Federal Republic of Germany
Federal Ministry of the Interior

Berlin, 17th June 2009

National Strategy for Critical Infrastructure Protection (CIP Strategy)

National Strategy for Critical Infrastructure Protection

1. Guiding policy concept

Infrastructure in general and critical infrastructure in particular are the lifeblood of modern, efficient societies. Germany is among the leading industrial and technology-oriented nations. Germany's importance as a location for business and industry and ensuring the country’s competitiveness in a globalized economic and technological setting are crucially dependent, as preconditions for prosperity and progress, on the availability of high-performance and well-functioning infrastructure.

Therefore, ensuring the protection of this infrastructure is a key function of security-related preparedness measures taken by industry and government agencies, and is a central issue of our country's security policy. Germany has, both nationally and internationally, actively addressed matters of critical infrastructure protection (CIP) and is guided by the principle of joint action by the state, society, and business and industry. The state co-operates, on a partnership basis, with other public and private actors in developing analyses and protection concepts. Either - primarily - as a moderator or - if required - by rule-making, the state regulates the measures for safeguarding and securing the overall system and the system procedural flows.

The implementation of infrastructure protection measures, on the basis of voluntary undertakings and by incorporating them in legal provisions, has helped to achieve and maintain a high level as regards the safety standard and failure safety of critical infrastructure in Germany. In order to come up to this level also in future in view of changed conditions regarding the security environment, we must continue and intensify our approach of trusting and constructive co-operation on the way to comprehensive critical infrastructure protection and must further develop co-operation among the relevant governmental and industrial players.

The National Strategy for Critical Infrastructure Protection summarizes the Federal Administration's aims and objectives and its political-strategic approach that is already applied in practice and, for the field of information technology, is included, for example, also in the National Plan for Information Infrastructure Protection *(Nationaler Plan zum Schutz der Informationsstrukturen - NPSI)*; the Strategy also is the starting point for consolidating the results achieved so far and for further developing them in view of novel challenges.

●●●

2. Progress made so far, and present status

Critical infrastructure protection is a task of society as a whole, which calls for co-ordinated action supported by all players – government, business and industry, and the general public. The importance of this task derives directly from the definition of the term "critical infrastructure" as used by the Federal Administration:

definition

Critical infrastructures (CI) are organizational and physical structures and facilities of such vital importance to a nation's society and economy that their failure or degradation would result in sustained supply shortages, significant disruption of public safety and security, or other dramatic consequences.

Germany has a close-meshed network of infrastructures that are of vital importance to the country's society. The provision of the population and of business and industry with energy, IT and transport services, with health care and financial facilities and with drinking water and food supplies is very good. A stable constitutional and legal system provides for the general conditions ensuring peaceful community life in security and prosperity also in the event of crises.

Not only in quantitative, but also in qualitative terms, Germany has a good record of achievement. Security of supply in the sense of failure safety, e.g. as regards power supply, ranks at the top as compared with other countries. This is due to the fact that privately organized power supply companies are under the legal obligation to operate a secure, reliable and high-performance supply network. Compliance with the (statutory) requirements is controlled by the industry's associations on the basis of the Energy Industry Act (i.e. the Act on the Supply of Electricity and Gas - *Energiewirtschaftsgesetz*) and, on the government side, by the Federal Network Agency *(Bundesnetzagentur - BNetzA)*[*], especially by means of technical checks and monitoring reports. Similarly, telecommunication service providers also are subject to legal regulations and must protect the relevant telecommunication and information processing systems, by means of technical safeguards and other measures, against unauthorized access. Moreover, the operators of telecommunication systems have to designate a security officer and provide the Federal Network Agency with a security concept which must state the threats to be expected and the technical precautions or other protective measures that have been taken or are planned.

[*] full name: Federal Network Agency for Electricity, Gas, Telecommunications, Post and Railway [translator's note]

However, society's vulnerability has, over the past few years, grown rapidly on account of the increasing extent to which nearly all spheres of life are pervaded with, and dependent on, critical infrastructure. Consequently, internal security aspects play an essential and increasingly important role in this particular field.

Already in the late 1990's, the Federal Government set itself the task of ensuring critical infrastructure protection as a key element of the state's security-related preparedness system. In this respect, especially cross-sectoral issues also play an important role, in addition to the sectoral aspects addressed by the line Ministries.

The Federal Ministry of the Interior (Federal MOI) provides inter-departmental co-ordination of the central national-level CIP measures. On behalf of the Ministry of the Interior, the authorities within the MOI's remit - such as the Federal Office for Civil Protection and Disaster Assistance (*Bundesamt für Bevölkerungsschutz und Katastrophenhilfe - BBK*), the Federal Office for Information Security *(Bundesamt für Sicherheit in der Informationstechnik - BSI)*, the Federal Criminal Police Office *(Bundeskriminalamt - BKA)* and the Federal Institute "Technical Support Service" (Federal Technical Relief Agency - *Bundesanstalt Technisches Hilfswerk, THW)* – develop threat assessments, analyses and protection concepts.

results

Overall, many initiatives have been launched and packages of measures have been implemented. Examples are:

- Comprehensive precautionary measures were taken by government agencies and by business and industry to cope with the so-called Y2K problem in order to ensure the operability of information technology and all computer-based infrastructures also after the turn of the millennium. The IT Baseline Protection Concept *(Basisschutzkonzept)* for information infrastructure, the National Plan for Information Infrastructure Protection *(NPSI)* and the related CIP Implementation Plan (*Umsetzungsplan KRITIS - UP KRITIS)* have provided for important concepts and specific measures. These instruments are implemented jointly with business and industry.

- Following the terrorist attacks of 11 September 2001 and the flood disaster in the summer of 2002, the focus of structured security-related preparedness has, at the government level, shifted not only to information technology but to all other CI systems as well. New priorities have been set for dealing with potential threats. Examples of major changes resulting from the attacks of 11 September 2001 are the introduction of preventive personnel-related counter-sabotage protection as a mandatory task of specific public and non-

public entities, or the international agreements on increased protective measures in the transport sector, e.g. for airports or for port infrastructure, which have been implemented in Germany.

- Apart from the IT security concepts, further results of the combined efforts of the public and the private sectors are a number of additional recommendations, guidance documents and practical leaflets and booklets prepared in close co-operation with public authorities, infrastructure companies and with associations, business and industry and the academic community. Examples are the guidance documents on "Critical Infrastructure Protection – Baseline Protection Concept" and on "Critical Infrastructure Protection – Risk and Crisis Management"; protection concepts for relief organizations, welfare associations and hospitals; or the Manual on In-Plant Pandemic Preparedness Planning *(Handbuch betriebliche Pandemieplanung)*.

- In addition, infrastructure companies are regularly invited to take part in the *LÜKEX* series of national table-top exercises (*Länderübergreifende Krisenmanagement Exercise* - a cross-State crisis management exercise) launched in 2004 so that they can familiarize themselves with, exercise and further develop, the structures and measures developed for crisis management by governmental and private partners as a 'module' of the national-level security preparedness system. These joint exercises have reinforced the trusting co-operation among the state and business and industry, based on the conviction that crisis management can only be achieved by joint action and effort.

- In order to ensure that in future preventive and precautionary measures can be taken, to an even greater extent than so far, in response to the changed risks and growing vulnerabilities, and in order to be able optimally to harness the potential offered by new technologies and procedures for critical infrastructure protection, the federal authorities take part in many activities under the national programme "Research for Civil Security" *(Forschung für die zivile Sicherheit)* which was launched in 2007 by the Federal Government as part of the HighTech Strategy for Germany. In association with the academic community, industry and infrastructure operators, innovative solutions for civil security are being investigated and developed.

This close-meshed network for information and communication flows between the state and companies and for joint projects and measures should, if and where required, be further developed and consolidated.

●●●

3. Criticality of infrastructure and areas of responsibility

Infrastructure is considered "critical" whenever it is of major importance to the functioning of modern societies and any failure or degradation would result in sustained disruptions in the overall system. An important criterium for this assessment is **criticality** as a

> *a relative measure of the importance of a given infrastructure in terms of the impact of its disruption or functional failure on the security of supply, i.e. providing society with important goods and services.*

definition: criticality

Such criticality may be of a systemic or symbolic nature or include both elements. An infrastructure will, in particular, be of *systemic criticality* whenever - due to its structural, functional and technical position within the overall system of infrastructure sectors - it is highly relevant as regards interdependencies. Examples are the *electricity* and *information and telecommunication infrastructures* which, on account of the size and density of their respective networks, are of particular relevance and where a large-area and prolonged outage may lead to serious disruptions of community life and processes and of public safety and security.
An infrastructure may be of *symbolic criticality* if its loss might, on account of its cultural significance or its important role in creating a sense of identity, emotionally unsettle a nation's society and psychologically have a lasting unbalancing effect on it.

Critical infrastructures may, with reference to their technical, structural and functional specifics, be classified as vital (absolutely essential) technical **basic infrastructure**, on the one hand, and vital (absolutely essential) socio-economic **services infrastructure**, on the other hand. In Germany, these include:

Technical basic infrastructure	Socio-economic services infrastructure
Power supply	Public health; food
Information and communications technology	Emergency and rescue services; disaster control and management
Transport(ation)	Parliament; government; public administration; law enforcement agencies
(Drinking-) water supply and sewage disposal	Finance; insurance business
	Media; and cultural objects (cultural heritage items)

Significant interdependencies exist between these two infrastructure sectors since nearly all of the socio-economic services infrastructures largely rely on the unrestricted availability of the technical basic infrastructure. However, technical basic infrastructures, in their turn, depend on socio-economic services infrastructure, such as a stable legal service or functioning first response, emergency medical and rescue services in the event of a crisis.

A look at the ownership structure shows that, as a rule, the various infrastructures are not state-owned facilities but that the majority of them are operated and controlled by private enterprises – part of which were privatized only recently.

Increasingly, the same also goes for the many and various public infrastructure services provided at the local government level, which more and more frequently are delivered by private-sector enterprises.

As a result of this tendency towards private ownership, also the responsibility for the security, reliability and availability of such infrastructure increasingly passes to the private sector or, at least, becomes a shared responsibility. Thus, the functions incumbent on the state and/or public authorities are primarily directed at making provisions for, or - at the most - safeguarding and controlling, the supply of goods and services in times of crisis when regular market mechanisms no longer function. Therefore, as a precaution against, and in view of coping with, serious disruptions and severe disasters/emergencies, the requirement is for institutionalized, organized co-operation of the state and business and industry within the framework of established security partnerships.

responsibility for CIP

●●●

4. Threats, risks, vulnerabilities and risk culture

Critical infrastructure may be exposed to various threats which must be included both in risk and threat analyses and in the selection of options for action (all-hazards approach). The overall spectrum of threats may be described as follows:

Natural events	Technical failure/ human error	Terrorism, crime, war
Extreme weather events inter alia, storms, heavy precipitation, drops in temperature, floods, heat waves, droughts	System failure inter alia, insufficient or excessive complexity of planning, defective hardware and/or software bugs	Terrorism
Forest and heathland fires	Negligence	Sabotage
Seismic events	Accidents and emergencies	Other forms of crime
Epidemics and pandemics in man, animals and plants	Failures in organization inter alia, shortcomings in risk and crisis management, inadequate co-ordination and co-operation	Civil wars and wars
Cosmic events inter alia, energy storms, meteorites and comets		

These events and incidents - which are due to very different causes - may impair, cause massive damage to, or destroy the infrastructure facilities which are vital to society and the population in general. Due to the great dependence on infrastructure services, society has become very vulnerable; and this vulnerability has greatly increased not only on account of *external* hazards and risks but also because of the important interdependencies among the various infrastructures *within* the relevant systems. Disruptions or failures may entail so-called domino effects and cascade effects which potentially can paralyze sectors of society and, in addition to the immediate damage caused to affected persons, can result in enormous damage to the national economy and in loss of confidence in a society's political leadership.

Since 11 September 2001, the threat posed by international terrorism, in particular, has been the main driving force behind the state’s efforts to achieve and maintain protection and security. The importance of this threat has increased even more over the past few years. Together with society’s dependence on reliable infrastructure, the increasing use of modern technologies by (potential)

violent terrorist criminals calls for continuing measures to ensure protection of critical infrastructure against terrorist attacks.

Apart from the risks resulting from intentional - especially terrorist - acts, consideration must also be given to possible and, in instances, immense damage caused to infrastructure by extreme natural occurrences. In Germany, severe damage to infrastructure facilities and thus to supply services may be caused, above all, by extreme weather events, such as violent storms or heavy precipitation. The global climate change, which has been scientifically confirmed and the effects of which are increasingly being felt, will in future engage the global community's attention intensively and on a long-term basis. Even though the consequences, in their entirety, are not yet fully foreseeable, the changes in climate will entail additional and, in part, extreme burdens on critical infrastructure even in the temperate latitude zones of Central Europe.

Therefore, the state's and society's attention must be directed to two threat causes, in particular: i.e. the terrorist threat and, in addition, natural hazards with their growing impact on infrastructure.

Of similar importance are the risks and threats to information infrastructure. Criminal acts, technical failure and/or human error or organizational shortcomings jeopardize the **operability** of this infrastructure since it is of vital importance to modern societies and their operational processes and its disruption or failure may, due to the existing interdependencies, have far-reaching consequences.

Irrespective of the nature and causes of the various threats, societies using highly industrialized, very complex **technologies** and relying on specialized, sophisticated **organizational structures** are particularly vulnerable as a result. Societies will, in the course of their technological development, be considerably more sensitive to any disruption of those infrastructures, in particular, that rely on sophisticated technologies because these societies are used to very high safety and security standards and to a high degree of security of supply. This phenomenon that, when robustness increases and breakdown susceptibility decreases, an absolutely fallacious sense of security develops and the impact of an "against-all-probability" incident [i.e. an unlikely incident which occurs nonetheless] will be disproportionately severe, is known as the "paradox of vulnerability":

paradox of vulnerability

> *The more a country's susceptibility to failures as regards supply services decreases, the more severe will be the impact of an actual disruptive incident.*

This paradox is constantly reinforced as a result of the increasing use, in nearly all sectors of society, of electrical appliances and electronic equipment, measurement and control engineering, information and communications technologies (ICT), and on account of their continuously growing dependence, for instance on the availability of electric power or on information and communications technologies. Therefore, importance should continue to be attached to technology (impact) assessments, also under security policy aspects regarding critical infrastructure protection.

Also in respect of the current security philosophy, there is a conclusion to be drawn from the identified newly emerged threats, risks and serious vulnerabilities and the resultant complexity as regards prevention and proactive (preparedness) arrangements:

No one-hundred percent protection of infrastructure and its operational effectiveness can be ensured by either the state or operators. The present security mentality must be converted into a new "risk culture". This novel risk culture is based, *inter alia*, on

risk culture

- open risk communication among the state, companies, citizens and the general public, taking account of the sensitivity of certain information;
- co-operation among all stakeholders in preventing and managing incidents;
- greater self-commitment by operators as regards incident prevention and management;
- a greater and self-reliant self-protection and self-help capability of individuals or institutions affected by the disruption or compromise of critical infrastructure services.

Such a novel risk culture can help to make society more robust and more resistant in view of handling growing vulnerabilities.

●●●

5. Strategic aims

In Germany, critical infrastructure protection is a task to be performed jointly by government, companies and/or operators and also by civil society. The guiding principles regarding critical infrastructure protection are, in particular

- trusting co-operation between the state and business and industry at all levels; and
- the requirement for, and suitability and proportionality of, the measures taken and the use of resources made for increasing the level of protection.

For joint action to be successful, strategic guidelines [statement of (overall) objectives] are required which describe the basic philosophy, action and practices in all essential security-policy matters regarding critical infrastructure protection with reference to all relevant risks. On this basis, it will be possible to develop sub-goals which, in turn, will be specified in, and implemented under programmes, plans or concepts. In the IT field, such a plan already exists in the form of the National Plan for Information Infrastructure Protection *(NPSI)*.

The state's efforts in the CIP field must aim at ensuring and raising the level of protection in Germany by suitable measures, co-ordinated with the other stakeholders, in such a way

- that all existing and anticipated risks will be spotted beforehand, and critical elements and processes are identified; and that severe disruption and failure of important infrastructure services will be avoided, to the extent possible, by means of comprehensive proactive (preparedness) arrangements and be minimized by an existing efficient risk and crisis management system and by providing adequate optional courses of action;
  the measures taken should, whenever possible, be regularly included for testing in exercises;

prevention

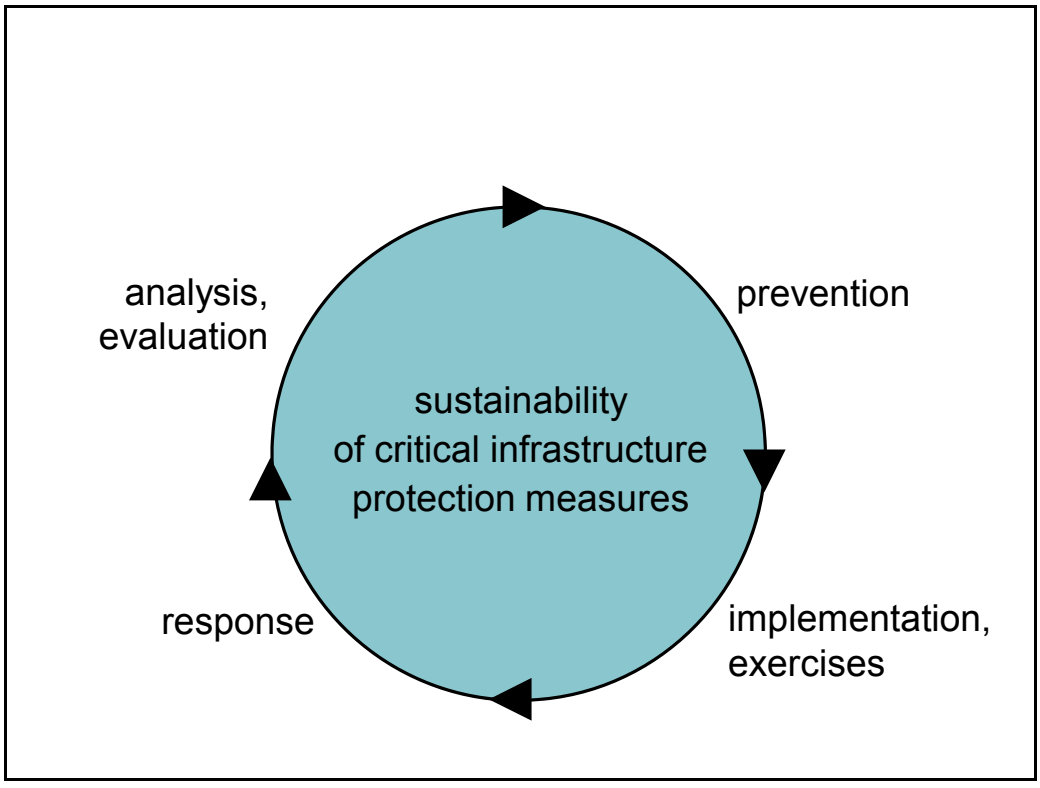
- that the consequences of severe disruptions and failures will be minimized to the greatest extent possible by means of effective emergency and crisis management and efficient redundancies as well as effective self-help capabilities of the entities and establishments directly affected; all activities undertaken at the time of an incident or disaster/emergency must aim at providing a maximum of effectiveness so that regular operations can be resumed without delay, if possible.

response

- In addition, 'lessons learnt' regarding enhanced critical infrastructure protection must be obtained from constantly updated threat analyses and from the analyses of technological and other incidents that occurred within the country or abroad, and these findings must be translated into protection standards to be developed jointly with the operators concerned and to be harmonized at the international level.

sustainability

Consistent implementation of these objectives in the form of a risk management cycle for critical infrastructure will offer the necessary guarantee of a consistent protective system of sustained effectiveness, which enhances the German security competencies that are also utilized in the international exchange of experience.



6. Co-operation, voluntary self-regulation, and legal regulations

Essential prerequisites for successful implementation of the stated strategic aims are well-functioning co-operation schemes and partnerships both with and among public authorities of different levels and belonging to different departments as well as with and among the infrastructure operators, which for the major part are private-law enterprises operating in the private sector of the economy, and the relevant associations as multipliers. Other stakeholding sectors of society, e.g. the academic community and industry, also are of importance, not least within the framework of European security research and in the context of the national programme "Research for Civil Security", which was initiated by the Federal Government and is monitored and supported by the Federal Ministry of Education and Research.
Therefore, in order to strengthen critical infrastructure protection, the requirement is for intensive co-operation, co-ordination and information between and among the relevant partners and players, including in particular:

- the Federal Administration[**]: Federal ministries and their specialist agencies;
- the federal states *(Länder)* and their authorities;
- the *Landkreise* [administrative districts], municipalities and local authority associations;
- infrastructure operators;
- the various relief and emergency response organizations;
- the relevant industrial associations and sectoral/professional associations;
- the science and research community;
- (security) industry;
- the general public (population, media);
- international and supranational institutions;

co-operative approach

and, if occasion demands, other institutions.

Critical infrastructure protection calls for joint action by the various federal government departments within their respective areas of responsibility, and by the various tiers of government [i.e. Federation, *Länder*, etc.] in accordance with the distribution of competence as provided under the Basic Law. Such co-operation includes exchanges of information among all parties involved and the development of action concepts co-ordinated with the relevant infrastructure providers and operators. The Federal Administration is committed to a co-operative

[**] *Bund* = Federal Ministries and their specialist agencies, such as the Federal Office of for Information Security *(BSI)*, the Federal Criminal Police Office *(BKA)*, the Federal Office for Civil Protection and Disaster Response *(BBK)*, the Federal Network Agency *(BNetzA)* [Translator's note]

approach and expects that important jointly developed analytical findings, framework recommendations and protection concepts will be implemented, in accordance with the security requirements, by infrastructure providers and operators and other important players, such as (trade) associations or standardization committees.

If identified substantial security deficiencies in critical infrastructure sectors are not remedied on the basis of voluntary commitments by the providers and operators or if, due to the emergence of new threats and risks, existing legal provisions do not offer adequate protection or do not apply in terms of plant safety and security, network security, operator-side security and user-side security, the Federation reserves itself the right, within its jurisdiction, to optimize the protection of the respective infrastructures by amending existing legislation or enacting new legal regulations.

federal law-making reservation

●●●

7. Implementation procedure

The Federation, the *Länder* and local governments are required *jointly* to enhance and implement critical infrastructure protection in their respective areas of responsibility. This purpose is served by a structured implementation procedure at these three tiers of government; this procedure comprises the following work packages, which in part are implemented in parallel, and is based on the co-operative approach adopted by the Federal Administration with the involvement of the other major players, i.e. operators and the relevant associations:

work packages

1. definition of general protection targets;
2. analysis of threats, vulnerabilities, and management capabilities;
3. assessment of the threats involved;
4. specification of protection targets, taking account of existing protective measures; analysis of existing regulations and, where applicable, identification of additional measures contributing to goal attainment; if and where required, legislation.

These work packages are implemented primarily by the public sector, with the collaboration of the companies and operators concerned. Responsibility for coordination at the federal level lies with the Federal Ministry of the Interior.

5. Implementation of goal attainment measures primarily by means of:
   - association-specific solutions and internal regulations;
   - self-commitment agreements by business and industry;
   - development of protection concepts by companies.
6. Continuous, intensive risk communication process
   (dialogue on analysis findings, assessments, protection targets, and action options).

Responsibility for the implementation of work packages 5 and 6 primarily lies with the relevant companies, operators and associations, with the participation of public agencies.

For the implementation of the National Critical Infrastructure Protection Strategy, an extensive set of instruments is available in the form of

instruments

- programmes and plans
  (e.g. the National Plan for Information Infrastructure Protection *(NPSI)* and the related implementation plans as a strategic concept for IT infrastructure protection);

- specific recommendations for action
  (e.g. the national Baseline Protection Concept as a basic guidance to physical critical infrastructure protection; the Risk and Crisis Management Guide for Critical Infrastructure Operators, or the national special protection concepts as detailed recommendations for action for the protection of individual CI sectors and sub-sectors);
- and standards, norms and regulations
  (e.g. the *BSI* Information Security Standards as a basic recommendation for action addressed to critical infrastructure operators; or the regulations of the German Gas and Water Supply Association *(DVGW)* on risk management in the field of drinking water supply).

On account of the chosen co-operative approach that must be given priority, suitably institutionalized platforms involving the state and public authorities, companies and associations are required in view of the procedural steps and instruments that serve to implement the politico-strategic framework concept. These security partnership platforms may be organized as:

security partnerships

- Round Tables on CIP (Federal level);
- Round Tables on CIP (*Länder*);
- Round Tables on CIP (local government level);

and as joint round tables of the Federation and the *Länder* or of the *Länder* and local authorities. The various round tables should organize their activities on the basis of a mutually agreed procedure based on the subjects and arrangements envisaged by the National Strategy, its philosophy, its procedural steps and mechanisms.

●●●

8. International co-operation

Disasters with an impact on the operability of critical infrastructure will not stop at national borders, as was forcefully shown by the Elbe River floods in 2002. Moreover, the transborder importance of critical infrastructure protection is on the increase on account of internationally important components, especially in the areas of information and communications technologies and energy and transport infrastructures, and this fact also has an influence on the objectives of any national strategy and is of relevance for the strategy's implementation.

For Germany, important international partners and co-operation fora are, in particular:

- our immediate neighbours;
- the European Union;
- the G 8 nations;
- NATO.

Within the framework of international co-operation, Germany supports all efforts and measures that are suited for identifying and minimizing the vulnerability especially of infrastructure of transborder relevance. Central importance attaches to the expansion of existing, and furtherance of new, bilateral co-operative schemes for the exchange of information and "best practices" and for the co-ordination of measures to protect transborder critical infrastructures.

Activities at the European level are of particular importance. As Germany sees it, bilateral and multilateral activities aimed at critical infrastructure protection, such as exchanges of information and methods as well as tried and tested procedures, are the proper approach in view of firmly establishing the CIP aims throughout the European Union while adhering to the principle of subsidiarity. To this end, the Federal Republic closely co-operates with the other EU Member States and with the European Commission. In doing so, Germany will dedicate its efforts to establishing adequate protective standards within the European area and will resolutely pursue the realization of its CIP-related concepts and visions on the basis of its National Strategy.

●●●