a power cut plunged millions of homes across Europe into darkness in early November 2006. An electricity failure in Germany revealed the mutual dependence of European grids, as power cuts cascaded across the continent. Romano Prodi, Italian prime minister, used the event to push for a single European power authority to coordinate supply (Strauss, 2006).

## Information and Communication Technologies (ICT)

The area of ICT security has developed extensively within the EU over the past few years. There is a large body of EU legislation, regulation and programs aimed at the protection of telecommunications, media and IT (the Commission addresses these infrastructures in combination) (Jönsson and Jarlsvik, 2005).

Within an area the EU calls 'Network and Information Security', the EU approach includes specific network and information security measures, a regulatory framework for electronic communications (which also addresses issues of privacy and data protection) and measures against cyber crime. The Member States are responsible for ensuring that the integrity and security of public communications networks are maintained – the *level* of security or *how* it should be maintained remains undefined.

Within the framework of the 'eEurope' program, which is part of the Lisbon Strategy, the aim is to create common specifications on, for example, personal integrity and user control, and to develop a secure infrastructure.[4] The eEurope 2005 action plan aims to improve the robustness of networks and information systems against both accidents and criminal attacks. The Commission and Member States are working together on the Interchange of Data between Administrations (IDA) project, designed to develop a secure trans-European communications network through which they can share classified information. The EU has also developed rules to secure electronic communications through such means as the electronic signatures directive and the data protection legislation for electronic communication.[5]

In 2005, the Council adopted a proposed Framework Decision on attacks against information systems. The objectives are to synchronize criminal law within the Union in the area of attacks against information systems and to ensure police and judicial cooperation regarding criminal offences related to attacks against information systems. It covers intentional hacking, distribution of viruses, denial of service attacks and website defacement, among other activities.

The EU has also established a bureau for information security: the European Network and Information Security Agency (ENISA). This centre is part of the implementation strategy of the EU ICT policy and is designed to help Member States, businesses and industries within the Union to prevent, manage, and solve problems of ICT security. The Member States maintain

the overall responsibility for ICT security in their territory. ENISA collects and analyses information from the Member States, using that information to develop recommendations and offer support.[6]

## Water

The EU has no legislation with an explicit goal of protecting water-delivery systems (Jönsson and Jarlsvik, 2005). The EU has adopted several directives concerning water quality, however. Legislation includes a framework directive in the area of water policy for the protection of inland surface waters, transitional waters, coastal waters and groundwater. The general purpose is to prevent and reduce pollution, promote sustainable water use, protect the aquatic environment, improve the status of aquatic ecosystems and mitigate the effects of floods and droughts.

A Council directive from 1998 defines essential quality standards that water intended for human consumption must meet (Council, 1998). The Council directive of 1991 addresses the collection, treatment and discharge of urban wastewater and the treatment and discharge of wastewater from certain industrial sectors (Council, 1991). The main goal of that legislation is to protect the environment.

## Food

Food safety is an extensive area of EU competence, aimed at protecting the health of European citizens. Historically, the Common Agricultural Policy (CAP) was created to ensure an adequate supply of food to the European population. That goal was accomplished and followed by an array of regulations seeking greater food safety 'from farm to fork'. Today's food safety activities in the EU relate to the areas of public health, animal health, nutrition and welfare, plant health, product labelling, packaging, food preparation hygiene, and contamination. One of the EU's goals is to improve capacities to detect and manage food crises effectively.

There is considerable legislation in this area. One important event was the widespread review of the 'general principles of food law' and the 'procedures relating to food safety' in 2002. The Council and Parliament adopted a new regulation at the same time as approving the creation of the European Food Safety Authority (EFSA). The regulation aims for a high level of human health and consumer protection in relation to food, while upholding and promoting the functioning of the internal market (Parliament and Council, 2002a). Four measures constitute the substance of the regulation, including: a rapid alert system for food safety, emergency procedures, crisis management guidelines, and the creation of a new regulatory committee.

EFSA was created to provide a scientific reference point for food-related control and evaluation. This means the agency offers scientific advice and risk analysis, while networking national food safety agencies. Several scientific committees housed in the Commission were moved to EFSA to improve capacity in these tasks. The agency also plays a role in RASFF, the rapid alert system for food and feed.[7] Member States, the Commission, and EFSA participate in this system in order to disseminate information on food-related risks rapidly and securely.

The EU's policies intend to cover food safety through the whole of the production and distribution chain, including both animal health and plant health. The remit of the Standing Committee on the Food Chain and Animal Health (SCFCAH), for instance, covers health risks in all food-related areas. There are six more committees that address specific aspects of safety: the Standing Committee on Plant Health; the Standing Committee on Propagating Material and Ornamental Plants; the Standing Committee on Agricultural, Horticultural and Forestry Seeds and Plants; and the Standing Committee on Community Plant Variety Rights and Standing Committee on Zootechnics.[8]

The implementation of European legislation on food safety is largely a national responsibility. The Commission has some oversight powers but, as in most policy areas, it lacks the resources to ensure a consistently high level of compliance.

## Health

Over the past few years, the EU has tried to enhance European capabilities for responding rapidly to health threats. The current 'European Health Strategy and Public Health Programme (2003–2008)' was adopted by the Commission in 2000. This programme encompasses three main objectives: to improve health information on all levels of society, to create a mechanism for responding rapidly to major health threats; and to address health determinants, notably harmful factors linked to lifestyle such as alcohol and drugs (Commission, 2000).

Since 1999, the Commission has managed a Member State network for epidemiological surveillance, which seeks to control communicable disease outbreaks by providing surveillance and early warning and response (Parliament and Council, 1998).[9]

A more complete European surveillance and early warning system entered into force in 2002 with the so-called Health Security Programme, which is part of the Community mechanism to facilitate reinforced co-operation in civil protection assistance (Parliament and Council, 2001). The aim of the Health Security Programme is to provide coordination and support in

terms of emergency preparedness and response capacity. The programme includes plans to coordinate against the threat of biological and chemical agents. In June 2002, as part of the Health Security Programme, a rapid alert system concerning the deliberate release of biological, chemical and radio-nuclear agents (RAS-BICHAT) was established. RAS-BICHAT is overseen by a Health Security Committee, composed of high-level health officials from each of the Member States. The committee is responsible for exchanging information on health-related threats, for coordinating preparedness and response plans, and for devising crisis management strategies.[10]

Another component of health protection in the EU is the European Centre for Disease Prevention and Control (ECDC), created in the spring of 2004 (Parliament and Council, 2004). The ECDC aims to strengthen Europe's defences against infectious diseases such as influenza, SARS and HIV/AIDS. With regards to bioterrorism, the centre contributes to activities related to risk assessment. This concerns bio-agents and their surveillance, laboratory diagnostics, clinical guidelines, training, modelling, and maintaining a directory of experts. The aim of the Commission is to make the ECDC responsibility for the implementation of EU policies in this area. During 2005, the EU adopted its first strategy for pandemic influenza preparedness and response (Commission, 2005b).

The EU health strategy focuses mainly on cooperation and coordination, supporting the exchange of information and knowledge, and assisting with national decision-making. Member States are still fully responsible for the organisation and delivery of health services and health care. This means that the actual CI of medical and hospital care remains the responsibility of national governments.

## Financial

While the financial sector is critical to the economic health of the EU and its Member States, not much attention has been paid at the supranational level to the threat of financial system breakdowns. A European code of conduct exists with regard to electronic payments, which aims to promote security for consumers, traders and issuers (Commission, 1987). In 2001, a Framework Decision on combating fraud and counterfeiting of non-cash means of payment was adopted, which recognizes international fraud and counterfeiting involving any form of non-cash payment as a criminal offence punishable in all Member States.[11] More recently, a directive on the capital adequacy of investment firms and credit card institutions has been adopted, promoting the importance of developing common standards for market risks that credit institutions may bring upon themselves. The directive also provides a framework for the supervision of such risks (Parliament and Council, 2006).

The Giovannini Group is a group of financial-market participants, which advises the European Commission on financial market issues. The group was formed in 1996 and has focused its work on identifying inefficiencies in EU financial markets and proposing practical solutions to improve market integration. The so-called Giovannini Reports address barriers between cross-border infrastructures and aim to eliminate those barriers. In the 'Financial Services Action Plan' for 2000–2005, financial market infrastructure protection was not included, but it has become one of the priorities for the post-2005 period.[12]

## Transport

According to the EPCIP Green Paper, the transport sector comprises road transport, rail transport, air traffic, inland waterways transport and ocean and short-sea shipping. Public transportation is not included, which is noteworthy in the light of the Madrid and London bombings.

The infrastructure for transportation of people and goods across national borders is addressed by the program on 'Trans-European Networks-Transport' (TEN-T), adopted July 1996 by the Council and European Parliament. These guidelines cover roads, railways, inland waterways, airports, seaports, inland ports and traffic management systems that serve the entire continent.[13] They aim to create conditions for effective provision of transport services, to promote an efficient common road transport system, to contribute to the harmonisation of the conditions for competition between transport operators and to encourage respect for rules on working conditions within the industry.[14] The EU's corpus of legislation on road transport is quite large, focusing mainly on individual security e.g. the European Road Safety Action Programme.

Tunnel security and transportation of dangerous goods can also be considered CI issues. In 2002, the Commission proposed a directive to enhance tunnel safety by harmonising minimum safety requirements.[15] International carriage of dangerous goods by land transport is governed by established international agreements.[16]

The European Railway Agency has the task of strengthening safety and interoperability of railways throughout Europe. A mandate has been given to the agency to identify safety levels in the Member States and to determine for each Member State the areas where safety will have to be improved, if necessary. Common Safety Methods (CSMs) and Common Safety Targets (CSTs) are under development. The first set of

CSMs regarding risk evaluation and assessment will be achieved by September 2007, whereas the first set of CSTs regarding examination of current safety performance are due for September 2008.[17]

Aviation security standards are laid down by the International Civil Aviation Organisation (ICAO) and the European Civil Aviation Conference (ECAC). Aviation security was dealt with on a national and intergovernmental basis before the events of 9/11 led to new Community competences in this area.[18] Each Member State must designate a single appropriate authority responsible for the coordination and the monitoring of the implementation of aviation security programmes (Parliament and Council, 2002b).

The European Aviation Safety Agency (EASA) was established in 2002 with specific regulatory and executive tasks in the field of aviation safety. The agency is tasked with providing technical expertise to the European Commission by assisting in the drafting of rules for aviation safety and by providing technical input to help conclude relevant international agreements.[19] The common rules of EASA are compulsory for Member States, and enter into force equally across Europe. Many European safety rules are still drawn up by a variety of bodies, such as the European Civil Aviation Conference and its technical body, the Joint Aviation Authorities (JAAs) and the Group of Aerodrome Safety Regulators (GASR). However, the rules these bodies draw up are not compulsory. As a result, considerable differences with regard to safety standards remain within Europe.[20]

After the *Erika* accident (December 1999) and the *Prestige* accident (November 2002), the EU has introduced legislation aimed at improving the level of maritime safety and the prevention of accidental pollution by ships. In 2002, the European Maritime Safety Agency (EMSA) was established in order to further the implementation of this legislation. The Member States have been directed to ensure the safety of Community shipping and ports in addition to safeguarding port staff, crews and passengers against intentional unlawful acts (Parliament and Council, 2002c).

## *Chemical and Nuclear Industry*

The Council directive on the control of major-accident hazards involving dangerous substances (Seveso II) aims to prevent and limit the consequences to humans and the environment of such accidents in the Union. Operators of facilities with chemical substances are required to produce a major-accident prevention policy and a safety report. Operators are also responsible for emergency plans to be acted upon inside the facility, whereas the proper authorities, decided upon by the Member State, draw up external emergency plans. Member state authorities shall conduct regular inspections of facilities and conduct follow-up assessments on the accident prevention policies and safety reports. Member States are obliged to ensure information dissemination with regard to facilities where an accident has a potential for cross-boundary effects.

A Major Accident Reporting System (MARS) was established to handle information on 'major accidents'. The Major Accident Hazards Bureau (MAHB) is tasked with providing scientific and technical support for the actions of the European Commission in the area of the control of major industrial hazards.

The Euratom Treaty went into force in 1958 with the general objective of contributing to the formation and development of Europe's nuclear industries. The tasks of Euratom are: to promote research and ensure the dissemination of technical information; to establish uniform safety standards to protect the health of workers and of the general public and ensure that they are applied; to facilitate investment and ensure the establishment of the basic installations necessary for the development of nuclear energy in the EU; to ensure that all users in the EU receive a regular and equitable supply of ores and nuclear fuels; and to make certain that civil nuclear materials are not diverted to other (particularly military) purposes. The Commission may send inspectors to Member States with access to all places and data and to all persons who deal with materials, equipment or installations subject to the safeguards.[21]

After the Chernobyl accident (1986), the Commission initiated activities with the intention of making early notification and reliable radiological information available to the EU Member States in case of nuclear accidents. The Joint Research Centre (JRC-IES/REM) in Ispra, Italy, is responsible for the scientific and technical development of three closely related projects that aim to generate information that can support European decision-making during major radiological accidents. ECURIE (European Community Urgent Radiological Information Exchange) notifies the competent authorities and continuously informs them about the current status of the accident and its consequences. EURDEP (European Radiological Data Exchange Platform) makes radiological monitoring data from most European countries available in real-time. ENSEMBLE produces a comprehensive overview and comparison of the contamination predictions calculated by long-range dispersion models.[22]

A directive adopted in 1996 sets forth regulations regarding the preparation and handling of a radiological emergency. The directive applies to all practices that carry the risk of ionizing radiation. It formulates guidelines for the production, processing, handling, use, holding, storage, transport, import to and export from the Community and disposal of radioactive substances (Council, 1996).

## Issues for Policy Development and Institutional Design

The EU has launched a pro-active, ambitious agenda for transboundary CIP. In just a few years, the CIP issue has gone from virtually unnoticed at the supranational level to a top political priority. When national leaders meet in Brussels, they are keen to emphasize the need for a European program. Their declarations suggest a genuine concern for, and understanding of, the dangers of transboundary CIP breakdowns. The Commission's responses, detailed above, set out plans for an encompassing program to identify CIs, to design means and mechanisms for protection, and to begin considering how to manage breakdowns.

Rhetoric, however, may be outpacing reality. Plans to carry forward EPCIP have met with national resistance. Key conceptual questions remain unanswered. Experts disagree on technical solutions. The precise role of the EU in these matters is unclear. Despite these obstacles to policy development, the Commission seems intent on pushing forward with legislation.

In this section, we identify four unresolved tensions regarding CIP at the European level. Technical, institutional, and political uncertainties make it hard to address these tensions. If they remain unresolved in EU policy development, these tensions may stunt the growth – and the effectiveness – of European CIP.

### *Worst-case scenarios versus actual experience*

How many recent breakdowns qualify as truly 'European' in nature? The EU approach to CIP emphasizes the 'what ifs', the dramatic scenarios that constitute worst-case situations for multiple Member States. This stance will undoubtedly meet with applause from some crisis experts in the field, who suggest that 'imagining the unimaginable' is the correct starting point to generate a pro-active approach to crisis management (Schwartz, 2003; Clarke, 2005). Using worst-case scenarios to drive policy approaches also benefits ambitious civil servants seeking to keep an issue high on the political agenda.

It bears considering, however, the actual experience of transboundary breakdowns in Europe. How many 'worst case' breakdowns have actually occurred? How many times has the 'unimaginable' happened? These questions challenge the rationale underlying a worst-case scenario approach. That rationale suggests that the ever-increasing complexity and system integration will inevitably lead to massive breakdowns, through small disturbances snowballing into multifaceted crises (Perrow, 1999). The indispensable nature of critical systems heightens the impression that breakdowns will be severe.

Most CIs, however, appear remarkably resilient. Actual experience in Europe suggests that modern systems are extremely reliable, especially if historical performance is used as a measure. This observation suggests a different analytical angle on CIP: that the reliability of CI is less a function of protection (reactive) efforts, and more the result of effective system design and high-quality personnel used to operate it (JCCM, 1996).

The EU does not seem to appreciate this more nuanced angle to ensuring reliable, resilient CI. The political and emotional force of recent terrorist attacks explains the EU's worst-case approach: it is easier to motivate political leaders to act if the prospect of the unimaginable seems on the horizon. Moreover, the EU's policy tools are better suited for protection activities – such as regulation, standard guidelines, and 'best practice' – than for system design initiatives.

Nevertheless, the EU must make a strong case for its role in CIP. Although the worst-case scenario approach may prove expedient in the short term, the absence of actual breakdowns or the lack of truly transnational crises will raise questions about the resources devoted to CIP. The same political actors who once agreed enthusiastically to protection-oriented programs may question whether the benefits of those programs outweigh the costs (cf. Wildavsky, 1988).

### *Private ownership versus public interest*

Much of what is deemed CI is owned and operated by private actors. The wave of deregulation of service provision and functions traditionally provided by national governments has changed the regulatory landscape. In many European countries, the provision of energy, communication, health care, financial services and transport is now fully or partly privatized.

The mix of private and public ownership of CI introduces challenging questions. Who should bear the costs for CIP: local or national governments, the EU, or the private sector? One may expect private firms to bear the cost of protecting the infrastructures they operate. This reasoning assumes that ensuring the reliability and resilience of systems is the central goal of their business, and is the key to their very existence. However, security measures are expensive. Emergency preparedness comes at a high cost, especially when owners and investors demand profitability. Firms are likely to under invest in measures that would be desirable for society.

The tensions associated with the private production of public goods raise technical, political and even moral issues (Andersson and Malm, 2006). The effects of a breakdown in critical systems can spread across society. Not only will private companies expect

government to bail them out in the event of a major disruption, but the public might expect the same. The question is whether or to what extent safety and security should be considered a public good.

The EU has yet to sort out these difficulties. In Europe, regulators must take account of the dominant role of the private sector. It is essential to establish when and where private sector obligations end and where public responsibilities begin. This major political issue touches upon core issues of 'the state' and thus requires a political debate across society.

Although national governments have begun to grapple with this issue, there appears to be little appetite for conducting such a debate at the EU level. Therefore, the Commission is forced to walk a tightrope between public interests and private responsibilities. In the Green Paper on CIP, for instance, the Commission stresses the importance of engaging owners and operators in partnerships, emphasizing that the success of its protection program depends on the close involvement of CI operators. In effect, the Commission can resort only to highlighting challenging questions – rather than taking steps towards resolving them.

### *Member states versus the Union*

An enduring question in EU politics concerns the division between national and supranational levels of policy competence. In some areas, 'Community competence' is wide ranging, meaning that national governments make policies in cooperation with other states rather than alone. In other areas, Member States have kept the EU institutions at bay. Most policy areas, however, lie in between these extremes.

CI is an example of this latter category. The exact division of competences is uncertain, and depends to a great extent on member state willingness to agree to common policies. As of the time of writing, national governments have yet to cede major responsibility to the Union in this area despite acknowledgements that coordination is necessary. This generates further uncertainties even at a technical level. Who will be responsible for which parts of CIP? Will policy formation take place collectively, whereas policy implementation occurs at the national and local level? How much of a role will binding law play in CIP? Will the current EPCIP be mandatory or voluntary?

These questions touch upon the different roles that the EU can play in European policies, which range from authoritative legislator to simple facilitator. The Council's endorsement of the move towards a European CIP program suggests the EU shall stimulate, support and facilitate, rather than require cooperation. This wording implies that EU policies will establish frameworks and general directions and leave it up to the Member States to work out the details (Council, 2004). The Commission, however, seems to prefer a more binding approach:

> '. . . only a legal framework would provide a strong and enforceable legal basis for a coherent and uniform implementation of measures to protect ECI, as well as defining clearly the respective responsibilities of MS and the Commission. Non-binding voluntary measures, while flexible, would not provide clarity on who does what' (Commission, 2005a: 6).

The Commission treads softly – owing to the recent rejection of the Constitutional Treaty – but there is much at stake. If EPCIP is approved as a binding supranational legislative framework, this could have far-reaching implications for the role of the EU as a security provider. Thus far the EU's role in security policy has been largely implicit, even if it appears to have recently adopted more explicit overtones (Boin, Ekengren and Rhinard, 2006).

At the time of writing, most Member States appear to support the view that the goal of EPCIP should be to raise CIP capability in Europe. The EU's role within that program would be to support, facilitate and provide the necessary tools to enhance CIP. A stronger EU role does not appear likely in view of the technical, institutional, and political difficulties to ensuring adequate security of infrastructures across the continent.

### *Robustness versus resilience*

The EU and national governments have finite resources to invest in CIP. This rather banal observation has profound consequences when considering policy design. Policies can be directed towards protecting against failures through identifying vulnerabilities and repairing weaknesses. Such an approach aims to improve the *robustness* of CIs, making them invulnerable to breakdowns. The hope is that by ensuring vital systems are hard to damage and disturb, the envisioned 'worst case scenario' will never unfold.

Academic debates, however, suggest that breakdowns are inevitable. It points to the importance of designing *resilience* into CIs, and, more broadly, to enhancing a resilient response to infrastructural breakdowns (Boin and McConnell, 2007; LaPorte, 2007).[23] The upshot of these debates is that a 'robustness' approach may not prove the best investment (JCCM, 1994; 1996).

The Green Paper on EPCIP suggests a fairly narrow focus on enhancing the robustness of Europe's CI. The concept of resilience does not feature highly. However, if we accept that CIs can never be completely protected to the degree that a shock, disruption, or attack is ruled

out, the capability to bounce back deserves more attention.

## Conclusion

The EU's CI program is best described as a work in progress. The current EPCIP is less a 'program' than a plan for a program: considerable uncertainties remain in key areas of policy development and institutional design.

The list of infrastructures deemed worthy of protection, for instance, is changing and expanding. There are no operational criteria for what is 'critical', which should be no surprise: different Member States have different answers to that question. Operational criteria can thus become overshadowed by political criteria, which, in turn, are shaped by national cultures and particularities.

Uncertainties in policy approach also remain unresolved. To fully ensure protection of CIs is virtually impossible. Today's vital systems are too complex, and too vulnerable to a wide array of threats, to build absolute robustness with any confidence. Another approach suggests a complementing focus on resilience, ensuring that inevitable breakdowns will be as short-lived as possible. The EU's current approach, although noble in intention, lacks a broad 'vision' or philosophy on addressing CIP.

Political and institutional uncertainties also remain. National governments appreciate the need for cross-border cooperation on CIP, but remain guarded about how much authority to delegate to the EU. Policy ideas thus come across muddled, emphasizing both national control over the issue and the possibility of binding supranational law. Before technical questions about 'how' to protect CIs can be addressed, basic questions of 'why' and 'who' demand clear answers.

We argued in this article that public rhetoric about supranational CIP should be tempered by a more honest look at the problems and prospects of an EU role. That examination must begin with a critical prerequisite: how the use of the EU as a governance system for developing CIP will shape outcomes. The EU is not simply a forum for intergovernmental coordination. The EU comes with its own set of institutions, political dynamics, and autonomous drivers that shape, and more often than not, constrain policy developments. Coming to terms with these dynamics, and their compatibility with the difficult but crucial task of cooperative CIP, should be a priority for both analysts and policymakers.

Objectively, the arguments for an EU role in CIP seem sound: infrastructures cross borders and breakdowns will most certainly have a transnational effect. Yet our 'knowledge base' of CI vulnerabilities remains low and the role of government authorities still needs to be clarified. For the EU, the problem is even more challenging, since so many political and inter-institutional issues come to the fore. A balanced and fair-minded appraisal of how the EU can add value to European CIP is urgently needed. That, alongside a political consensus around the EU's role in CIP, will help clear barriers to progress.

## Acknowledgements

The authors would like to thank the numerous European Union officials who assisted with research related to this article, as well as the Swedish Emergency Management Agency (Krisberedskapsmyndigheten) for funding the larger program under which this project took place. For more information, see http://www.eucm.leidenuniv.nl.

## Notes

1. For a discussion on transboundary crises, see Rosenthal, Boin and Comfort (2001). See also the special issue of this journal ('t Hart, Heyse and Boin, 2001).
2. http://ec.europa.eu/energy/oil/index_en.htm (accessed 3 July 2006).
3. http://ec.europa.eu/ten/energy/index_en.htm (accessed 3 July 2006).
4. http://europa.eu.int/information_society/eeurope/2005/all_about/security/index_en.htm (accessed 3 July 2006).
5. http://europa.eu.int/information_society/eeurope/2005/all_about/security/index_en.htm (accessed 3 July 2006).
6. http://europa.eu.int/information_society/eeurope/2005/all_about/security/index_en.htm http://www.enisa.eu.int/ (accessed 4 July 2006).
7. http://www.efsa.europa.eu (accessed 5 July 2006).
8. http://europa.eu.int/comm/food/commitees/regulatory/index_en.htm (accessed 29 March 2006).
9. For more information on the Commission's early alert and response systems across the policy spectrum, see Matzén and Svantesson (2005).
10. http://europa.eu/scadplus/leg/en/cha/c11576.htm (accessed 6 July 2006).
11. http://ec.europa.eu/justice_home/fsj/criminal/financial/fsj_criminal_financial_en.htm (accessed 10 July 2006).
12. http://ec.europa.eu/economy_finance/index_en.htm (accessed 6 July 2006).
13. http://ec.europa.eu/ten/transport/guidelines/index_en.htm (accessed 4 July 2006).
14. http://ec.europa.eu/transport/road/policy/index_en.htm (accessed 4 July 2006).
15. http://ec.europa.eu/transport/road/roadsafety/roadinfra/tunnels/index_en.htm (accessed 4 July 2006).
16. http://ec.europa.eu/transport/road/roadsafety/danggoods/index_en.htm (accessed 4 July 2006).
17. http://www.era.europa.eu/ (accessed 4 July 2006).

18. http://ec.europa.eu/transport/air/safety/safety_en.htm (accessed 5 July 2006).
19. http://europa.eu.int/agencies/community_agencies/easa/index_en.htm (accessed 5 July 2006).
20. http://ec.europa.eu/transport/air/safety/doc/2005_11_16/2005_11_16_2005_memo_en.pdf.
21. http://europa.eu/scadplus/treaties/euratom_en.htm (accessed 11 July 2006).
22. http://www.sckcen.be/sckcen_en/activities/train/tcm2003/presentations/S7_5_DeCort_DataExchange_Addendum.pdf (accessed 11 July 2006).
23. The concept of resilience finds its origins in material science and describes the ability of a material to recover its shape after being subjected to strain. In the study of systems, resilience refers to the capacity to absorb shocks while maintaining its function. Resilience here refers to the capability to 'bounce back' after a breakdown.

## References


Andersson, J.J. and Malm, A. (2006), 'Public-Private Partnerships and the Challenge of Critical Infrastructure Protection', in Dunn, M. and Mauer, V. (Eds), *International CIIP Handbook 2006 Vol II*, Center for Security Studies, Zurich, pp. 139–166.

Boin, A., Ekengren, M. and Rhinard, M. (2006), 'Protecting the Union: Analyzing an Emerging Policy Space', *Journal of European Integration*, Volume 28, Number 5, pp. 405–421.

Boin, R.A. and McConnell, A. (2007), 'Preparing for Critical Infrastructure Breakdowns: The Limits of Crisis Management and the Need for Resilience', *Journal of Contingencies and Crisis Management*, Volume 15, Number 1, pp. 50–59.

Clarke, L. (2005), *Worst Cases: Terror and Catastrophe in the Popular Imagination*, University of Chicago Press, Chicago.

Commission (1987), 'Commission Recommendation 87/598/EEC of 8 December 1987 Concerning a European Code of Conduct Relating to Electronic Payments', *Official Journal* L365, 24 December 1987, pp. 0072–0076.

Commission (2000), 'Communication from the Commission on the Health Strategy of the European Community', COM(200)0285 final, Brussels, 16 May 2000.

Commission (2003), 'Proposal for a Directive of the European Parliament and of the Council Concerning Measures to Safeguard Security of Electricity Supply and Infrastructure Investment', COM(2003)740final, Brussels, 10 December 2003.

Commission (2004), 'Communication from the Commission on Critical Infrastructure Protection in the fight against terrorism', COM(2004)702 final, Brussels, 20 October 2004.

Commission (2005a), 'Green Paper on a European Programme for Critical Infrastructure Protection', COM(2005)576 final, Brussels, 17 November 2005.

Commission (2005b) 'Communication from the Commission on Pandemic Influenza Preparedness and Response Planning in the European Community', COM(2005)0607 final, Brussels, 28 November 2005.

Commission (2006a) 'Green paper: A European Strategy for Sustainable, Competitive and Secure Energy', COM(2006) 105 final, Brussels, 8 March 2006.

Commission (2006b) 'The European Programme for Critical Infrastructure Protection (EPCIP)', MEMO/06/477, Brussels, 12 December 2006.

Council (1991), 'Council Directive 91/271/EEC of 21 May 1991 Concerning Urban Waste-water Treatment', *Official Journal*, L135, 30 May 1991, pp. 0040–0052.

Council (1996), 'Council Directive 96/29/Euratom of May 1996 Laying Down the Basic Safety Standards for the Protection of the Health of Workers and the General Public Against the Dangers Arising from Ionizing Radiation', *Official Journal*, L159, 29 June 1996, p. 1.

Council (1998), 'Council Directive 98/83/EC of 3 November 1998 on the Quality of Water Intended for Human Consumption', *Official Journal*, L330, 5 December 1998, pp. 0032–0054.

Council (2004) 'EU Solidarity Program on the consequences of terrorist threats and attacks (revised/widened CBRN Programme', Council Document Number 15480/04 (Internal), 1 December 2004.

de Bruijne, M. and van Eeten, M. (2007), 'Systems That Should Have Failed: Critical Infrastructure Protection in an Institutionally Fragmented Environment', *Journal of Contingencies and Crisis Management*, Volume 15, Number 1.

Duke, S. and Ojanen, H. (2006), 'Bridging Internal and External Security: Lessons from the European Security and Defence Policy', *Journal of European Integration*, 28, 5, pp. 477–494.

Eriksson, P. and Barck-Holst, S. (2005), *Politik för skydd av kritisk infrastruktur i EU och Sverige – en jämförande analys*, FOI-R-1793-SE, FOI – Totalförsvarets Forskningsinstitut, Stockholm.

Executive Order (1996), President of the United States, 'U.S. Executive Order 13010 on Critical Infrastructure Protection 11949', 15 July 1996.

Hix, S. (2005), *The Political System of the European Union*, Palgrave, London.

*Journal of Contingencies and Crisis Management* (1994), Volume 2, Number 4 (special issue).

*Journal of Contingencies and Crisis Management* (1996), Volume 4, Number 2 (special issue).

Jönsson, T. and Jarlsvik, H. (2005), *Krisberedskapsmyndigheten och Europeiska unionen*, FOI-R-1654-SE, FOI – Totalförsvarets Forskningsinstitut, Stockholm.

LaPorte, T.R. (2007), 'Critical Infrastructure in the Face of a Predatory Future: Preparing for Untoward Surprise', *Journal of Contingencies and Crisis Management*, Volume 15, Number 1.

Matzén, N. and Svantesson, M. (2005), 'Annex to Draft Report: An Inventory of Crisis Management Mechanisms, Procedures and Institutions Currently in Place at the EU Level', Research report available at the European Union Crisis Management (EUCM) project website: www.eucm.leidenuniv.nl, first published February, 2005.

Metzger, J. (2004), 'The Concept of Critical Infrastructure Protection', in Bailes, A. and Frommelt, I. (Eds), *Business and Security Public-Private Sector Relationships in a New Security*

*Environment*, Oxford University Press, New York, pp. 197–209.

Parliament and Council (1998), 'Decision No. 2119/98/EC of the European Parliament and of the Council of 24 September 1998 Setting up a Network for Epidemiological Surveillance and Control of Communicable Diseases in the Community', *Official Journal* L268, 3 October 1998, pp. 0001–0007.

Parliament and Council (2001), 'European Parliament and Council Decision 2001/792/EC Euratom of 23 October 2001 Establishing a Community Mechanism to Facilitate Reinforced Co-operation in Civil Protection Assistance', *Official Journal* L297, 15 November 2001, pp. 0007–0011.

Parliament and Council (2002a), 'Regulation (EC) No 178/2002 of the European Parliament and of the Council of 28 January 2002 Laying Down the General Principles and Requirements of Food Law, Establishing the European Food Safety Authority and Laying Down Procedures in Matters of Food Safety', *Official Journal* L031, 1 February 2002, pp. 0001–0024.

Parliament and Council (2002b), 'Regulation (EC) No 1406/2002 of the European Parliament and of the Council of 27 June 2002 Establishing a European Maritime Safety Agency', *Official Journal* L208, 5 August 2002, pp. 0001–0009.

Parliament and Council (2002c), 'Regulation (EC) No 2320/2002 of the European Parliament and of the Council of 16 December 2002 Establishing Common Rules in the Field of Civil Aviation Security', *Official Journal* L355, 30 December 2002, pp. 0001–0022.

Parliament and Council (2004), 'Regulation 2004/851/EC of the European Parliament and of the Council of 21 April 2004 Establishing a European Centre for Disease Prevention and Control', *Official Journal* L142, 30 April 2004, pp. 0001–0011.

Parliament and Council (2006), 'Directive 2006/49/EC of the European Parliament and of the Council of 14 June 2006 on the Capital Adequacy of Investment Firms and Credit Institutions', *Official Journal* L177, 30 June 2006, pp. 0201–0255.

Perrow, C. (1999), *Normal Accidents: Living with High-Risk Technologies*, (2nd Edition), Princeton University Press, Princeton.

Rosenthal, U., Boin, R.A. and Comfort, L.K. (Eds), (2001), *Managing Crises: Threats, Dilemmas, Opportunities*, Charles C. Thomas, Springfield.

Schwartz, P. (2003), *Inevitable Surprises: Thinking Ahead in a Time of Turbulence*, Gotham Books, New York.

Strauss, D. (2006), 'Power Cuts Plunge Europe into Darkness', *Financial Times*, 5 November 2006, www.ft.com, accessed 6 November 2006.

't Hart, P., Heyse, L. and Boin, R.A. (Eds) (2001), 'New Trends in Crisis Management Practice and Crisis Management Research: Setting the Agenda', special issue of the *Journal of Contingencies and Crisis Management*, Volume 9, Number 4, December, pp. 179–245.

Wildavsky, A. (1988), *Searching for Safety*, Transaction, New Brunswick.