CIVIL DIMENSION OF SECURITY

162 CDS 07 E rev 1
Original: English

NATO Parliamentary Assembly

THE PROTECTION OF CRITICAL INFRASTRUCTURES

SPECIAL REPORT

LORD JOPLING (UNITED KINGDOM)
SPECIAL RAPPORTEUR

International Secretariat

7 October 2007

TABLE OF CONTENTS

1. Ensuring the continuous provision of essential services to the population is a core state responsibility. In this sense, concerns relating to the protection of critical infrastructures are not new. The terrorist attacks of 11 September 2001 in the United States, however, have given both a new meaning and a new dimension to the concept of Critical Infrastructure Protection (CIP). Terrorist attacks on the subway system and the railway in London and Madrid have only confirmed the urgency of an in-depth review of existing policies. Additionally, hurricane Katrina in the United States and the tsunami in South-East Asia have demonstrated that natural disasters can also have devastating consequences on infrastructure. Finally, NATO countries are vulnerable to the impact of political decisions, which could seriously disrupt infrastructure, particularly in the energy sector. Although this aspect will not be dealt with in this report, which will focus on the threat posed by terrorism and natural disasters, it certainly belongs in a broader discussion on critical infrastructures.

2. This new awareness of threats appears as critical infrastructures themselves face new realities. The process of globalisation has led to a growing interdependence and interconnection of markets and networks in a number of essential sectors such as energy, information and communications, food, transport, which increases the vulnerability of infrastructure in each of these sectors. Additionally, the wave of privatisation and liberalisation in many of these sectors has eroded the dominant role previously played by public authorities. Most critical infrastructures are today owned and operated by private sector businesses, which therefore bear the primary responsibility for protecting their infrastructure. This situation raises difficult questions regarding the relative roles of governments and private sector stakeholders in the CIP architecture, and the compatibility of national security objectives with business interests.

3. European and North American countries have had to adapt to these new threats and realities. A number of governments had already taken initial steps in the mid 90s or even earlier, but for all of them 9/11 was a major wake-up call. Many countries are far from completing a comprehensive review of their CIP policies and many issues remain unresolved.

4. It is important to clarify at this point that CIP is not an isolated policy area. CIP fits in the broader framework of counter-terrorism and civil protection policies. These policies aim broadly at building civic resilience in the face of threats posed by natural disasters, technological incidents and terrorist attacks and generally rely on a multi-layered strategy, which includes prevention of terrorist threats; protection of people and infrastructure against the threats posed by natural disasters, technological incidents and terrorist attacks; preparedness and consequence management; response and recovery. In this framework, CIP thus contributes to the second objective, that of protecting the people and infrastructure.

5. CIP policies also increasingly include an external dimension, as individual countries have come to realise that the global nature of the challenge and the growing interdependence of their infrastructure requires co-operative solutions. Various regional and international organisations promote CIP co-operation. NATO and the European Union have until recently played a relatively minor role, but have both stepped up their efforts in recent years.

6. This report will start with an overview of the basics of CIP, presenting the concepts, objectives and methodology underlying CIP efforts; in other words, what are we protecting, why and how. The second chapter will identify some of the main entities responsible for CIP at the national and international levels, and examine interactions between them. The third chapter will present case studies of measures taken to protect critical infrastructures in four major sectors. Additional information on some of these issues is also available in the Secretariat report of the Committee’s visit to Belgium in January-February 2007 [024 CDS 07 E].

I. PROTECTING CRITICAL INFRASTRUCTURES: WHAT, WHY AND HOW?

7. A quick look at the policies adopted by various national and international actors shows that CIP requires a number of successive steps: first, define what is considered as critical infrastructure; second, identify those infrastructures that fit the definition; third, assess the risk that those infrastructures face and identify security gaps; finally, define and implement appropriate protection measures to reduce this risk. The first section will look at the way European and North American nations are defining critical infrastructures; the second section will examine issues relating to the adoption and implementation of protection measures.

A. DEFINING AND IDENTIFYING CRITICAL INFRASTRUCTURES

8. Defining critical infrastructure is the logical first step towards protecting it and therefore the definition that is used by a country is often a reflection of that nation's priorities. Although there is no universally agreed definition, critical infrastructure is generally understood as those facilities and services that are vital to the basic operations of a given society, or those without which the functioning of a given society would be greatly impaired.

9. In most countries, this definition has evolved over the years to include an ever-broader range of infrastructures. Critical infrastructure has come to include not only facilities as such, but also services, such as government services, emergency services, etc. "Cyber-infrastructure" is also widely considered a critical infrastructure, along with physical assets, and its protection has in some cases preceded that of physical infrastructure. Critical infrastructures also have been identified in a growing number of sectors, from traditional areas such as defence, transport and energy, to areas such as banking and finance, health care, and IT, which have been labelled critical more recently. Additionally, the criticality of an infrastructure has come to cover not only its "systemic" importance, i.e. its centrality to the operations of society, but also sometimes its symbolic importance as a national icon.

10. National definitions differ slightly in the criteria used to define the criticality of an infrastructure. Most countries and institutions use crosscutting criteria, which cover all infrastructures in all sectors. Sectoral criteria are then used to refine this definition for each specific sector. In some countries, those criteria stress the finality or purpose of the infrastructure (i.e. the infrastructure is critical because it performs a function that is vital to society), whereas in others they stress the severity or effects of the disruption or destruction of a given infrastructure on society (i.e. the infrastructure is critical because its loss would be extremely disruptive). The latter approach is more widespread, but the former is preferred in some countries, such as France. Below are some examples of the definitions used in a number of countries.

11. **Germany**: critical infrastructure are those "facilities and organisations of major importance to the community whose failure or impairment would cause a sustained shortage of supplies, significant disruptions to public order or other dramatic consequences" (source: KRITIS Task Force of the Ministry of Interior).

12. **United States**: critical infrastructure are those "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters" (source: USA PATRIOT Act). Later documents, including the 2006 National Infrastructure Protection Program (NIPP), add "networks" and "functions" as other elements of the critical infrastructure, along "systems and assets".

13. **United Kingdom**: the Critical National Infrastructure comprises “those assets, services and systems that support the economic, political and social life of the United Kingdom whose importance is such that loss could:

- cause large-scale loss of life;
- have a serious impact on the national economy;
- have other grave social consequences for the community;
- or be of immediate concern to the national government.”

(source: Home Office website).

14. **France**: critical infrastructure are “those activities that are indispensable to the public's essential needs and the maintenance of the security and defence capabilities of the country: food, water, energy, transport, financial institutions, information and communications systems, and command and decision centres” (source: Governmental White Paper on Domestic Security in the Face of Terrorism).

15. The sectors covered by these definitions differ from country to country, but generally include:

- transportation systems (air, rail, road, sea);
- energy production and shipping;
- government facilities and services, including, in particular, defence, law enforcement and emergency services ;
- information and communication technology;
- food and water;
- public health and health care;
- financial institutions.

Nevertheless, it has to be noted that some European countries, including Austria and Sweden, have no official list of CIP sectors.

16. Once a proper definition has been agreed, it is generally used to identify those infrastructures in a given area that fit the definition and establish an inventory of critical facilities. Because definitions of the type cited above are often very broad, the process of identification is particularly important. It raises a number of major challenges. First is the development of a common or harmonised methodology, which public authorities and owners or operators of infrastructure can use to identify elements of the national infrastructure, which fit the definition. Another challenge is to distinguish specifically those elements of the infrastructure that are critical nationally, as opposed to infrastructure that might be critical at a local or regional level, but do not require central intervention. This process further raises a serious issue relating to the protection of the information thus collected, which often includes not only a list of critical infrastructures, but also sensitive security information. This list also needs to be regularly updated.

B. PROTECTING CRITICAL INFRASTRUCTURE

17. National and international CIP strategies recognise that it is impossible to protect critical infrastructure fully against all types of threats. In this sense, CIP is a risk management exercise. Its main goal is to reduce the risk to critical infrastructure to an acceptable level. Most CIP strategies follow a similar methodology. A first phase aims to assess risk to the critical infrastructure. Protection measures are then designed in order to reduce this risk. The paragraphs below will examine these successive steps in an abstract manner. The issue of who is responsible for these various phases is examined in the following chapter.

Assessing the risk to critical infrastructures

18. Risk is generally defined as a factor of the likelihood of a threat to the infrastructure, of vulnerability of this infrastructure, and of the expected consequences or impact on the

infrastructure should that threat materialise. Assessing the risk to an infrastructure thus requires a proper analysis of these three elements. The order in which those analyses are done varies from country to country.

19. CIP authorities need to identify the threats posed to their critical infrastructure, decide which of these threats need to be addressed and how likely they are to occur.

20. Following the terrorists attacks of 11 September 2001, protection of the critical infrastructure against terrorism has received priority attention in the United States although policy documents continued to refer to an all-hazards approach, i.e. encompassing natural disasters, technological incidents and terrorist or criminal acts. However, the devastation caused by Hurricane Katrina, which damaged much of the infrastructure of the Gulf Coast region, including key energy assets, prompted federal authorities to re-focus certain policies. European countries generally use an all-hazard approach, as does the European Union. However, in many of these European countries – including France and the United Kingdom, protection against the threat of terrorism is given priority.

21. National intelligence or law enforcement authorities generally produce regular nationwide threat assessments, which often translate into a threat level indicator (a scale of the threat to the nation, which is generally made public and regularly updated). Threat assessments at the infrastructure level take into account these nationwide assessments to evaluate threats to a specific infrastructure. This process however presupposes that proper and secure mechanisms are in place for sharing information about the threats among CIP stakeholders.

22. Another step in this phase is assessing the vulnerability of critical infrastructures, i.e. identifying where their weaknesses lie. These weaknesses can affect the physical components of an infrastructure (buildings, facilities, etc.); its human components (staff, visitors, etc.); or its IT components. A vulnerability assessment can be general or based on specific threat scenarios. It can be conducted by the infrastructure owner or operator, or by an outsider. This process thus raises a number of questions: who is responsible for vulnerability assessments; is there a harmonised methodology; are there common standards; are there mechanisms in place to oversee implementation of this methodology or these standards?

23. A third pillar of risk assessment aims to identify the potential consequences on an infrastructure should a specific threat materialise. This step raises questions as to which consequences are taken into account and whether all consequences – on human life, the economy, the environment, public morale, etc – should be considered on an equal basis or some given higher priority over others. An important issue is that of intra-sector and cross-sector dependencies, i.e. the impact on an infrastructure / on a sector of a disruption in another infrastructure / sector. For instance, a major cyber-attack will not only affect the information infrastructure, but also all government services and private sector operators that are dependent on information networks for their communications. However interdependencies are still very poorly understood and relevant information is not always easily available. Many national and international CIP policies are only beginning to consider this issue.

24. The combination of information about threat, vulnerability and consequence provides an assessment of the risk to a specific infrastructure. Taking into account existing protective measures, it helps identify security gaps, which will need to be addressed through specific protection measures.

Reducing the risk to critical infrastructure

25. CIP stakeholders can use a broad range of protective measures to reduce the risk to their infrastructure. Protection measures aim primarily at addressing vulnerabilities identified in the

previous phase. However, protection can also aim at mitigating the impact of an event should it occur. In the case of a nuclear power plant, reducing the vulnerability of the plant to a terrorist attack means for instance reinforcing access control for personnel; mitigating the impact of an attack is achieved in particular through the various protective layers around the reactor. Better protecting critical infrastructures is also expected to deter the threat whenever possible.

26. Some protection measures are generic and can be used for almost all types of infrastructures. However, in many cases, the choice of protective measures also depends on the type of infrastructure. Thus, for instance, certain sectors depend heavily on fixed infrastructures (e.g. transport, energy), whereas others rely on networked infrastructures (e.g. information and communication). In the former case, protection is likely to focus on hardening these fixed infrastructures, whereas in the latter, such an approach makes little sense and protection measures will aim at ensuring that the network is able to continue to perform its function.

27. Protection measures can be classified in four broad categories, depending on what aspect of the infrastructure they target: physical protection measures – which target the physical components of an infrastructure; electronic or cyber-protection measures – which aim to protect the ICT infrastructure against attacks; human or personnel protection measures – which target the infrastructure's staff and other categories of people bearing some direct relation to the infrastructure; and organisational measures – which relate to the way the infrastructure is managed. To use the example above, hardening the containment structure of a reactor is an example of a physical protection measure, while enhanced access controls are examples of a human protection measure.

28. Finally, protection measures can be permanent / long-term or they can be flexible, i.e. be gradually implemented according to varying risk and threat levels. This points to the fact that the CIP strategy should organise a review process to ensure the ongoing adaptation of protection measures to meet evolving threats and vulnerabilities and benefit from advances in protection techniques and technologies.

29. In the process of elaboration of a CIP strategy, a number of issues and challenges need to be tackled. A first issue relates to information on CIP measures. Obviously, CIP is a very sensitive area, and it is therefore important that a high level of confidentiality be ensured regarding the most critical elements of the strategy, including the inventory of critical infrastructures. While sharing of information between CIP stakeholders – from private sector to public sector and vice versa – is crucial, it is often a very delicate issue. Therefore, efficient information sharing will only happen if appropriate rules ensure that information is shared strictly on a need-to-know basis and in a fully secure mode.

30. A second crucial issue is the need to prioritise among possible protection measures. As mentioned above, comprehensive all-hazards protection of all critical infrastructures is almost always impossible, not only for technical reasons, but also because of other limitations, in particular the high costs of CIP. For instance, in the United States, the federal government alone has spent US$18 billion a year on CIP in 2005 and 2006, and should spend a similar amount in 2007. Because of the high costs of protection, cost-effectiveness is often a necessity. Priority will thus be given to those measures that provide the greatest mitigation of risk for any given investment. However, prioritisation can also be achieved in other ways, focusing on the type of threat, on those consequences that are considered most unacceptable, on a specific type of infrastructure, on the criticality of an asset compared to another one, etc. Cost-effectiveness will most likely drive decisions made by private CIP stakeholders. Other criteria are of a more political nature and would require intervention by public authorities to influence private decision-making.

31. Finally, a third generic issue regarding CIP is one of responsibility. Who should be responsible for each of the steps described above? Is state intervention necessary and to what

degree? How does this fit with risk management decisions taken by private CIP stakeholders? The following chapter will specifically address these issues and examine further national case studies.

II. PROTECTING CRITICAL INFRASTRUCTURES: WHOSE RESPONSIBILITY?

32. CIP involves several stakeholders: public authorities – at the national and local levels, including various public agencies; critical infrastructure operators, which are often private sector firms; and the population at large. CIP has also increasingly gained an international dimension, which raises the question of international co-operation on CIP.

A. NATIONAL CIP STAKEHOLDERS

33. CIP is first and foremost a national responsibility. Protecting those primary functions that ensure the basic functioning of government and society is a central responsibility for any state. However, in many NATO countries, entire sectors of the national infrastructure have been privatised. As a result, most critical infrastructures are today owned and operated by private sector businesses, which therefore bear the primary responsibility for protecting their infrastructure. Owners or operators of infrastructure routinely perform risk assessments and develop risk management strategies to protect their infrastructure. Meanwhile, however, indications that infrastructures have become prime targets for terrorists, coupled with an increasing awareness of the potentially devastating consequences of natural disasters, have put governments under increasing pressure to review existing policies for the protection of populations and critical infrastructures. In many cases, this has meant greater emphasis put on the coordination of CIP-related efforts.

34. A first priority is intra-government co-ordination. As the case studies below will show, CIP often involves several departments within the central administration. In the case of decentralised or federal state, it can also fall within the responsibility of local or regional authorities. The division of labour between these various levels of administration can thus be a challenge. A second and somewhat more complicated challenge relates to co-ordination between public authorities and CIP owners and operators.

Promoting public-private synergy

35. The distribution of tasks between public and private CIP stakeholders varies considerably from one country to another. One major dividing line is between, on the one side, those states which emphasise the primary responsibility of public authorities and state regulation, and, on the other side, those where infrastructure operators play a central role. In reality, this distinction is more subtle. All states recognise the need for public-private partnership, but organise this partnership in different ways. An overview of some national policies will provide a few examples of the variety of national solutions.

36. In the **United States**, the Department of Homeland Security (DHS) plays the leading role in managing the overall national effort to protect critical infrastructure. It oversees the implementation of the national CIP strategy. This strategy relies on a sector-based approach. In each sector, a “lead agency” within the federal government is responsible for co-ordinating the efforts by federal, state, and local governments and the private sector to protect that sector’s infrastructure. The DHS itself acts as the lead agency for several sectors.

37. Private sector owners and operators of critical infrastructure are responsible for undertaking protection, restoration, co-ordination and co-operation activities, and for providing advice, recommendations, and subject matter expertise to the federal government. Public-private

partnership is essential since it is estimated that over 85% of what can be classified as critical infrastructure in the United States is owned and operated by the private sector.

38. A series of structures allows for co-ordination and planning within one sector and across sectors. In each sector, Sector Co-ordinating Councils bring together private sector representatives, and Government Co-ordinating Councils bring together representatives from all levels of government involved in that specific sector. A Partnership for Critical Infrastructure Security deals with cross-sector issues among private industry, and a Government Cross-Sector Council with government cross-sector review.

39. The **United Kingdom** follows a fairly similar model. The Home Office is the lead authority for the protection of critical national infrastructure. As part of the current process of reform and re-organisation of the Home Office, responsibilities for CIP were included in the mandate of the newly created Office for Security and Counter-Terrorism. Other government departments have lead responsibility for identifying critical infrastructure within their sectors and ensuring appropriate steps are taken to improve protective security.

40. Additionally, a Centre for the Protection of National Infrastructure (CPNI) was formed in February 2007 from the merger of two other government services. CPNI, which is accountable to the Director General of the Security Service (MI5), is responsible for providing security advice for all organisations across the national infrastructure, including businesses and government departments. Co-ordination between all government stakeholders is done through reporting arrangements to one Ministerial Committee chaired by the Home Secretary. The future Counter-Terrorism Bill, scheduled to be presented at the end of 2007, is expected to modify these structure and arrangements slightly, by including additional powers in terms of protective security.

41. In **Germany**, it is estimated that over 90% of critical infrastructure is managed by private operators. The German CIP architecture is little centralised and puts emphasis on the role of infrastructure operators. The main institution responsible for co-ordinating CIP policies at the federal level is the Centre for the Protection of Critical Infrastructure within the Federal Office for Civil Protection and Disaster Response (Federal Ministry of Interior). The Centre is a focal point for promoting information and awareness of CIP issues, public-private co-ordination and co-operation, analysis and protection concepts, and protection measures.

42. The Centre released in 2005 a framework policy document on CIP in Germany – the Baseline Protection Concept, which aims to provide guidelines for infrastructure operators to develop protection measures. Recommendations focus both on the methodology for adopting protection measures and on minimum protection requirements. A questionnaire and a checklist are provided to assist private sector operators in completing or upgrading their infrastructure protection plans.

43. The Baseline Protection Concept lists a number of public authorities at the federal, state and local level, which can or should be consulted in the implementation of baseline protection. The role of public authorities is highlighted in particular in 3 areas: information on hazards and risks, disaster relief, and criminal matters.

44. In **France**, the Governmental White Paper on Domestic Security in the Face of Terrorism also makes it clear that public or private operators of vital infrastructures are responsible for internal protection measures against all possible threats, notably threats of a terrorist nature. Operators, however, need to base their protection plans on the mandatory guidelines and standards set for each sector by a national regulation, which includes a threat definition and security objectives. Additionally, in some cases, operator plans can be reinforced by the government's VIGIPIRATE plan, which contains a number of measures for vigilance, prevention and protection against terrorism based on four alert levels. One of these measures is a military

presence in airports and train stations. Other national emergency plans deal specifically with the threat posed by Chemical, Biological, Radiological and Nuclear (CBRN) terrorism, as well as attacks on aircraft or sea lanes.

45. To sum up, existing national CIP strategies generally recognise that CIP is a shared responsibility and requires a close partnership between public authorities and infrastructure operators – which can themselves be public or private actors. Operators are primarily responsible for the implementation of protection measures, but they often do so in accordance with the parameters or frameworks set by public authorities. Below is a simplified presentation of the most common division of labour between operators and government authorities based on the steps identified in the first chapter. The table shows clearly that most responsibilities involve some form of interaction between operators of infrastructures and government authorities, which can be either top-down or bottom-up.

Steps	Type of responsibility	Responsible authority
1. Define critical infrastructure	Exclusive	Government
2. Identify critical infrastructure	Shared	Operator input Government guidance (standards, methodology, oversight)
3. Assess risk: - Assess threat - Assess vulnerability and consequence	Shared	 Government (intelligence and law enforcement) at the national level / operator at the infrastructure level Mainly operator / government guidance (standards, methodology, oversight)
4. Define and implement protection measures	Shared	Mainly operator Government support
5. Set priorities of protection	Shared	Government / operator
6. Review implementation of the strategy	Shared	Government / operator

46. State intervention focuses on the following priority areas:

- provide the overall framework of the CIP strategy - including definitions and concepts, as well as in some cases the identification of critical infrastructure; co-ordinate efforts undertaken by all CIP stakeholders;
- ensure that these fit within the broader strategies and policies relating to civil protection / counter-terrorism / homeland security, and are compatible with the overall security goals;
- collect and share information on threats;
- ensure that risk assessments performed by operators are done in a harmonised / comparable and efficient manner, leading to the identification of security gaps at the national level; monitor / oversee this process;
- provide advice, guidance, or oversight of measures taken by infrastructure operators to protect their facilities;
- ensure in particular that intra-sector and cross-sector interdependencies are taken into account;

- complement protection measures whenever necessary, e.g. through the deployment of police or military forces;
- provide financial assistance to support CIP efforts – funding research on protection technologies and contributing towards implementation costs;
- promote awareness of the need for CIP and inform businesses and the population at large.

47. Some of these areas allow for a more or less active intervention by government authorities depending on individual political priorities and models of governance. They are thus the ones that make the difference between states that can be said to have a "hands-off" approach to protection and those with a more "interventionist" approach to CIP. Differences relate in particular to the:

- level of government oversight over the process of risk assessment: whether the government sets and enforces compulsory standards; sets and enforces minimum standards; recommends a harmonised methodology; suggests best practices, etc.
  level of government oversight over operator protection plans;
- level of government guidance in setting protection priorities and defining the acceptable level of risk;
- willingness of the state to implement protection measures in addition to operator plans.

48. Among the four countries studied above, France certainly has the most interventionist model, which guarantees strong oversight of infrastructure operators by public authorities. The United Kingdom and Germany favour a system based on incentive and guidance, rather than regulation. Finally, the US model is a mixed approach, which recognises the primary role of infrastructure operators in implementing protection measures, while including a relatively high level of state intervention.

49. Several areas of public-private interaction have proved problematic in practice. It is easy to understand that in some cases, the private sector has been resistant to expanded investment in security improvements. The recent debate in the United States regarding security rules for chemical plants is a good illustration of the possible conflict between public and private interests. Since the 2001 terrorist attacks, the US chemical industry has spent over US$3.5 billion on security updates to implement the voluntary standards it had set for itself. While cautiously embracing the need for government regulation as a way to ensure an "equal playing field" for all manufacturers, the chemical industry initially resisted attempts by Congress to tighten these rules and expand the federal government's oversight. Such resistance is natural, given that security improvements are generally expensive and usually provide no added efficiency to an organisation. Put another way, there is little financial incentive for private firms to invest in a socially desirable level of security, as the true cost of an attack to society is much larger than the damage this attack would cause to a private firm. Another problem is that private firms expect that the government will bail them out of financial distress if they are the victims of a major terrorist attack and therefore firms do not feel the need to prepare to bear all the burden of a possible attack. In this sense, the division of costs between the public and the private sector and the establishment of a proper system of incentives are crucial elements of an efficient CIP strategy. Governments have also engaged in awareness-raising campaigns to inform about the imperatives of CIP.

50. Public-private sharing of information is also far from perfect. The private sector has often proven reluctant to share information on vulnerabilities, as this could constitute valuable market intelligence for competitors. For instance, this remains an issue in the United States despite the establishment of various frameworks to facilitate and secure public-private information sharing. In a report from October 2006 surveying difficulties encountered in setting up the abovementioned Government and Sector Coordinating Councils, the US Government Accounting Office noted that representatives for about a third of these councils expressed concerns about sharing sensitive information about infrastructure vulnerabilities with the government and other sector members, due mainly to the fear that it might be publicly disclosed. Efficient public-private partnerships therefore require that public authorities organise a proper system of incentives and strong

guarantees of confidentiality. Public authorities in many countries also need to improve their own system of intelligence sharing so that information on threats is communicated to relevant infrastructure operators in a timely and accurate, yet appropriate, manner.

The role of the military

51. The military generally only plays a supportive role in CIP, focusing mainly on consequence management, that is on the aftermath of an emergency. However, several countries also authorise the use of the military as an extra patrolling force, which can be dispatched along with other police forces to monitor critical infrastructures (airports, public transportation system, etc.) or protect large-scale high-profile public events in the event of an elevated threat alert. These preventive deployments are expected to act as a deterrent to terrorists. An example of this occurred when intelligence information led to a strong military presence at London’s Heathrow airport in February 2003, where the army was last deployed in 1994. This is routinely the case in France in the framework of the VIGIPIRATE plan.

52. There is also another important aspect to the role of the military in relation to critical infrastructures. The planning and conduct of military operations rely on critical infrastructures, not only in the country of origin of the military assets but also in areas of operation. Therefore, the protection of critical infrastructures onsite is an important component of operations.

Informing, involving and protecting the public

53. If CIP focuses primarily on facilities rather than people, the ultimate purpose of CIP is to protect the population by ensuring the continuous operation of essential services. In some cases, particularly when considering infrastructure destined for public use such as airports or public transportation systems, CIP is inseparable from civil protection. In this sense, informing and involving the public is crucial and usually represents a major component of national CIP policies.

B. CIP AND INTERNATIONAL CO-OPERATION: THE ROLE OF THE EUROPEAN UNION AND NATO

54. In the current security environment, CIP efforts cannot remain isolated. Many critical sectors – transport, energy, information and communication – are increasingly globalised and interconnected. An incident in one country can have devastating consequences in another one. A recent example was the major electricity blackout which was triggered by a failure in Germany on 4 November 2006 which also affected Austria, Belgium, France, the Netherlands, Spain and Portugal.

55. Therefore CIP efforts require an international dimension in order to rationalise national efforts and avoid both gaps and duplications. The following section will focus specifically on the role of the European Union and of NATO in protecting critical infrastructures in Europe and North America.

The European Union

56. A number of sectoral measures already exist in several EU-regulated sectors (IT, health, finance, transport, port security, chemical and nuclear industries). However, no horizontal provisions on CIP currently exist at EU level, as EU institutions have only recently begun to examine the opportunity for broader involvement in CIP. This process, launched in 2004, has resulted in the presentation by the European Commission, in December 2006, of a comprehensive CIP package including a "Communication on a European Programme for Critical Infrastructure

Protection" (EPCIP) and a "proposal for a Directive on the identification and designation of European Critical Infrastructure to improve the protection of critical infrastructure in the EU".

57. The European Commission’s communication acknowledges that the primary responsibility for protecting critical infrastructure falls on EU member states and the owners or operators of critical infrastructure. However, it recognises the need to distinguish between two categories of infrastructure: those infrastructures that are critical nationally and the European Critical Infrastructures (ECI), whose characteristics make them critical for two or more EU member states and therefore require co-ordinated action.

58. The communication also identifies the protection of critical infrastructure in third countries as a priority for the EU, and therefore encourages dialogue and the exchange of best practices with specific EU partners, as well as within global institutions. Obviously, a major concern is that oil pipelines could be destroyed in third countries, which are suppliers of energy to the EU or transit countries, such as Russia, Azerbaijan, Kazakhstan, Georgia or Turkey, with a potentially devastating impact on EU economies. Nevertheless, as several EU officials explained to the Committee, so far only preliminary steps have been taken to address the foreign policy implications of CIP.

59. The core of the European Commission’s proposal is a draft directive, which establishes common procedures for identifying and designating ECI, and for assessing the need to improve their protection. ECI is defined as those “critical infrastructures the disruption or destruction of which would significantly affect two or more member states, or a single member state if the critical infrastructure is located in another member state”. The directive includes a provisional list of 11 critical infrastructure sectors, which are further divided into 29 sub-sectors, as presented in Appendix I.

60. According to the draft, member states would be responsible for identifying ECI on their territory based on a combination of cross-cutting and sectoral criteria to be defined at EU level. The European Commission would then draw up a list of ECI based on notifications from member states. When the CDS was in Brussels, it expressed criticism about whether the contents of this list could remain secure. Put in the hands of terrorists, they would be a major gift. ECI operators would be responsible for conducting a proper risk assessment, then adopting and updating an Operator Security Plan detailing the measures taken to protect the ECI in accordance with the risk assessment.

61. The directive was submitted to the European Parliament, which, in a resolution adopted on 10 July 2007, suggested a major overhaul of the purpose and procedures proposed by the Commission. Below are some of the main conclusions:

- insist on the fact that CIP is a national responsibility and any EU initiative should be based on a bottom-up approach;
- a common framework is necessary, but its objectives should be re-focused;
- ECI should be defined as those “critical infrastructures the disruption or destruction of which would significantly affect *three* or more member states, *or at least two member states other than that in which the critical infrastructure is located*”;
- member states should be responsible for identifying ECI located on their territory based on common criteria, but there should be no list of ECI at the Community level;
- the directive as modified establishes a procedure leading to the establishment of a list of ECI priority *sectors* at the EU level, rather than a list of ECI;
- duplication should be avoided at all cost; criteria for the identification of ECI and guidance regarding methodology and protection measures already exist in a number of sectors; therefore, in those sectors, no new action should be necessary;
- insist on the need for ECI to be located preferably on the territory of the EU; the EU should avoid being dependent on infrastructure situated in a third country.

62. The directive will now be submitted to the Council, which is expected to decide on its final adoption by the end of 2007. This will not be an easy process, as adoption of the directive requires a unanimous decision, and several governments continue to challenge the need for EU intervention in this field. In its conclusions of 19-20 April 2007, the Justice and Home Affairs Council had adopted a balanced opinion on the Commission's proposal, recognising the added value of EU action, while emphasizing the primacy of national responsibility in the protection of critical infrastructures and warning against unnecessary duplication and excessive regulation and costs. It also insisted on the need for adequate security arrangements regarding CIP-related information-sharing. Nevertheless, the European Commission has already started to build on its proposal in specific sectors. On 2 February 2007, it presented a communication on Protecting Europe's Critical Energy and Transport Infrastructure, which proposes criteria for the identification of ECI in each transport and energy sub-sector.

NATO

63. Although at first glance CIP is not a natural area of competence for NATO, the Alliance has been promoting CIP for several years now. NATO's interest in CIP started in 2001 with a first review of the state of readiness of NATO members in terms of planning and infrastructure mapping. Studies and activities on CIP were initiated by the specialised planning boards and committees working under the Senior Civil Emergency Planning Committee (SCEPC), NATO's main decision-making body in the field of civil emergency planning (CEP).

64. In 2003, SCEPC adopted a Concept Paper on CIP, as well as a road map with six areas of work, which aim to encourage the development of tools that nations can use to prepare for and manage the consequences of CBRN incidents, as well as, to some extent, of natural disasters, on their critical infrastructures. Main objectives include: promoting information sharing among CEP stakeholders; assisting in the development of training and education programmes; contributing to the identification of critical infrastructure; identifying research and development projects to support CIP; and streamlining CIP in field exercises.

65. NATO's activities in this area are part of a broader framework, the Civil Emergency Planning Action Plan for the protection of civilian population against CBRN events, which focuses in particular on CBRN-related terrorism. These and other NATO activities in the field of CEP are presented in greater detail in this Committee's Special report for 2006 on "*NATO and Civil Protection*" [166 CDSDG 06 E rev. 1].

66. Besides CEP activities, another pillar of NATO's work is the Programme of Work on Defence Against Terrorism adopted in 2004 by Heads of State and Government and which aims to promote the development of cutting-edge technologies for the protection of military assets and troops. CIP is one of the ten priorities of the Programme of Work and is led by Belgium. Activities developed in this framework aim to use military know-how, technology and capabilities to enhance the protection of strategic sites on the territory of allied nations, including airports, nuclear power plants, communication networks, etc. NATO has also recently stepped up its reflection regarding the protection of critical infrastructures in areas of operation.

67. NATO member states generally support NATO's role in CIP, though some allies – primarily France – are openly sceptical about NATO's added value in this field. All allies recognise also that CIP, like CEP, remains primarily a national responsibility. At the NATO summit in Riga in November 2006, Heads of State and Government confirmed the Alliance's role in CIP, reiterating their "determination to protect [our] populations, territories, infrastructure and forces against the consequences of terrorist attacks" and underscoring that "Alliance security interests can also be affected by the disruption of the flow of vital resources". A similar reference appears in the Comprehensive Political Guidance also endorsed by Heads of State and Government in Riga.

68. NATO's approach in the field of CIP is quite different from that of the EU. Seen from the CEP perspective, NATO does not aim at regulation. Rather, Alliance programmes aim to support national plans by promoting higher standards of preparedness and better interoperability in consequence management. Through the Civil Emergency Planning Action Plan, NATO also extends this support to its 23 partner countries, thereby promoting greater resilience in those countries.

69. Nevertheless, the risk remains that, given the current state of relations between NATO and the EU, lack of dialogue might lead to duplication of efforts. As the CDS's Special report of 2006 pointed out, and as was confirmed during the Committee's meetings in Brussels in January-February 2007, duplications already exist in a number of areas relating to civil protection. Yet, there is no institutional framework for EU-NATO dialogue on these issues and at least one member state of both organisations – France – is opposed to any step in that direction. The problem is further complicated by the fact that on the EU side, many of these issues fall within the competence of the European Commission, yet NATO's sole institutional partner is the EU Council. This situation is regrettable; given the enormity of the challenge and the current deficiencies in the protection of critical infrastructure in EU and NATO member states, international co-ordination is essential and should focus on the specific assets and strengths of each organisation and the added value each can bring to national efforts. In order to achieve this goal, dialogue is crucial and should happen at all levels, including high-level inter-institutional dialogue.

III. SECTORAL POLICIES

70. As mentioned in the previous chapters, besides the necessary common foundations of CIP strategies, implementation is done primarily within designated CIP sectors. The following sections will examine four case studies of CIP sectors, whose specificities make international co-operation particularly necessary

A. CRITICAL INFORMATION INFRASTRUCTURE PROTECTION (CIIP)[1]

71. Information and communication have been one of the first sectors in which the need to protect critical infrastructure against potential threats was acknowledged. First steps were taken in the late 90s, with the United States playing a pioneering role. The fears relating to anticipated problems on the threshold of the year 2000 have also helped to raise awareness of the potential implications of a global "cyber-crisis". These initial steps have promoted the emergence of the specific policy field referred to as Critical Information Infrastructure Protection (CIIP). The terrorist attacks of 11 September 2001 have given national and international efforts new impetus.

72. Critical information infrastructure is a broad concept that designates both the information itself (the data flow) and the channels through which information is created and conveyed (mainly computer networks). Consequently, CIIP is usually understood as including both the protection of data (including issues of privacy) and the protection of information infrastructure (also called "network security").

73. The CIIP sector presents a number of particularities compared to other CIP sectors. First, it can be said that, with the spread of IT within our societies, virtually everyone has become a potential weak link of IT security. Consequently, protecting critical information infrastructure is

[1] The Centre for Security Studies of the Swiss Federal Institute of Technology published in 2006 an updated version in two volumes of its CIIP Handbook, which provide a detailed analysis of the challenges of CIIP, as well as a survey of a large variety of national and international policies. The information presented in the following developments is largely based on the two handbooks.

particularly challenging, as it involves an almost infinite number of stakeholders. Secondly, information is an area where national boundaries have little relevance and interdependency is the norm. Therefore, in this sector more than in others, national protection policies will have to be complemented by co-operative multilateral efforts.

74. The threat to these infrastructures is essentially manmade, but until recently cyber-terrorism and cyber-warfare were considered as a relatively abstract threat. So far, terrorist networks have used the Internet mostly as a tool for intelligence gathering, recruitment and fundraising activities. Cyber-attacks, including against government computer systems, have been isolated and come essentially from unstructured hackers with no ideological motivation. There were only a few instances of politically-motivated attacks.

75. A recent massive cyber-attack in Estonia has prompted many states and international institutions to reassess the threat posed by cyber-terrorism and cyber-warfare. The wave of attacks on Estonian websites started on 27 April 2007 with the website of the Prime Minister, while the President’s site and those of other ministries followed soon thereafter. The attacks continued in waves over a period of almost three weeks, progressively striking other areas of Estonia’s cyber-infrastructure, including newspapers, television stations, banks, etc. Sites that typically received 1,000 visits a day were flooded with thousands of hits a second, overwhelming servers and forcing them to shut down. Attempted attacks targeted the mobile phone networks and rescue service systems, but did not last long enough to paralyse them. The attackers did, however, manage to hit the national emergency number, which was out of commission for a short time.

76. The attacks on Estonia were unprecedented in that they constituted a co-ordinated and large-scale attack against a broad range of government assets and public and private services. Their origin remains unclear to this day. Estonian officials have claimed that most attacks originated from servers based in Russia, including a number of official websites. In their view, these attacks fit into the series of retaliatory incidents following Estonia’s decision to relocate a Soviet-era war monument. Russian authorities have denied any involvement in these attacks. Recently, a report by an Israeli expert commissioned by the Estonian government concluded that the attacks did not appear to be co-ordinated by a foreign government, but rather constituted some kind of “cyber-riot”, which spread through blogs. Although Estonia’s cyber-infrastructure is particularly developed and many activities in the country rely heavily on electronic communications, these attacks luckily did not result in any severe consequence. However, they constituted a wake-up call for many about the potentially devastating effect of cyber-attacks, particularly if combined with a physical attack.

77. National CIIP policies differ primarily in the way they define the respective responsibilities of state authorities and the private sector. In France or Sweden for example, state authorities, including the defence establishment, play a major role, whereas in the United Kingdom or Switzerland the private sector takes on an equal share of responsibility. Nevertheless, all countries have developed structures for public-private co-ordination.

78. Despite this diversity, national approaches seem to converge on two aspects. First, they recognise that, given the specificities of the IT sector, early warning is crucial to allow for rapid reaction. This requires in particular increased information sharing between state authorities and the private sector. Second, national policies increasingly emphasise law enforcement activities, that is, the fight against cyber-crime and the pursuit of offenders.

79. International co-operation on CIIP remains relatively underdeveloped. Its value so far has been mostly to raise awareness of the threats and challenges, encourage the adoption of adequate legislation, and facilitate cross-border forensics and arrests. The Council of Europe adopted in 2001 an international Convention on Cyber-crime, which included binding provisions to facilitate international co-operation in the investigation and prosecution of computer crimes. The

convention entered into force in 2004 and as of 15 August 2007, it was ratified by 21 countries. The G8 started discussion cyber-crimes in 1998, but focused mainly on preventing the dissemination of paedophilia, drug trafficking, money-laundering and electronic fraud. In the aftermath of events in Estonia, the Group called for greater co-operation against cyber-crime and cyber-terrorism.

80. The European Union has also taken several steps to promote co-operation among member states on CIIP: harmonisation of legislation on data protection and privacy; creation of the European Network and Information Security Agency (ENISA); adoption of a Strategy for a Secure Information Society in May 2006; promotion of research and development. It should be noted that ENISA acts as a centre of expertise and does not play any operational role in fighting cyber-attacks. Nonetheless, ENISA has been conducting an investigation in Estonia following the events of April-May 2007.

81. The European Commission announced in May 2007 a new communication entitled “towards a general policy on the fight against cyber-crime”, which covers three categories of criminal activities: crimes, such as fraud or forgery, committed over electronic communication networks and information systems; the publication of illegal content over electronic media; crimes directed against electronic networks, such as attacks against information systems, denial of service, hacking, etc. The communication plans actions to improve co-ordination of Internet surveillance, reinforce operational cross-border law enforcement co-operation, and strengthen public-private co-operation. Despite these additional efforts, the Union’s initiatives are constrained by the reluctance of some member states to acknowledge its competence in this area.

82. NATO is also contributing to the protection of Allied communication and information systems against cyber-attacks. The SCEPC Civil Communication Planning Committee is principally in charge of promoting dialogue among relevant national authorities and examining NATO’s potential contribution to enhancing national CIIP capabilities. Additionally, Estonia has recently suggested the creation of a Centre of Excellence on Cooperative Cyber-defence to promote co-operation between NATO members, to draft training programmes and to deal with the legal aspects of fighting cyber terrorism. This initiative seems all the more relevant following recent events in this country. NATO has also developed capabilities to protect its own communications under the umbrella of the NATO Communication and Information Systems Services Agency (NCSA).

83. NATO has been prompt to react to events in Estonia and decided to dispatch a small group of experts. The NCSA was also called upon to monitor any future incidents. Estonian authorities have been actively calling on the Alliance to learn the lessons from their experience and develop a common cyber-defence policy.

B. ENERGY SECURITY

84. Energy security has recently re-gained prominence as a major concern for governments in Europe and North America. It is a broad topic, which includes both the security of energy supplies and the security of energy infrastructure. The 2006 General Report of the Economics and Security Committee on *Energy Security* [170 ESC 06 E rev. 1] provides an excellent analysis of the various challenges that NATO and EU countries face in relation to energy security. This section will focus exclusively on the protection of critical energy infrastructure.

85. It is widely agreed that energy infrastructures have already become a target for terrorists and that the evolution of global energy markets will only make this target more attractive to terrorists. It is already estimated that the oil market loses over one million barrels per day due to politically motivated sabotage. Recent incidents include a failed attack against the Abaqiq facility in Saudi Arabia, which holds one of the world’s largest oil fields. Iraq is another example, with an estimated 290 attacks against oil facilities between April 2003 and March 2006. Nigeria is also facing an

active campaign of violence against its oil facilities in the Niger Delta, which has already resulted in a significant drop of its oil output.

86. Existing CIP measures in the energy field have focused disproportionately on a few areas. The protection of nuclear power plants is a case in point, where strict national and international regulations already exist, in particular under the auspices of the International Atomic Energy Agency. However, other production and storage sites could represent attractive targets for terrorists. For instance, one could easily imagine the devastating consequences of a terrorist attack on a major dam. The same is true of infrastructure dedicated to the transport of energy – particularly pipelines and tankers. Yet, the protection of every route or even of every choke point is virtually impossible. For instance, the United States alone is home to 77,000 dams and reservoirs and nearly two million miles of oil and gas pipelines. In many cases, the cost of protection might actually exceed the potential damage caused by an attack. Therefore, prioritisation of protection is necessary.

87. Many national governments and international institutions are currently reviewing or enhancing their policies for the protection of critical energy infrastructure. In the United States, the American Petroleum Institute (API), along with several other oil and gas industry organisations, have created security guidelines for the entire industry, which managers can use to assess vulnerabilities and address them. API and the Department of Energy also operate an Energy Information Sharing and Analysis Center, which is an internet-based system that allows threat assessments to reach energy security personnel quickly. In 2004, 19 different oil and gas associations combined to form the Oil and Natural Gas Homeland Security Co-ordination Council, which serves as the focal point of contact between industry and the government.

88. The European Union has also moved into the field of energy security with several initiatives. The European Commission's Green Paper on energy of March 2006 identifies supply security as one of the objectives of a European energy strategy. The Commission proposes in particular the establishment of a European Energy Supply Observatory to identify infrastructure vulnerabilities and of a European Centre for Energy Networks to promote information exchange while establishing common standards for energy infrastructure. The recent communication on Protecting Europe’s Critical Energy and Transport Infrastructure of February 2007, which proposes criteria for the identification of European Critical Infrastructure in those two sectors, is also another step towards enhancing the protection of critical energy infrastructure in Europe.

89. However, protecting energy infrastructure at home only provides a partial response to the challenge posed by energy security. European and North American countries are highly and increasingly dependent on the outside world for their energy supplies. This means that Europe and North America also have an interest in enhancing protection of energy infrastructure in producing and transit countries, and of energy routes worldwide.

90. The United States has already taken several initiatives to this aim. The US navy has effectively become a guarantor of open shipping lanes throughout the world. Additionally, the US Global Critical Energy Infrastructure Protection Strategy involves an interagency effort to offer advice to nations that host critical energy assets on how to protect them better, including sending American security experts to work in these countries. However, these efforts already impose a heavy financial burden on US finances. The Institute for the Analysis of Global Security reports that the cost of defending the sea lanes of communication and providing military assistance to partners in oil supplying nations costs the United States $50 billion per year.

91. Co-operative efforts in this area are embryonic. Although EU documents take into account the external dimension of the Union’s energy security, the European Union is only just starting to consider its potential role for the protection of energy infrastructure in third countries. Meanwhile, NATO has stepped up its reflection about the Alliance’s contribution to energy security. At the Riga

Summit, Heads of State and Government called for a “co-ordinated, international effort to assess risks to energy infrastructures and promote energy infrastructure security” and tasked the North Atlantic Council to define “those areas where NATO may add value to safeguard the security interests of the Allies”. High-level NATO officials have floated several ideas. They have suggested that NATO could play a greater role in promoting political dialogue among Allies and Partners on energy issues. It could also improve its monitoring and assessment of energy security issues, including through intelligence sharing. NATO could further provide security assistance to partners for the protection of their energy infrastructure. NATO officials often cite maritime surveillance as another area where NATO could play an enhance role. Finally, they suggest that NATO could take on the role of enforcing maritime protection and interdiction operations in periods of conflict.

92. These suggestions cover a broad a range of actions and involve many aspects of NATO’s activities: partnership and co-operation; civil emergency planning; surveillance; intelligence sharing; military operations and rapid reaction capabilities. At the low end of this spectrum are a number of actions that would be relatively uncontroversial, such as preparedness co-operation, something the Alliance does on a regular basis. Azerbaijan and Qatar for instance have already expressed an interest in co-operating with the Alliance for the protection of their energy facilities. NATO could also be called upon for isolated patrolling and surveillance missions of specific sites in much the same way as it has in the past provided security assistance for the protection of high-profile events. At the higher end of the spectrum are actions that would involve a deployment of NATO’s military capabilities, including the NATO Response Force. Suggestions that NATO should protect major choke points or build on its current activities in the high sea, particularly the counter-terrorist operation Active Endeavour, are more problematic and would certainly be met with strong reservations by several Allied countries, concerned to see NATO involved in far-away places, where a NATO presence might be unwelcome.

93. Given that the protection of energy infrastructure is a relatively new area of focus both for NATO and the EU, duplication of efforts is not yet a major concern. Nevertheless, co-operation should be encouraged in this field as in others. Potential areas for co-operation could include for instance shared assessments of the threat to energy infrastructure; joint funding of research and development projects; and cross-participation in emergency preparedness exercises.

C. CIVIL AVIATION SECURITY

94. The terrorist attacks of 11 September 2001 have cruelly revealed the deficiencies of national and international aviation security regulations, and prompted governments to reconsider their policies in the light of the new threat posed by international terrorism. This has led to a major overhaul of existing national efforts, as well as a stronger focus on international co-operation and harmonisation. New aviation security rules have been developed to enhance security of airports, aircraft, and of air traffic control systems. Nevertheless, the discovery on 10 August 2006 of an alleged plot to set off bombs on aircraft flying from the United Kingdom to the United States using liquid explosives has demonstrated that the threat of terrorist attacks on civilian aircraft is still very real. The explosion of a bomb at the Madrid airport in December 2006 and the car bomb attack at the Glasgow airport in June 2007 demonstrate that airports also remain major targets for terrorists.

95. At the worldwide level, the International Civil Aviation Organisation (ICAO) is primarily responsible for the promotion of international standards and recommended practices on civil aviation security. In June 2002, the organisation adopted an Aviation Security Plan of Action aimed at strengthening aviation security worldwide. A central element of the Plan of Action is regular, mandatory, systematic and harmonised audits of measures taken by member states of the organisation to implement ICAO security-related standards in order to identify and correct deficiencies. The flip side of the ICAO’s security regulations is the facilitation programme, which aims at developing mechanisms to enhance the efficiency of border clearance operations, while maintaining high standards of security. The aviation industry has also been very active in

implementing new international regulations through the International Air Transport Association (IATA), which brings together some 260 member airlines.

96. Since 2002, the European Union has also started to play a more central role co-ordinating member states' policies in the field of aviation security. Whereas prior to 2002, aviation security was considered a national prerogative, common rules have since been adopted on airport security, aircraft security, baggage screening, cargo, mail, etc. The European Commission carries out inspections of airports and of national authorities in charge of civil aviation to verify the proper implementation of these standards. In November 2006, the Commission enacted new regulations to restrict the size of hand luggage as well as the amount of liquids that passengers may carry on board aircraft for all flights departing from EU airports. It is also considering authorising the presence of armed air marshals on flights. Current EU projects regarding the identification and protection of European Critical Infrastructure, including the specific proposals presented in the transport sector, should further reinforce this set of measures. Finally, the European Union's activities also include an external dimension, as the Union has engaged in a dialogue with its main partners on aviation security. Since 9/11, transatlantic co-operation has been identified as a major priority and has led to major achievements, despite serious disagreements on a number of issues, including passenger data protection. In October 2006, the Union signed an interim agreement with the United States authorising US authorities to access electronically passenger name record (PNR) data from air carriers' reservation and departure control systems located within the territory of the EU. This followed a legal battle, which resulted in the annulment by the European Court of Justice of the previous agreement signed in 2004. The interim agreement should now be replaced by a permanent agreement signed by both parties at the end of July 2007. This text, however, is heavily criticised by the European Parliament and other national parliaments, which denounce a serious assault on civil liberties.

97. Several initiatives within NATO also relate to civil aviation security. SCEPC Civil Aviation Planning Committee promotes initiatives for assisting NATO members with identifying vulnerabilities and adopting protective measures. NATO has also developed air defence concepts and capabilities. In the aftermath of 9/11, the Prague Summit in 2002 adopted the "RENEGADE concept" in the event of use of an aircraft as a weapon to perpetrate terrorist attacks. The Programme of Work Defence against Terrorism also agreed on the same occasion includes the objective of reducing the vulnerability of civilian and military aircraft to MANPADS. NATO's own military capabilities have been used on several occasions to prevent terrorist attacks using aircraft. In the immediate aftermath of the terrorist attacks of 11 September 2001, the North Atlantic Council agreed the deployment of AWACS aircraft to patrol US airspace and help prevent further attacks. Since this first and highly symbolic deployment, AWACS have been used to provide air surveillance during several large-scale public events. Finally, since 2002, NATO co-operates with other international and regional organisations to enhance the security of air traffic management (ATM) systems. NATO and the pan European organisation EUROCONTROL have set up a coordinating group to develop a joint ATM strategy. It is worth noting that the European Commission also participates to this joint effort.

D. PORT SECURITY

98. Maritime security has been one of the key concerns of the international community after the terrorist attacks of 11 September 2001. Ports, waterways, and shores across Europe and North America are lined with military facilities, nuclear power plants, locks, oil refineries, levees, passenger terminals, fuel tanks, pipelines, chemical plants, tunnels, cargo terminals, and bridges, all of which could be dangerous terrorist targets. Ports in particular have inherent security vulnerabilities: they are sprawling, easily accessible by water and land, close to crowded metropolitan areas, and interwoven with complex transportation networks. It is estimated that 90% of all traded goods travel by sea on approximately 72 million sea containers a year.

99. International efforts to increase maritime security have resulted in a significant body of international regulations and initiatives. A landmark document is the International Ship and Port Facility Security Code (ISPS) adopted in the framework of the International Maritime Organisation and ratified by 148 countries. This code went into effect on 1 July 2004, and requires all port facilities and vessels to create and submit a security assessment and plan to address vulnerabilities. Any ship not meeting this standard can be denied entry into any participating country. An EU directive of October 2005 incorporates and builds upon the provisions of the ISPS code.

100. The United States has been at the forefront of international efforts to protect ports and cargo and has initiated a number of multilateral projects. The Container Security Initiative is a worldwide strategy to inspect containerised cargo destined for the United States before it leaves its homeport, thereby preventing any potential dangerous substance from reaching US shores. US customs inspectors have now been stationed in 37 of the world's largest seaports, 20 of which are in the EU. Additionally, the Customs-Trade Partnership Against Terrorism offers private shipping companies in the programme faster customs processing if these companies take extra security precautions. There are currently 8,200 companies that are certified members of the programme, representing 40% by value of the cargo entering the United States. Finally, the 2003 Mega-Port Initiative is a co-operative effort through which the United States supports the installation of radiation detection capabilities at participating ports.

101. However, as the example of the port of Antwerp, which the CDS visited in February 2007, demonstrates, if the frameworks and regulations are already well in place, implementation of some of these aspects is still lagging. In particular, current levels of cargo and container screening are far from the 100% target set by several countries and in many ways, this objective seems unrealistic in the short or medium term. The main value of current efforts is therefore deterrence rather than protection as such, at least when considering the threat posed by CBRN terrorism.

IV. CONCLUSIONS

102. The task of protecting critical infrastructure in Europe and North America is daunting. As the list of existing initiatives presented in this report suggests, a lot has been done in recent years. Nevertheless, the unrelenting threat of international terrorism is a permanent test to these efforts and many challenges remain. As full protection of all infrastructures against all types of threats is impossible, governments have adopted strategies to identify critical infrastructures on their territory and prioritise protection.

103. However, as this report suggests, CIP is a particularly challenging policy area. First, critical infrastructures include an increasing number of facilities and activities that fall outside the realm of government control, as they are owned or operated by the private sector. CIP policies therefore need to include a variety of stakeholders with sometimes diverging interests. A crucial component of CIP is therefore the establishment of public-private partnerships. These partnerships should include an adequate system of incentives, engaging the private sector in the fulfilment of national security objectives. This in turn requires a fair division of the costs of protection.

104. A sector-based approach, which breaks down national strategic guidelines into priorities and objectives for each CIP sector, has become the norm for national and international CIP efforts. However, this approach needs to be complemented by a proper analysis of cross-sectors interdependencies. These involve very complex dynamics, which are still poorly understood and have therefore too often been neglected by policy-makers.

105. Another major challenge stems from the limited relevance of national borders in many major CIP sectors. Information, air transport, energy, all rely on cross-border interdependent networks of

infrastructures. Given this configuration, international co-ordination is crucial to promote effective protection and avoid weak links which could endanger the whole security chain. However, existing initiatives have highlighted the difficulties of international co-operation on CIP. First, different countries face different threats and will therefore tend to promote different standards of protection. Moreover, national traditions shape national approaches, which differ greatly, particularly in the balance they organise between state intervention and private sector involvement. Additionally, the multiplicity of stakeholders is also a complicating factor for international co-operation. More thought should be given to the wisdom of preparing a physical list of European Critical Infrastructures which could provide a “shopping list” for terrorists.

106. As the four case studies in the previous chapter have demonstrated, a large number of regional and international organisations and groups deal with various aspects of CIP. However, these initiatives sometimes give the impression of an uncoordinated proliferation of efforts. Given the enormity of the task facing our governments, it is particularly important to ensure the complementarity of international efforts, and avoid duplication and waste of resources in Europe and beyond.

APPENDIX

European Critical Infrastructure Sectors in the EU Directive

I Energy	1 Oil and gas production, refining, treatment, storage and distribution by pipelines 2 Electricity generation and transmission
II Nuclear industry	3 Production and storage/processing of nuclear substances
III Information, Communication Technologies, ICT	4 Information system and network protection 5 Instrumentation automation and control systems (SCADA, etc.) 6 Internet 7 Provision of fixed telecommunications 8 Provision of mobile telecommunications 9 Radio communication and navigation 10 Satellite communication 11 Broadcasting
IV Water	12 Provision of drinking water 13 Control of water quality 14 Stemming and control of water quantity
V Food	15 Provision of food and safeguarding food safety and security
VI Health	16 Medical and hospital care 17 Medicines, serums, vaccines and pharmaceuticals 18 Bio-laboratories and bio-agents
VII Financial	19 Payment and securities clearing and settlement infrastructures and systems 20 Regulated markets
VIII Transport	21 Road transport 22 Rail transport 23 Air transport 24 Inland waterways transport 25 Ocean and short-sea shipping
IX Chemical industry	26 Production and storage/processing of chemical substances 27 Pipelines of dangerous goods (chemical substances)
X Space	28 Space
XI Research facilities	29 Research facilities

Source: European Commission