EUROPEAN
COMMISSION

Brussels, 28.8.2013
SWD(2013) 318 final

COMMISSION STAFF WORKING DOCUMENT

on a new approach to the European Programme for Critical Infrastructure Protection
Making European Critical Infrastructures more secure

COMMISSION STAFF WORKING DOCUMENT

on a new approach to the European Programme for Critical Infrastructure Protection
Making European Critical Infrastructures more secure

1. CONTEXT AND OBJECTIVES

This document sets out a revised and more practical implementation of the European Programme for Critical Infrastructure Protection (EPCIP).

The new approach to EPCIP builds on a comprehensive review of the 2006 European Programme for Critical Infrastructure Protection[1] and the Council Directive 2008/114/EC[2], conducted in close cooperation with EU Member States and stakeholders.

It provides a stocktaking analysis of the elements of the current programme and proposes a reshaped EU CIP approach, based on the practical implementation of activities under the prevention, preparedness and response work streams.

Critical Infrastructure Protection (CIP) is about ensuring that services vital to the society continue to function. An EU critical infrastructure is an *'asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions*'[3].

By **ensuring a high degree of protection of EU infrastructures** and **increasing their resilience** (against all threats and hazards), we can minimise the consequences of loss of services to society as a whole. These objectives feature predominately in the Stockholm Programme[4] and in the EU Internal Security Strategy[5].

A part of our new approach is looking at the **interdependencies**[6] between critical infrastructures, industry, and state actors. Threats to a single critical infrastructure can have a very significant impact on a broad range of actors in different infrastructures and more widely.

Of course, the effects of those interdependencies are not limited to single countries. Many critical infrastructures have a cross border dimension. In addition to **interdependencies between sectors**, there are also many interdependencies within the same sector but spanning a number of European countries. One such example is the European high-voltage electricity grid, composed of the interconnected national high-voltage electricity grids.

---

1 COM(2006) 786 final

2 Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, Official Journal of the European Union, L345/75.

3 *Idem*, art.2 (a).

4 Conclusions of the European Council of 10/11 December 2009 on 'The Stockholm Programme — An open and secure Europe serving and protecting citizens (2010-2014)'; 17024/09.

5 COM (2010) 673 final. The EU Internal Security Strategy in Action: Five steps toward a more secure Europe. Objective 2: Prevent terrorism and address radicalisation and recruitment. Objective 5: Increase Europe's resilience to crisis and disasters.

6 *'Interdependency: A bidirectional relationship between two infrastructures through which the state of each infrastructure influences or is correlated to the state of the other.'* Steven M. Rinaldi, James P. Peerenboom, Terrence K. Kelly, Identifying, Understanding and Analysing Critical Infrastructure Interdependencies, IEEE Control Systems Magazine, December 2001, p.14.

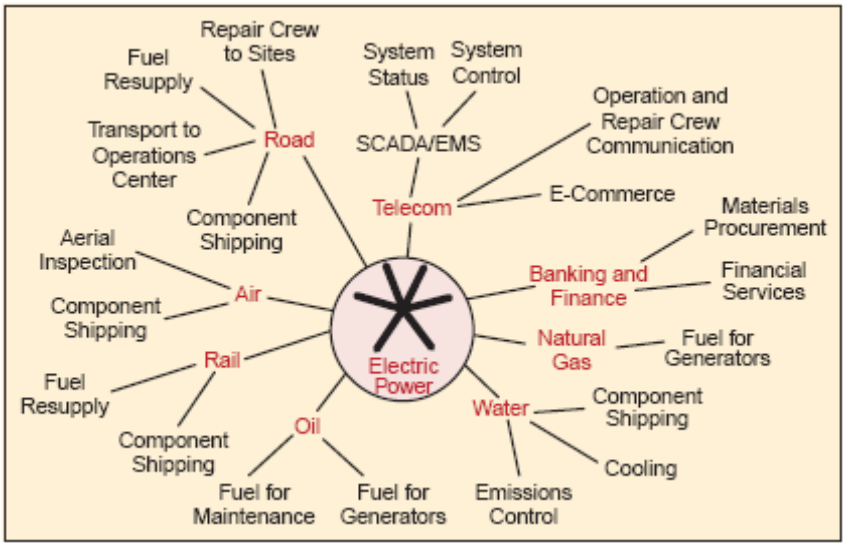

Figure 1[7] - Example of electric power infrastructure dependencies

In this context, we will for instance look at the extent to which that impact is taken into account in current CIP planning, and how consideration of interdependencies can be improved. The review process of the current EPCIP[8], conducted in close cooperation with the Member States and other stakeholders, revealed that there has not been enough consideration of the links between critical infrastructures in different sectors, nor indeed across national boundaries. In order to properly protect our critical infrastructures, and in order to build their resilience, we need a new approach which will tackle this gap. To pilot the new approach, we will start by working with four critical infrastructures of European dimension: Eurocontrol, Galileo, the electricity transmission grid and the gas transmission network (the Four). These were selected on the basis of their pan-European nature and also their own interest in working with the Commission to explore an approach to CI protection and resilience, which takes better account of interdependencies. It is expected that other relevant infrastructures could then benefit from the processes and tools developed when carrying out the work with the Four.

Through work with the Four and developing the new approach, the EU, led by the European Commission, can both play a supporting role for Member States in their own CI protection and resilience work and facilitate better cooperation on CI protection and resilience within the EU. Given that many critical infrastructures are privately owned, better cooperation includes supporting the development of private-public structured dialogues.

2. BUILDING ON THE CURRENT PROGRAMME

In its EPCIP Communication of 12 December 2006, the Commission sets out an overall policy approach and framework for critical infrastructure protection activities in the EU. The new approach proposed here will build upon this framework by focusing on its strengths and addressing the gaps identified in the review process. The four main focus areas of the current EPCIP are:

[7] *Idem.*

[8] Commission Staff Working Document on the Review of the European Programme for Critical Infrastructure Protection (EPCIP), SWD(2012) 190 final

- a procedure for the identification and designation of European critical infrastructures and assessment of the need to improve their protection (addressed in detail in Council Directive 2008/114/EC);
- measures designed to facilitate the implementation of EPCIP, including an Action Plan, the Critical Infrastructure Warning Information Network (CIWIN), the use of CIP expert groups at EU level, a CIP information-sharing process, and the identification and analysis of interdependencies;
- funding for CIP-related measures and projects focussing on 'Prevention, Preparedness and Consequence Management of Terrorism and other Security-Related Risks' for the period 2007-2013; and
- the development of an EPCIP external dimension.

2.1 The European Critical Infrastructures Directive

Council Directive 2008/114/EC[9] calls on Member States to identify and designate European critical infrastructures and assess the need to improve their protection. All Member States have implemented the Directive by establishing a process to identify and designate European critical infrastructures in the energy and transport sectors.

However, less than 20 European critical infrastructures have been designated and consequently very few new Operator Security Plans have been produced. Some clear critical infrastructures of European dimension, such as main energy transmission networks, are not included. Despite having helped foster European cooperation in the CIP process, the Directive has mainly encouraged bilateral engagement of Member States instead of a real European forum for cooperation.

The sector-focused approach of the Directive likewise represents a challenge to a number of Member States, as in practice the analysis of criticalities is not confined to sectoral boundaries and follows rather a 'system' or 'service' approach (e.g. hospitals, financial services).

On the other hand, the majority view of the CIP community is that general CIP awareness and the level of cooperation in the EU have increased through the various activities and fora organised under the Directive, particularly in the energy and transport sectors.

While there are mixed opinions on the improvement of security, it appears that the very existence of a legal instrument has encouraged policies for the protection of national critical infrastructures. This has resulted in concrete actions such as the creation of specific national bodies to deal with CIP policies. In the energy sector, there has been progress in putting in place both risk management and protection measures in cooperation with operators.

All in all, Council Directive 2008/114/EC is considered to be essential by a majority of stakeholders. Furthermore, the economic and political costs of adopting and implementing a new legislative instrument are expected to be high, especially given that only a short time has elapsed since the transposition and implementation of the current Directive. The majority of the CIP community expects that the benefits brought by the current Directive, notably in raising awareness, will continue to increase.

By keeping the current Directive, consolidating the work done so far, and developing a **cross-sectoral approach** to EPCIP (set out in chapter 3), we can address the shortcomings of the current approach without losing the benefits (current and potential) of the current legal

[9] Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, Official Journal of the European Union, L345/75.

framework. Through this approach, we can continue to foster an environment of trust and common goals, as well as allow for flexible targeting of specific areas, countries and sectors in need of improvement.

Operators of critical infrastructures, including those operating in the energy and transport sector, would, moreover, fall under the risk management and incident reporting requirements of the proposed Directive on network and information security[10].

2.2 CIWIN

The 2006 EPCIP Communication called for the creation of a Critical Infrastructure Warning Information Network (CIWIN), an internet-based protected information and communication system for exchanging and discussing CIP-related information, studies and/or good practices among the EU CIP community. CIWIN was moved into the production phase in October 2012 and has been operational since January 2013. In the first months of operation, positive developments were observed, including an increase in usage statistics and the use of the dedicated CIWIN area for national purposes.

It is expected that CIWIN will continue to improve, serving as an important interactive tool for the development of the EU approach outlined here. That role can be filled by CIWIN's performance of several important functions:

- We will use the network to showcase the evolution of selected cases of pan-European critical infrastructures and receive feedback from CIWIN users.
- It aims to provide a toolbox, comprising risk assessment methodologies and the tools necessary to perform a risk analysis (e.g. templates).
- It can become the host platform for several national CIP areas in Member States.
- The network will include all relevant information regarding cooperation with selected third countries, such as the US, Canada and the EFTA countries.

2.3 External dimension of EPCIP

The Council gave the Commission a mandate to further develop the external dimension of EPCIP in its Conclusions of June 2011[11]. The Conclusions invite both the Commission and the Member States to step up their cooperation with third countries, in order to exchange good practices, but also in order to identify critical infrastructures in third countries which could potentially affect them and vice versa.

Member States have expressed the view that the external dimension is of particular importance for CIP. In particular, collaboration with the EFTA countries is considered a priority. To formalise this cooperation with the EEA, the Commission presented a proposal for a Council Decision for the expansion of the applicability of Directive 2008/114/EC to the EEA countries[12], which led to an EEA Joint Committee Decision on the identification and designation of European critical infrastructures[13]. Both Norway and Iceland have recently

---

10 COM(2013)48

11 Council Conclusions of 9-10 June 2011 on the development of the external dimension of the EuropeanProgramme for Critical Infrastructure Protection.

12 Proposal for a Council Decision to the EFTA working party on the position to be taken by the European Union in the EEA Joint Committee concerning an amendment to Protocol 31 to the EEA Agreement, on cooperation in specific fields outside the four freedoms (agreement — doc. 7539/12 EEE 19 AELE 15 PROCIV 40).

13 EEA Joint Committee Decision 101/2012 (identification and designation of European critical infrastructures).

notified the fulfilment of their constitutional requirements for the entry into force of this Decision[14].

The proposed Regulation establishing an Instrument for Stability (IfS)[15] — an external cooperation instrument — allows for assistance to protect critical infrastructure in third countries, in the fields of international transport (aviation and maritime), energy operations and distribution infrastructure, and electronic information and communication networks (cyber security).

Furthermore, to foster strategic partnerships beyond Europe, EU-US and EU-Canada expert meetings have been held yearly, most recently in May 2013. These meetings addressed mainly the need to strengthen cooperation by sharing knowledge, best practices and information on CIP, including the development of a global infrastructure security toolkit. Its purpose would be to promote the exchange of best practices, methodologies, analysis, lessons learned, and other useful materials between the EU, U.S. and Canada. In future meetings, we will focus on selected topics considered of growing importance for CIP in terms of the international dimension, namely: foreign interdependencies; interconnectedness of critical infrastructure; the possibility of global cascading effects; and the interdependence of physical and cyber infrastructure.

2.4 CIP-related projects

At EU level many actions have been undertaken to build knowledge on how to better protect critical infrastructures. We have funded over 100 diverse projects under the Programme **'Prevention, Preparedness and Consequence Management of Terrorism and other Security Related Risks'** (CIPS) during the 2007-2012 period, addressing CIP and crisis management[16]. These projects have a broad scope, covering all sectors, and including analyses of criticalities and dependencies.

The key objective of that set of projects was to provide expert knowledge and a deeper understanding of critical infrastructure at all levels, feeding into policy priorities and providing the scientific basis for such work. Some examples of projects that had cross-sectoral relevance, visibility in the CIP community and delivered good output are:

- Definition of a methodology for the assessment of mutual interdependencies between ICT and electricity generation/transmission infrastructures[17];
- CIP good practices manual for policy makers[18];
- Improving knowledge of effective critical infrastructure protection and facilitating exchange of best practices[19];
- National and European information sharing and alerting system[20];
- Critical ICT infrastructure simulation of interdependency models[21].

---

14 Notifications from Norway (7/12/2012) and Iceland (4/3/2013) of Fulfilment of Constitutional Requirements for Decision 101/2012 - amending Protocol 31 to the EEA Agreement - Council Directive 2008/114/EC.

15 COM(2011) 845 final.

16 CIPS 2007-2012: 111 awarded projects (CIP — 70; Crisis management — 32; Combined — 9). Total awarded amount: 45 million euros.

17 JLS/2007/CIPS/019.

18 JLS/2009/CIPS/AG/C1-036.

19 JLS/2008/CIPS/011.

20 JLS/2008/CIPS/016.

21 JLS/2009/CIPS/AG/C2-42.

One flagship four-year project is ERNCIP (European Reference Network for CIP). Its mission is '*to foster the emergence of innovative, qualified, efficient and competitive security solutions, through networking of European experimental capabilities'*. In order to achieve this goal, ERNCIP maintains a repository of the EU's experimental capabilities; it is developing a network of experts in a variety of CIP-related areas, such as CBRN, explosives detection, cyber security and protection against earthquakes; and it is also contributing to standardisation activities.

Through the FP7 Security Theme more than 40 CIP related projects have been funded so far. Projects have covered all types of critical infrastructure and all types of threats, including cyber threats[22].

Regarding **risk assessment** and **risk management** methodologies, the Commission has also funded numerous projects covering all sectors under the CIPS Programme. These include: the development of a risk assessment methodology to enhance security awareness in air traffic management[23]; the assessment of resilience to threats to control and data management systems of electrical transmission networks[24]; and an interactive risk assessment in the critical infrastructure field based on Earth Observation data and an integrated geographic information system[25].

The studies indicate that risk assessment methodologies for CIP follow either: 1) a sectoral approach, where each sector is treated separately with its own risk methodologies and risk ranking; or 2) a systems approach, where critical infrastructures are treated as an interconnected network. Most work has been sectoral, but these methodologies show their limits when cross-sectoral issues need to be addressed, so a **systems approach** will be encouraged by the Commission from now on.

3. PILOTING A NEW APPROACH TO EPCIP

The first phase is to pilot a more hands-on approach with the four selected critical infrastructures of a European dimension – Eurocontrol, Galileo, the electricity transmission grid and the gas transmission network in order to optimise their protection and resilience.

The Four were selected on the basis of:

- their European nature due to their cross-border dimension. They are cross-border both physically (i.e. the infrastructures are located in the territory of more than one Member State) and at the level of the service provided (i.e. a disruption of service in one Member State can affect several other Member States — a domino effect);
- their representativeness — the selected cases cover the transport, space and energy sectors; and
- their operators/owners' interest to participate in this pilot and to share best practices.

EUROCONTROL[26] is designated as the EU Air Traffic Management (ATM) Network Manager, managing the flow of approximately 30 000 flights per day. The objective, tasks and functions of the Network Manager are regulated by the Commission Regulation (EU) No

22 One major demonstration project with an EU contribution of 25 million Euro is currently under way. Its objective is to develop a set of tools to improve urban transport security through the development of packaged modular solutions validated via demonstrations in large European cities.

23 HOME/2010/CIPS/AG/030.

24 JLS/2008/CIPS/018.

25 HOME/2010/CIPS/AG/037.

26 See Annex I.

677/2011 of 7 July 2011 laying down detailed rules for the implementation of ATM network functions[27].

GALILEO[28] is the European programme for a global satellite navigation system, which is partly owned by the EU and will provide services of vital importance for our citizens and economy.

The **Electricity Transmission Grid**[29] and the **European Gas Transmission Network**[30] are networks without national boundaries, which mean that a failure of one portion of the network could propagate to other areas, potentially involving several countries.

Having identified the importance of taking a systems approach, we now need to look at what we can best do in working with the Four to enable them to take cross-sectoral factors into account in strengthening their critical infrastructure protection work.

The first stage will be to work with the Four to ensure a comprehensive understanding of their CIP measures to date in each of the prevention, preparedness and response work streams, including looking at how interdependencies and cascading effects feed into their CIP planning. We will then work together to identify common factors and consider ways in which their CI protection and resilience measures can be improved.

I. Prevention

We will begin by taking stock of the work done so far in order to provide an update on the progress in security measures and the evolving interdependences with other sectors (ICT, water, etc.). This work will form the basis on which we can build.

We will then work with the Four to set up tools for **risk assessment and risk management,** taking stock of existing research and innovation activities conducted notably in the Environment (including climate change) Theme of FP7. These in particular are related to the Group on Earth Observation (GEO) – such as the Supersites Initiative – and to the development of hazard risk assessment methodologies for low-probability – high-consequences events that could be applied in future "stress tests" for critical infrastructures.

Regarding the ICT sector, the EU Cybersecurity Strategy – An Open, Safe and Secure Cyberspace[31] – identifies actions that will further contribute to the cyber resilience and security of infrastructures covered by EPCIP. The strategy's proposals include coordinated prevention mechanisms, improved preparedness and the involvement of the private sector.

Where appropriate, we will share the knowledge among the Four to identify opportunities to strengthen existing protection plans. We will promote a dialogue between the critical infrastructure operators and the actors upon whom they rely; and foster exchanges of best practices and the development of scenario exercises, guidelines and recommendations. We will look at where tools such as the analyses provided by e.g. the EU Intelligence Analysis Centre (INTCEN) and the development of a methodology for stress tests could play a role in improving the effectiveness of existing measures. We will also work with the Four to consider

27 Commission Regulation (EU) No 677/2011 of 7 July 2011 laying down detailed rules for the implementation of air traffic management (ATM) network functions and amending Regulation (EU) No 691/2010, Official Journal of the European Union, L 185/1.

28 See Annex II.

29 See Annex III.

30 See Annex IV.

31 JOIN (2013) 1.

whether there might usefully be better links with the risk assessment and management activities undertaken within the Union Civil Protection Mechanism[32].

For all the above activities, the Commission will play a supporting and facilitating role, developing guidelines, methodological tools, and other support tools to contribute to the overall assessment of dependencies and criticalities.

II. Preparedness

We will then support the development of preparedness strategies based around contingency planning, stress tests, awareness raising, training, joint courses, exercises and staff exchange. The establishment of such structures can also be supported by promoting incident reporting, which can be encouraged as a means to improve the level of knowledge on the performance of critical infrastructures during a disruptive event (e.g. the extent of cascading effects, overall impact, etc.). We will work with the Four to further develop a picture of what is useful at European level.

We will also promote and facilitate dialogue between the operators of the critical infrastructures and those who rely upon them. The aim is to increase **consideration by the Member States and other actors reliant upon critical infrastructures of how they can prepare in response to events affecting European critical infrastructures.** Member States and other actors could share, on a voluntary basis, information on incidents in relation to the Four which could affect them. By getting this dialogue going, we can further improve the overall preparedness level.

Furthermore, we will explore the possibility of linking the civil protection training network, envisaged in the proposal for a new Union Civil Protection Mechanism, with relevant critical infrastructure training activities. In addition, joint exercises with the relevant sectors or with the Civil Protection Mechanism may highlight the complementarity of EU preparedness measures.

III. Response

Having facilitated dialogue on preparedness, the Commission can then help identified actors think about their response to events. We aim to strengthen the links between the critical infrastructure community and early warning systems, as early warning tools for natural disasters can point to potential threats to critical infrastructures. We also want to get people thinking about the mechanisms for on-going communication between the Four and other actors reliant upon them until functionality is restored.

Given that the current Union Civil Protection mechanism only focuses on the immediate response to an incident, we will explore how the mechanism could further promote the use of recovery specialists to help with the **long-term recovery of critical services,** to be deployed at the request of Member States. We will work with the Four on whether establishing specific CIP modules within the mechanism, or possibly including the required CIP expertise in existing modules, would add value to civil infrastructure protection.

4. WAY AHEAD

The Commission will continue to develop the protection and resilience measures already in place, looking to improve their utility. In addition, the new approach looks to increase the

[32] 2007/779/EC, Euratom: Council Decision of 8 November 2007 establishing a Community Civil Protection Mechanism (recast).

dialogue between critical infrastructures and all those actors across Europe who would be impacted by any event affecting functionality. We will do so under the prevention, preparedness and response framework, having identified relevant pan-European critical infrastructures. The Commission's role remains one of facilitating and supporting the work of critical infrastructures, Member States, and industry and providing services which those actors can use to improve CIP across Europe.

It is also important that, in parallel with this new approach, Member States and the private sector continue their efforts of identifying European Critical Infrastructures – building on their work so far and on the results of the projects already pursued. CIWIN will continue to be a support tool in this process.

In terms of the new approach, the pilot phase will start immediately, establishing a roadmap, setting out the aims to be completed by the second half of 2014, after which time the Commission will report back on progress and the way ahead. It is led by DG HOME with the scientific support of the Joint Research Centre, in conjunction with the four selected critical infrastructures and associated Directorates-General (i.e. DG MOVE, DG ENTR, DG RTD, DG ENER and DG ECHO).

Member States and other stakeholders (such as operators' associations), will be invited to have an active role in all stages of the pilot phase. Their technical input would be of great value in its successful completion. The benefits will be three-fold: an increased understanding of how actors in the Member States (both public and private sector) rely on the Four; greater access to the tools and best practice identified by the Commission during this process; and the opportunity to contribute to the discussion on how the critical infrastructures can best benefit from European Union structures to improve their protection going forward after the pilot.

This approach gives us the opportunity to make CIP planning in Europe more cohesive. By talking to some of Europe’s leading critical infrastructures about what they do well and how they could learn from each other, we can help ensure that each has an optimum CIP plan. By getting sectors to talk to each other, and involving Member States in the dialogue, we can disseminate their best practice and help to use it with other critical infrastructures in Europe. And by exploring the possibility of involving EU structures, we can improve the ability to respond to an event.

Following the pilot phase, we anticipate that it could lead in the following directions:

- The application of the work streams in these four pan-European critical infrastructures should provide the necessary indicators to allow for the shaping of an **EU approach towards CIP**. It would be based on the results achieved and the gaps identified through working with the Four, and seek to provide useful tools for improving protection and resilience, including through providing for **strengthened risk mitigation, preparedness and response measures**.
- The following step could be to **implement this approach** in **regions** where Member States are interested in cooperating with each other. Examples could potentially include a resilience concept for the overall critical transport infrastructure around the Baltic Sea, and a programme for supply chain criticalities in the Danube region.
- The reshaped programme should also be aligned with the time frame for the new MFF 2014-2020 (of relevance here, Internal Security Fund — Police) and emphasise the strategic role of the **funds available** for the implementation of activities at all levels, clearly linking them with the key priorities described here. Instead of funding a large number of diverse projects, a few large cross-border strategic projects could be launched to implement the agreed EU tools and methodologies.

- The EU will play a **facilitating role** in this context, fostering CIP policy developments and increased cooperation among the CIP community, as well as allocating funding to support the key policy objectives outlined in this document.

The new EU approach could thus encourage and nurture the development of CIP at all levels, from local and national to European and international, making the EU more secure and better prepared for threats to its critical infrastructures, and improving overall resilience if disruptions do occur.

ANNEXES: SELECTED PAN-EUROPEAN CRITICAL INFRASTRUCTURES

Annex I. EUROCONTROL

In the context of the development and functioning of the Single European Sky, the EUROCONTROL agency has been designated as the *Network Manager for the EU ATM network*. This has implied the creation of cooperative arrangements for consultation and decision-making with all the actors involved in air traffic operations (e.g. national air traffic service providers, airspace users, airports, competent national authorities and military at both authority and service provision level). An important operational activity of the Network Manager is the coordination of Air Traffic Flow Management with the Air Traffic Control organisations in Europe.

Related to this, one of the tasks of the Network Manager is to provide support for network crisis management: a European Aviation Crisis Coordination Cell (EACCC), involving permanent representatives of all the ATM stakeholders and of various EU institutions as well as focal points in the corresponding structures in the Member States, has been formally set up to mitigate potential network crises. It is used to meet on a regular basis, to simulate possible scenarios adversely affecting aviation and which could be declared as network crisis events and to organise ad hoc events with its focal points in the Member States. The Network Manager, in conjunction with the EACCC members, is responsible for activating and deactivating the EACCC, coordinating the management of response to network crisis, monitoring the implementation of the contingency plans and proposing procedures if no contingency plans exist.

The operation of EUROCONTROL as a Network Manager and the EACCC could be one of the subjects for a large-scale case study, conducted by HOME in association with other services concerned, aiming at identifying best practices in applying measures under the prevention-preparedness and response work streams mentioned above, and leading to the development of risk mitigation strategies, etc. which could contribute to better protect also other critical infrastructures and sectors.

Its complex infrastructure, subject to several threat scenarios, including cyber threats, where a disruption of its services could have a significant impact on the European economy, and the interdependencies among the various subsystems leading to various cascading effects, also makes this an interesting case to study.

Some recent crisis situations have also fully justified the need for the EACCC, and drawing lessons from that work would be useful. It includes:

- the 9/11 2001 attacks, when, from the moment EUROCONTROL received the information that US airspace was closed, it took only a few minutes to alert all European aircraft operators and airports to prevent flights bound to the US from departing;

- the volcanic ash cloud crisis, from 15 to 21 April 2010, led to the cancellation of 100 000 flights in Europe (54 % of all flights), with an impact on the world economy of approximately € 3 billion. It is estimated that ten million passengers were stranded at airports for a period of six days. EUROCONTROL played a key role in communication, information sharing and awareness; and

- the heavy snow in December 2010, when thousands of flights were cancelled across Europe, many others delayed and thousands of passengers were stranded at airports for several days.

(The proposed study should not affect the regulatory framework governing the ATM Network Manager, nor tasks, tools or processes already in place).

Annex II. GALILEO

Space-based systems enable a wide spectrum of applications, which play a fundamental role in our everyday life, are critical to key areas of the economy, and help ensuring our security. With increasing dependence on space-based services, the ability to protect space infrastructure has become essential to our society.

Any shutdown of even a part of space infrastructures could have significant consequences for the well-functioning of economic activities and our citizens' safety and security, and would impair the provision of emergency services. This is particularly true for Galileo – the European Global Navigation Satellite Systems (GNSS) – which is the first EU owned Space Infrastructure. A major failure, whether accidental or intentional, of such GNSS infrastructure will impact the users but also affect many other critical infrastructures in which GNSS services are already deeply integrated: Transport, telecommunications, trade and banking activities rely on GNSS signals for timing, navigation and secure transactions.

Galileo, like other space infrastructures, faces specific threats to the signals and to the satellites. GNSS signals can be subject to a number of threats on the radiofrequency links such as interference, unauthorised access and misuse, jamming, falsification and cyber-attacks. The Galileo system has undergone specific security processes to mitigate the risks induced. In addition, one of the services of Galileo, the Public Regulated Service (PRS) has been specifically developed to support EU Member States and government-authorised users, for sensitive applications that require effective access control and an unlimited and uninterrupted service worldwide.

Furthermore, the increasing number of space debris has become a serious threat to the sustainability of space activities including the operations of the Galileo satellite constellation, the Copernicus space segment or contributing national public and commercial satellites. In order to mitigate the risk of collision it is necessary to identify and monitor satellites and space debris, catalogue their positions, and track their movements (trajectory) when a potential risk of collision has been identified, so that satellite operators can be alerted to move their satellites. This activity is known as space surveillance and tracking (SST), and is today mostly based on ground-based sensors such as telescopes and radars. At present there is no SST capability at European level; satellite and launch operators are dependent on US data for anti-collision alerts. The Commission has put forward a proposal for an EU space surveillance and tracking (SST) support programme. The aim of the programme is to support Member States' to cooperate and network their SST capacities and provide anti-collision alert services at European level.

Annex III. The European Electricity Transmission Grid

As the wide-area black-outs of past years have shown, a single incident affecting one significant element of the grid can affect supply on the whole continent. Threats (man-made) also have similar aims and modus operandi across country borders, while single attackers or coordinated action may target networks on a regional, European or international scale, as is the case with cyber-attacks.

An extensive power disruption occurred in the north German transmission grid on 4 November 2006, and was felt over most of the continent, including Austria, Belgium, France, Slovenia and Spain, in addition to Germany. Although the action taken by the transmission system operators (TSOs) prevented the blackout, this case is considered among the most severe and largest disturbances ever in Europe. The effects were important in terms of power cuts at industrial and domestic level (more than 15 million households), while electricity-dependent services such as transport were affected (for example hundreds of trains were cancelled or delayed).

This calls for a coordinated protection mechanism, involving all operators and their sectoral bodies. The risks associated with the above threats can only be properly tackled by response at system level, as the integrity and functionality of the whole system is affected. The sector (ENTSO-E in particular) has already invested in CIP measures and has expressed strong support for an EU approach that would also tie in with the requirements of the internal market regulations. The Network Codes offer a sensible framework to foster the incorporation of common protection methodologies for the European grid operators. The Commission could support this process over the coming years with the CIP tools and methods to be provided.

Furthermore, the evolution towards Smart Grids calls for enhanced synergies between the information and communications technology (ICT) sector and the energy sector. More than ever, industry and investors are concerned by cyber-security threats. The Commission has therefore initiated action under the Smart Grids Task Force, where stakeholders from the energy and ICT sectors are currently developing a cyber-security assessment framework. This framework includes the evaluation of available methodologies for a trustworthy network, sharing the vulnerability and threat analyses for smart grid and smart metering systems as well as the identification of best available techniques for smart metering systems.

Annex IV. The European Gas Transmission Network

The physical threats (ranging from terrorism to boycotts and strikes), disruptive natural events (earthquakes, floods, very cold periods, big storms) and commercial disputes to which this network is subject make it vulnerable and jeopardises Europe's secure access to gas.

An illustrative example of the effects of a disruption of the gas network is the Brotherhood pipeline case of 2009. This pipeline, which transports almost 300 million cubic metres of Russian gas every day to Europe, passing through Ukraine, started reducing its flow in early January, leading to a complete shutdown. Its disruption had a significant impact on many Member States, in particular those that depend exclusively on this supply route, leaving homes without gas for heating and forcing production stops in some industries. Gas supplies were only fully restored on 21 January 2009. This disruption was the most serious of its kind in Europe in recent history: for an unprecedented period of two weeks, Europe was cut off from 30 % of its total gas imports, an equivalent of 20 % of its gas supplies.

The need for coordination at European level is therefore clear, and is recognised by Gas Infrastructure Europe (GIE), representing European operators in the sector. GIE has expressed its support for the EPCIP programme and suggested the development of a common methodology for risk/threat assessment in Europe for gas sector infrastructures, taking an all-hazard approach. This would be in line with the prevention and response coordination implemented in the gas sector under Regulation 994/2010, in particular the preparation of the national risk assessment and the preventive action and emergency plans to be developed on the basis of the risk assessments.

Annex V. Roadmap

Action 1 – Design of an EU approach for the protection and increased resilience of European Critical Infrastructure	***Actor***	***Timeframe***
Detailed assessment and analysis of processes and methodologies used in the selected cases.	DG HOME (lead), JRC (support) and selected stakeholders	Starting in the second half of 2013
Agree on the criticalities and interdependencies of the selected cases. Agree on concepts, definitions and a methodology for CI risk assessment and risk management.	DG HOME (lead), JRC (support) and selected stakeholders	Starting in the second half of 2013
Agree on preparedness measures, such as contingency planning, stress tests, awareness raising, training programmes, joint courses, exercises and/or staff exchanges.	DG HOME (lead), JRC (support) and selected stakeholders	Starting in the second half of 2013
Explore the possibilities for the establishment of teams of EU recovery specialists, in case of major CI, to help with long-term recovery of critical services and to be deployed at request of Member States.	DG HOME and DG ECHO	Starting in the second half of 2013
Assess of the achieved results and identified gaps.	DG HOME (lead) and JRC (support)	First half of 2014
Discuss and validate of the EU approach by Member States and stakeholders.	DG HOME, Member States and CI operators	First half of 2014
Action 2 - Broadening the implementation of the EU approach	***Actor***	***Timeframe***
Identify and select other possible pan-European infrastructures for the implementation of the developed approach.	DG HOME, Member States and CI operators	Second half of 2014

Implement on the selected pan-European critical infrastructures. Continued mutualisation and dissemination of the selected approach to regions, with projects covering Euro-regions or involving a group of Member States.	DG HOME (lead), JRC (support), CI operators and Member States.	Second half of 2014
Link the funds under the ISF to the implementation of the developed EU approach.	Commission	As from 2014