

 Gerold Reichenbach, MdB
 Ralf Göbel, MdB

 Hartfrid Wolff, MdB
 Silke Stokar von Neuforn, MdB

RISKS AND CHALLENGES FOR GERMANY

SCENARIOS AND KEY QUESTIONS

Green Paper of the
FORUM ON THE FUTURE OF PUBLIC SAFETY AND SECURITY

CONTENTS

Preface	5
Contributors	6
1. Introduction	10
1.1 New challenges	
1.2 Aims of the Green Paper	
1.3 The changed security environment	11
1.4 Globalisation harbours new risks	12
1.5 Players involved in public safety and security	
2. Basic principles in drawing up scenarios	14
2.1 Assumptions and methods	
2.2 Definitions and aims	
3. Key scenario "Power cut in Germany"	16
3.1 Nothing works without electricity	
Background: Modern information and communications technology opens up new areas of vulnerability	
3.2 Basic assumptions	19
3.3 Many possible causes	20
3.4 Effects of a power cut	22
Background: Communication influences the course of a crisis	
3.5 Sustainable risk and crisis management	26
3.6 Conclusion	27
4. Security threats in Germany from terrorism and organised crime	28
4.1 The internet: A new challenge	
4.2 Symbiosis despite different aims	
4.3 Precipitating and aggravating crises	29
4.4 Conclusion	31

5. Key scenario “An epidemic in Germany” _____	32
Background: Impact of an influenza pandemic	
5.1 Chikungunya fever	34
Background: Impact of climate change in Germany	
5.2 The SARS virus	39
5.3 Effects of the scenarios	40
5.4 Parallelism of effects	41
5.5 Conclusion	
6. Towards a modern definition of security _____	42
6.1 Key questions: Philosophy and aims of security	43
6.2 Key questions: Resources and mobilising them	44
6.3 Key questions: Elements of critical infrastructure	
6.4 Key questions: Population and civil protection	45
6.5 Key questions: Risk and emergency communication	
6.6 Key questions: Institutional requirements and implementation	
7. Glossary _____	48
Publishing details	55

References to appendices and further scenarios are contained in the text. These are available for download in German at: www.zukunftsforum-oeffentliche-sicherheit.de.

PREFACE

The FORUM ON THE FUTURE OF PUBLIC SAFETY AND SECURITY was called into being by a multi-party initiative within the German Bundestag. The suggestion was put forward by the Member of the German Bundestag Gerold Reichenbach, Social Democratic Party of Germany (SPD), who was joined by members of three other parliamentary groups in the Bundestag, all with responsibility for internal affairs, who agreed to create a joint platform for public security and safety: Bundestag Members Ralf Göbel of the Christian Democratic Union/Christian Social Union (CDU/CSU), Hartfrid Wolff of the Free Democratic Party (FDP) and Silke Stokar von Neuforn of Alliance 90/The Greens. The initiative is also supported by representatives of the business sector, the scientific community and NGOs. Also involved are police and non-police risk aversion representatives and experts from national, Länder and municipal authorities. The initiative has also developed loose but on-going contacts at EU level.

The FORUM ON THE FUTURE OF PUBLIC SAFETY AND SECURITY has decided to produce a Green Paper. A Green Paper is intended, within the EU, to be a starting point for processes of change in society. The FORUM ON THE FUTURE OF PUBLIC SAFETY AND SECURITY'S Green Paper summarises the discussions which have taken place in the expert working groups and the forum and develops central scenarios and key questions based on these discussions. On the basis of this work, the Forum hopes to provoke broad debate among politicians, economists, associations and the public about the many types of challenges involved in modern civil protection. It is hoped that the debate on the scenarios will open up a political evaluation. The Green Paper intends to provide pointers for this, without providing a ready-made political evaluation or solution.

PARTICIPANTS

EDITORS:

Gerold **Reichenbach**, Member of the German Bundestag, member of the Committee on Internal Affairs for the SPD parliamentary group in which he is responsible for reporting to the committee on civil protection and internal security issues.

Ralf **Göbel**, Member of the German Bundestag, member of the Committee on Internal Affairs for the CDU/CSU parliamentary group, in which he is responsible for reporting to the committee on internal security issues; deputy spokesman on domestic policy for his party.

Hartfrid **Wolff**, Member of the German Bundestag, member of the Committee on Internal Affairs for the FDP parliamentary group, in which he is responsible for reporting to the committee on civil protection and internal security issues.

Silke **Stokar von Neuforn**, Member of the German Bundestag, member of the Committee on Internal Affairs for the Alliance 90/The Greens parliamentary group, in which she is responsible for reporting to the committee on civil protection and internal security issues, spokeswoman on domestic policy issues for her party.

AUTHORS:

Michael **Bartsch***, Director of the Competence Center for Internal and External Security, T-Systems Enterprise Services GmbH.

Marie-Luise **Beck***, office manager for Gerold Reichenbach, Member of the German Bundestag.

Detlev L. **Burgartz**, head of the department for the prevention of crime and money laundering, German Insurance Association (GDV), head of the Green Paper working group on terrorism and organised crime.

Dr Achim **Daschkeit**, German Federal Environment Agency, Department I 2.1 climate protection, competence centre for climate impact and adaptation (KomPass), Dessau, head of the Green Paper working group on climate.

Professor Wolf R. **Dombrowsky***, head of the disaster research centre, Christian Albrechts University, Kiel.

Christian **Endress**, staff member, national secretariat, German Red Cross (DRK).

Dr Wolfram **Geier**, head of the division for emergency planning and critical infrastructure, Federal Office of Civil Protection and Disaster Assistance (BBK), Bonn, head of the Green Paper working group on corporate security and infrastructure.

Dr René **Gottschalk**, consultant for internal medicine, infectiology and public health, head of the competence centre for highly contagious diseases; Hesse and Rhineland Palatinate, chief medical director of the Infectiology department and deputy chief officer of the Frankfurt public health authority.

Benedikt **Liefländer**, (graduate lawyer) head of department, Maltese Cross Relief Service (MHD e.V.), general secretariat.

Dr Harald **Michels**, head of the public health authority, public order and internal affairs dept, district of Trier-Saarburg.

Ortwin **Neuschwander***, Ortwin Neuschwander Management Consultants e.K.

Dr Karsten **Ocker**, doctor of occupational medicine, doctor for the German Workers Samaritans Federation (ASB), chairman of the Permanent Conference on Disaster Preparedness and Civil Protection.

Professor Reinhard **Ries**, (graduate engineer) Director of the Municipal Fire Department, Frankfurt am Main.

Hagen **Saberschinsky**, former Berlin Chief of Police, Berlin (rtd).

Detlev **Samland***, Partner, Pleon GmbH.

Professor Hermann J. **Thomann**, (graduate engineer) Branch manager Government, TÜV Rheinland Group Cologne/Berlin, head of the Green Paper working group on corporate security and infrastructure.

Clemens Graf von **Waldburg-Zeil***, secretary general, German Red Cross, head of the Green Paper working group on capabilities, players, resources and population.

Prof. Dr DVM, Dipl. ECVPH Lothar **Wieler**, editor of the veterinary medical journal Berliner und Münchner Tierärztliche Wochenschrift, Managing director of the Institute of Microbiology and Epizootics, Freie Universität, Berlin, head of the Green Paper working group on epidemics.

EXPERT ADVISERS:

Prof. Dr med. Hans Anton **Adams**, head of the staff office for interdisciplinary emergency and disaster medicine, Hannover Medical School.

Lieutenant Colonel (General Staff) Frank **Baumgard** (graduate engineer), responsible for civilian-military cooperation at the Federal Ministry of Defence, Armed Forces Staff (Fü S IV 3).

Dr med. Walter **Biederbick**, director and professor, head of the Federal Information Centre for Biological Safety, Robert Koch Institute.

Albrecht **Broemme**, President of the Federal Agency for Technical Relief (THW).

Jochen U. **Budde** (graduate engineer) Deutsche Telekom AG, head of the liaison office Nord.

Axel **Dechamps**, chairman of Working Group V of the Standing Conference of the Ministers and Senators of the Interior of the Länder, civil protection, fire service issues, emergency services, civil defence; member of Working Group of the Standing Conference of the Ministers and Senators of the Interior of the Länder II, internal security, Standing Conference of the Ministers and Senators of the Interior of the Länder, head of the public safety and order department, of the Berlin senate.

Authors marked with an * are members of the FORUM ON THE FUTURE OF PUBLIC SAFETY AND SECURITY steering group.

Dr Uwe **Fischer**, Federal Ministry of the Interior, Division G II 1/ international developments; analysis and evaluation.

Jochen **Grimmelt**, head of civil emergency preparedness for Deutsche Bahn Sicherheit (German railway security) GmbH, a subsidiary of Deutsche Bahn AG.

Sven **Jarmuth**, vice president of the medical disaster aid organisation MHW.

Frank **Jörres**, First Aid team leader, rescue service, disaster protection, National Secretariat, German Red Cross.

Rudolf **Kögel**, Head of Special Business Development Programs, EADS Defence Electronics.

Manfred **Kuntz** (graduate engineer), Key Account Manager, Fire Services, opinion leader and lobbyist, Dräger Safety AG & Co. KGaA.

Jörg **Marks** (graduate engineer), Head of Department, Eastern Region, Siemens Building Technologies GmbH & Co.oHG, Berlin.

Professor Dr Sachar **Paulus**, honorary professor for Security Management, head of the competence centre for security and safety (KomSiB), Brandenburg University of Applied Sciences.

Dirk **Reinermann**, department for critical infrastructures and IT security review, Federal Office for Information Security (BSI).

Frank **Sauer** (graduate political scientist), research assistant at the Institute for Political Science, Bundeswehr University Munich; doctoral student at the Goethe University, Frankfurt am Main.

Professor Harald **Schaub**, head of department and professor of psychology, IABG, Ottobrunn and Otto Friedrich University, Bamberg.

Professor Jochen **Schiller** (graduate engineer), Vice-president, Freie Universität, Berlin.

Dr Volker **Zurwehn**, deputy head of the Fraunhofer ISST (Institute for Software and Systems Technology).

Heiner **Wegesin**, head of international terrorism and organised crime department, Federal Intelligence Service (BND).

Professor Dr Friedemann **Wenzel**, Center for Disaster Management and Risk Reduction Technology (CEDIM), Geophysical Institute, University of Karlsruhe.

Dirk **Würger**, head of the working group on crisis management, civil and disaster protection, Senate Department for the Interior and Sport, Berlin.

Special thanks for the cooperation and the valuable contributions to the conferences FORUM FOR THE FUTURE OF PUBLIC SAFETY AND SECURITY to:

Peter **Altmaier**, Parliamentary State Secretary of the Federal Ministry of the Interior and Member of the German Bundestag.

Roland **Bombardella**, Haut-Commissaire, Haut-Commissariat à la Protection Nationale, Luxembourg.

Pia **Bucella**, director, European Commission, Environment DG, Directorate A – Communication, Legal Affairs and Civil Protection.

Christopher **Bunting**, Secretary General, International Risk Governance Council, Geneva, Switzerland.

Fred **Chiacharella**, head of the committee for business management and information technology, German Insurance Association (GDV).

Dr Markus **Dürig**, head of Division IT 3: Information Security, Federal Ministry of the Interior.

Christoph **Flury**, lic.phil., head of planning and coordination, member of the management board, Federal Office for Civil Protection (FOCP), Switzerland.

Michael von **Foerster**, Head of Association Governmental and Public Affairs, Bosch Sicherheitssysteme, vice chairman of the product division Security Systems, German Electrical and Electronic Manufacturers Association (ZVEI).

Dr Markus **Hellenthal**, Senior Vice President, CEO, Thales Deutschland.

Prof. Dr. Peter **Höppe**, Head of the geological risk research department at the Climate Centre Münchener Rückversicherungs-Gesellschaft AG.

Waldemar **Kindler**, State Chief of Police, head of Department IC, Public Safety and Order, Bavarian Ministry of the Interior; chairman of Working Group II, internal security, Standing Conference of the Ministers and Senators of the Interior of the Länder.

Professor Dr Hans-Jürgen **Lange**, Witten/Herdecke University, Faculty for Studium Fundamentale, Chair of Political Science, safety/security research and management.

Fire Services Officer Dieter **Oberndörfer**, head of department, Frankfurt Institute for emergency medicine and emergency care, Fire Authority, Frankfurt am Main.

Karl-Andreas **Moll**, Corporate Business Development, 3M Deutschland GmbH.

K. John **Pournoor**, MBA, Ph.D., International Government Executive, National Infrastructure, Public Health, Safety, Security and Defense, 3M Company - Government Markets & Public Affairs, USA.

Oliver-Patrick **Rodewald**, head of department, International Assistance and disaster relief, Johanner Emergency Service (JUH) e.V.

Bernhard **Schneck**, Managing Director, GeNUA Gesellschaft für Netzwerk- und Unix-Administration mbH, a German IT security specialist company.

Joachim **Steig**, Country Vice President Business Development, Thales Germany, head of ministry department (rtd).

Christoph **Unger**, President, Federal Office of Civil Protection and Disaster Assistance (BBK).

01

1. INTRODUCTION

Recent decades have seen profound changes in the security environment of individuals and society, resulting in new risks and threats which are perceived in very different ways. The issues of terrorism and violent crime arouse reactions of distrust, fear and even panic in the population and the media, while possible risks of a breakdown in infrastructure and organised crime are rarely mentioned, tending to be ignored or underestimated.

A constant flood of technological innovation, a high level of security and safety in everyday life, the permanent availability of means of communication which we now take for granted and high standards of justice: all these factors contribute to a feeling of security. In fact, however, vulnerability to less obvious, gradually developing risks and the chain reaction of crises is actually rising. These risks include the increasing and all-encompassing dependency on infrastructure such as the electricity supply, the spread of transnational underground economies and the increased likelihood of pandemics, promoted by climate change and high levels of mobility for goods and people.

1.1 NEW CHALLENGES

Policymakers, the economy and society must face up to new challenges, assess the changing risks and find strategies of crisis management. This will involve more than merely extending the current legal regulations on civil protection and the prescribed measures to be taken by the various responsible bodies. Fundamental decisions must be taken; we need an entirely new concept of risk management and crisis response. Germany cannot afford a large-scale disaster, perhaps even affecting the whole Federal Republic and lasting days or even weeks, especially if the official response is chaotic and the situation only partially brought under control. Such an event could not only result in human tragedy and serious economic losses, but could also lead to long-term loss of confidence in the state's ability to organise our national community. The consequences for our society would be incalculable.

So far, there is universal agreement only on the fact that the risks and threats have changed fundamentally. However, many key questions in the face of the new level of risks remain unanswered.

1.2 AIMS OF THE GREEN PAPER

With this Green Paper, the FORUM ON THE FUTURE OF PUBLIC SAFETY AND SECURITY aims to initiate public debate across party boundaries. The Green Paper illustrates the changed conditions of public security, above and beyond day-to-day politics. Central scenarios based on these changes have been developed by leading experts from many fields of public life such as politics, risk aversion, administration, science, industry, expert associations and aid organisations. The types of scenario and their interdependence pose entirely new challenges. The Green Paper and so the FORUM ON THE FUTURE OF PUBLIC SAFETY AND SECURITY are unusual in providing a common platform for the different experiences and positions of specialists who otherwise rarely work together.

The primary aim of the Green Paper is to increase public awareness of the risks and future challenges and tasks. Decision-makers will not be able to react appropriately to ensure the safety of the people until the dangers facing Germany can be assessed more accurately. This presentation of new or previously disregarded interrelationships is intended to stimulate a public debate based on facts and not guided by particular interests. The Green Paper contains important starting points for the direction of future political decisions – but without presenting political solutions.

The Green Paper constitutes an invitation to all those who are reflecting on these questions to take part in the debate.

So far, there is universal agreement only on the fact that the risks and threats have changed fundamentally.

1.3 THE CHANGED SECURITY ENVIRONMENT

The end of the East-West conflict and the dissolution of the bi-polar world order around twenty years ago have resulted in the emergence of a completely different security environment. The burgeoning hopes of a “peace dividend” soon proved illusory, despite the fact that, for Germany, the threat by an all-out territorial war has become unlikely.

Instead, new risks and threats have arisen:

- **International terrorism:** Asymmetric warfare and the new vulnerability of modern industrial societies have altered the previously static security situation. Transnational factors are now the primary threat, rather than interstate conflicts. This has blurred the line between internal and external security, increasingly restricting nation states’ capacity to act. Yet the question of whether terrorism can be classed as war in international law remains highly controversial. Experience abroad has shown that the attempt to combat terrorism by purely military means is doomed to failure. Terrorism has multiple causes and manifestations which cannot be adequately dealt with merely by the traditional police methods of prevention and repression. There is a general trend towards an increase of external determinants. Potential threats and (security) interests must therefore be newly defined.
- **Transnational organised crime:** The classical fields of activity of organised crime are drugs, human trafficking, the illegal arms trade, protection rackets, kidnapping, organised theft of extremely valuable items, property offences, economic crime, internet fraud etc., carried out on a world-wide scale and in a highly professional manner. Organised crime is closely connected with terrorism; indeed it is its main source of finance. At the same time, there are no clear boundaries between organised crime and economic crime such as money laundering and tax and customs fraud.
- **Climate change and its consequences:** Experts predict an increasing number of extreme weather events such as torrential rain or long heat waves in certain regions of Germany. These can cause enormous amounts of material damage and result in health hazards. Gradual climatic changes can already be observed and this will probably increase in intensity towards the end of the century.
- **The information society:** Technical dependence on so-called critical infrastructure has now penetrated all aspects of life. The spread of information and communications technology makes society vulnerable in new ways. Electronic infrastructure, without which hardly anything works these days, is particularly vulnerable. The high degree of interconnectedness means that even small faults, technical failure, human error or a single case of sabotage could result in domino or cascade effects. At worst, whole systems can collapse.
- **Infectious diseases:** As a result of the increasing mobility of goods and people, infectious diseases can spread around the globe rapidly and trigger an epidemic or pandemic. Climate change enables pathogens and their vectors to colonise new regions permanently. It is extremely doubtful whether essential infrastructure could continue to operate in case of high rates of infection.
- **Privatisation of the provision of essential community services:** Infrastructure and services in public hands or with a public majority are increasingly rare. Large areas of services have been privatised or are organised under private law. Companies are subject to competition and the control of private owners. Economic necessity does not automatically correspond to overriding security requirements and leads to new challenges, including the creation of a suitable legal framework and appropriate communications.

Technical dependence on so-called critical infrastructure has now penetrated all aspects of life

1.4 GLOBALISATION HARBOURS NEW RISKS

The changes in the security environment are closely connected to globalisation. This process started before the political changes mentioned above and is still ongoing: globalisation is considered to be the biggest megatrend up to 2020 as the interdependence of different societies will continue to increase. The full impact of globalisation has not yet been adequately understood. The new risks and threats described above must therefore be seen in a context of developments which at present hardly seem to apply to the Federal Republic of Germany and which are therefore scarcely consciously perceived.

As a result of globalisation, the following trends will be among those to increase:

- Erosion of the forms of political order and responsibility in (nation) states and reorganisation into new structures,
- Global movement of goods and capital,
- Exchange of information and knowledge,
- Urbanisation,
- Migration (caused by climate change, scarcity of resources and the globalisation of the labour market).

1.5 PLAYERS INVOLVED IN PUBLIC SAFETY AND SECURITY

The traditional players involved in public safety and security are the organisations and authorities relating to police and non-police risk aversion bodies (polizeiliche und nicht polizeiliche Gefahrenabwehr). Police risk aversion bodies include:

- Federal and Länder police forces
- Federal and Länder Offices for the Protection of the Constitution
- The Federal Intelligence Service (BND)
- Military Counterintelligence (MAD)

Non-police bodies include:

- The fire services
- The Federal Agency for Technical Relief (THW)
- Recognised private aid agencies such as the Workers Samaritan Federation (ASB e.V.), the German Lifeguard Association (DLRG e.V.), the German Red Cross (DRK), the Johanniter Emergency Service (JUH e.V.) and the Maltese Cross

Relief Service (MHD e.V.)

- The Federal Office of Civil Protection and Disaster Assistance (BBK)
- The authorities responsible for law and order and disaster relief in municipalities and the Länder
- The Bundeswehr, which may be called on as a subsidiary support under Article 35 of the Basic Law of the Federal Republic of Germany.

Taking the new risks and threats mentioned above as a starting point, the circle of players involved is extended. We refer to the list of participants in the LÜKEX "Pandemic" exercise held in 2007 by the Federal Office of Civil Protection and Disaster Assistance (BBK); the list is not exhaustive, but includes:

- the Robert Koch Institute
- the Friedrich Löffler Institute
- the Federal Institute for Drugs and Medical Devices (BfArM)
- the Paul-Ehrlich-Institute
- the Federal Office for Agriculture and Food
- the Chambers of Physicians
- charities
- hospitals
- rest homes and nursing homes
- the Federal Office for Information Security
- the Federal Railway Authority
- the Deutsche Bahn AG,
- the Federal Labour Court
- the Federal Aviation Office
- the Federal Waterways and Shipping Administration
- the German Meteorological Service (DWD)
- the Bundesbank
- airport operators
- the media.

The private sector of the economy must also be regarded as an increasingly important player, due to its role in taking on significant tasks in the public safety realm and due to the fact that it is also confronted with the new risks as a potential victim. This applies in particular to commercial and service companies in transport, logistics and communications, to finance and insurance companies, suppliers of food and energy, waste disposal companies and a wide range of health care and security services.

The changes in the security environment are closely connected to globalisation

Many infrastructure services which were formerly state or publicly owned are now privatised or about to be so. An estimated three quarters of providers for infrastructure, vital to society, public safety and order are now in private hands. The state only has limited influence on these companies. Hospitals are now owned and operated by municipalities, town councils, districts and non-governmental sponsors as well as private companies. This results in a variety of legal obligations and decision-making authorities.

Finally, the people themselves must be mentioned as a decisive player. They are, after all, the justification, the reason and financier for the state's risk and crisis management – and they can make a vital contribution to crisis prevention and management.

The fact that there are so many players involved has both advantages and disadvantages. On the one hand, they provide a copious source of ideas and creativity. Responsibility allotted on the basis of the subsidiarity principle ensures that solutions are tailored to suit local requirements, in a way which centralised structures could not achieve. On the other hand, information, communications and coordination structures must be very well organised in view of the large number of players. Expanding risk and crisis communication between all participants – including the citizens – is therefore particularly important for successful crisis management.

2. BASIC PRINCIPLES IN DRAWING UP THE SCENARIOS

The FORUM ON THE FUTURE OF PUBLIC SAFETY AND SECURITY has brought together the experience and expertise of science, business, politics and administration. Together, representatives from these fields discuss the changed conditions of public safety and security, define the requirements which derive from these changes and can then anticipate future adjustments.

2.1 ASSUMPTIONS AND METHODS

In view of the complexity of the problem, appropriate methods and processes of knowledge gain and presentation are required. The participants in the FORUM ON THE FUTURE OF PUBLIC SAFETY AND SECURITY are agreed that the physical and political existence of the Federal Republic of Germany could only be threatened or destroyed by a single event in exceptional circumstances, for example a meteorite or comet impact. A national emergency threatening the state's existence is far more likely to arise from the interplay of several negative events. A domino effect would lead to an interaction of natural, technological, social and economic factors, so the disaster could take very different courses, depending on the mix of factors and their dynamics.

Constructing scenarios jointly

The authors of the Green Paper have selected plausible courses of disaster from the infinite number of possible threats, deriving two key scenarios: (1) power cuts and (2) an epidemic in Germany. The Delphi method was applied in this process, using feedback loops and involving additional experts. The authors also chose to also present the threat posed to safety and security by terrorism and organised crime. In this context, three possible scenarios are outlined below. They are presented in detail in the digital appendix at www.zukunftsforum-oeffentliche-sicherheit.de (in German language only).

The key scenarios have been selected to provide examples of how possible threats might develop, enabling the future tasks of "public safety and

security" to be defined. Further explanations, definitions and more detailed background presentations are provided to enable the reader to follow the selection and clarification processes of the Forum members. More detailed texts on this can also be found in the digital appendix in German.

In principle it is important to remember that the scenarios are "stories": though plausible, consistent and possible, they will not necessarily take place. These imagined courses of events make it possible to picture future events at all in the first place. Scenarios are a method of making concrete predictions and are not intended to reflect what is most likely to happen.

2.2 DEFINITIONS AND AIMS

Public safety and security comprises the protection of society from negative effects in the widest sense. The definitions are derived from police and regulatory law and from the endeavour to establish a legal framework and certainty for the well-being of the whole population.

Internal security and national security as well as specific areas such as social security developed as nation states were founded. Although the terms internal security and public safety and security are often used synonymously, their meaning and implications are not identical. Public safety and security is an umbrella term which includes internal security. Internal security refers above all to the boundaries of the community within which the state is to carry out its protective function. Public safety and security, on the other hand, centres on the maintenance of the structures and functions of a society. This interpretation is also expressed in the terms public security and public order, which are often used in German everyday speech.

The initiators of the FORUM ON THE FUTURE OF PUBLIC SAFETY AND SECURITY and the authors of the Green Paper have therefore settled on the following interpretation of public safety and security: providing for the safety and protection of all

the people living in the human-rights compliant social organisation of the Federal Republic of Germany.

The aim of all security efforts is to avert harm and damage to life and limb, to protect freedom and legally guaranteed property, for each individual. The legal system itself and its institutions and organisations are also to be protected. In sum: to ensure the continued existence of the state.

The objects to be protected are therefore:

- Protection of human life,
- Protection of physical and psychological health (also in the sense of public health),
- Protection of the natural foundations of life,
- Protection of democratic structures and civil liberties,
- Protection of essential institutions of public safety and order,
- Protection of property, assets and cultural assets,
- Protection of essential economic institutions and structures,
- Protection of essential supply and communications structures.

The authors consider the much-used English expression “homeland security”, and even more the German version “Heimatschutz”, popular since the terrorist attacks of 11 September 2001, to be unsuitable for a European understanding of civil society.

What is a disaster?

The expression disaster is usually employed by the general public or the media to express or evoke an emotional reaction to a particular event. The

term has a range of different meanings in the various Länder civil protection laws; in Baden-Württemberg and Saxony Anhalt, for example, it is given a broad definition; in North Rhine-Westphalia it is restricted to an event causing major damage and in other Länder laws, it is not used at all.

The Green Paper uses the term disaster in its original sense to refer to a large-scale, long-term collapse of central public structures, systems and functions, resulting in danger to the objects to be protected as listed above, in part or in whole, due to the fact that large numbers of people are affected or that there is considerable material damage¹. Consequently, disaster response entails: saving, rescuing, protecting, treating, caring, securing and reconstructing in an environment where the structures are no longer functioning or destroyed.

The term disaster is not used to refer to large-scale accidents or incidents such as the railway accident at Eschede or the terrorist attacks on the London Underground. The Länder and local authorities in Germany have a very well organised and equipped system of assistance for such tragic cases. The same applies to the flooding of the rivers Oder (1999) and Elbe (2002), which are usually referred to as disasters. However, in those cases, the functioning of public life and the economy were not affected on a large scale. The affected areas could be supplied from an intact infrastructure, because most of the country was not affected. In fact, resources were mobilised on a large scale. Thus having been sufficient to largely compensate for erratic allocation and malfunctioning supply.

Disaster response entails: saving, rescuing, protecting, treating, caring, securing and reconstructing in an environment where the structures are no longer functioning or destroyed.

¹ This interpretation is largely consistent with the definition in Saxony-Anhalt’s civil protection law (KatSG-LSA) in § 1 (2): “A disaster in the sense of this law is an emergency situation which endangers or damages the life and health of a large number of people or essential services or property on a large scale and which requires the coordinated application of all available personnel and means under joint overall leadership to overcome it.”

3. KEY SCENARIO: "POWER CUT IN GERMANY"

Modern society cannot function without electricity. Almost all technological, administrative and social activities depend on a constant, adequate supply of electricity. This is particularly true of Germany, as one of the leading industrial nations.

3.1 NOTHING WORKS WITHOUT ELECTRICITY

The electricity supply is one of the central aspects of infrastructure for the operation and control of industrial production processes. It ensures that drinking water, food and health services are available. Many means of transport and traffic management systems cannot function without electricity; emergency and rescue services are paralysed. Financial service providers, financial transfers and public administration including national crisis management – nothing can work without electricity.

If this critical infrastructure is incapacitated for a longer period of time, the whole of society is affected. This scenario is realistic, as shown by the Europe-wide blackouts in recent years, for example on 28 September 2003 in Switzerland and Italy, or on 04 November 2006 in Germany, Belgium, France, Italy and Spain. One of the most serious power cuts ever to occur in Germany began on 25 November 2005 in Münsterland and lasted several days.

"Power cut" can be regarded as a key scenario because other critical infrastructure elements are directly dependent on the power supply. For example, telecommunications and information technology would soon be seriously affected, just as if they had been directly hit. The corresponding consequences must therefore also be taken into account in this scenario.

BACKGROUND

Modern information and communications technology opens up new areas of vulnerability

Information and communications technology (ICT) has changed society and created innovations. The merging of communications and information technology is the decisive factor. This convergence has produced completely new types of services. The widespread use of information and communications technology and global interconnectedness through the world-wide web have made processes more efficient and provided access to new busi-

ness areas. In some industries such as telecommunications and finance, ICT is almost the only means of operation. ICT is an element of critical infrastructure.

ICT is everywhere

ICT can be used in many ways even in private households: consumers have access to telephone services, the internet and television via broadband connections². New applications are constantly being developed in other areas as well, car electronics being a good example. Originally they supported existing functions, such as power stee-

² The product range is extensive: more information is available, for example, on the website www.breitbandatlas.de [German language website]. Technologies offered include DSL, cable, radio, satellite, electricity cable, fibre optic cable, UMTS, WLAN hotspots and, coming soon, WiMAX.

BACKGROUND

ring or anti-lock braking systems. Now car electronics include extra features which go far beyond mere driving: for example, they announce that an inspection is due, automatically coordinate appointments at the workshop or protect against theft with radio chips.

Other fields of application for ICT are also emerging beyond its "traditional" applications:

- Logistics systems enable branch stores in the retail trade to be supplied on demand. Modern till systems no longer simply add up the bill: they also update stock records and initiate ordering.
- ICT applications in hospitals range from administration through logistics and supplies to actual medical technology and supervision of patients in intensive care. The introduction of telematics, for example in the health insurance cards, will change the health system by linking all players – doctors, hospitals, pharmacies, health professionals, health insurance funds – in one network beyond the boundaries of individual institutions.
- Critical infrastructure is also highly dependent on ICT, including energy and water supply and waste water disposal. The complex processes of transport systems, such as airport management, coordination of fleets of freight vehicles or control of rail traffic also require comprehensive ICT operations. This also applies to the control of power stations and supply networks and for the location and repair of faults.
- Internet access makes a wide variety of information, entertainment and shopping services available to the user as well as giving access to e-government facilities at Federal, Länder and district level.

Dependency on ICT and possible consequences

Disruptions to ICT systems have immediate effects on the processes and services they support. Administration in public authorities and companies is affected and so is production. Malfunctions in one area can also have direct or indirect effects on other areas.

Organisations responsible for crisis management (public authorities, organisations with security responsibilities, aid services) make use of ICT. In a crisis, especially, their ability to act, depends on the necessary technology being available and reliable. For example, with modern control centre technology fewer centres are needed, because they can control operations over a large area. Operations management uses ICT supported executive information systems. Scarce resources are coordinated using ICT throughout the whole Federal Republic, for example the closed internet platform deNIS II plus, the German Joint Information and Situation Centre (GMLZ) at the Federal Office of Civil Protection and Disaster Assistance (BBK) and the regional DISMA system. Today's crisis management depends for its very workings on a continuous and reliable availability of ICT.

Weak points and threats

The Year 2000 problem (Y2K) clearly showed that even if the problem is known in advance, it is difficult to locate and rectify weak points in ICT completely. This event made the wider public aware for the first time of the extent to which ICT has penetrated all areas of society. Y2K was an isolated problem, recognised early. Now, thousands of weak points³ in computer programmes are identified annually. Some permit malicious

BACKGROUND

players to control the affected system completely via the internet. Others have a negative effect on the system directly⁴. Weak points like these do not just exist in standard computers but also in central components of data processing centres, process control technology and the internet.

These circumstances make computer systems an inviting target for criminal hackers in particular. Nowadays it is no longer young "script kiddies" or "normal" hackers who are responsible for the majority of attacks; the attackers are mostly professional. For example, they can use malware to take over a large number of poorly protected computers, link them in so-called botnets and offer them on the black market. A spectacular instance of this type of operation was the botnet attack on Estonia in April 2007. For weeks, the ICT infrastructure of banks, public authorities and the stock market was not just affected; parts of it actually collapsed. The source of the attack has still not been identified though organised crime, political activists and secret service activities have all been suspected.

Poorly protected home computers are not the only targets of organised attacks. Much more extensive damage is caused when corporate computers and so-called application servers are targeted. For example, the multi-billion-euro scandal at the French bank Société Générale in 2007 was caused by defective access rights management: Jérôme Kerviel, a stock broker employed by the bank, evidently had access to transaction options to which he was not entitled.

Corporate infrastructure is also targeted by so-called social engineering, the acquisition of confidential data by social manipulation. Most attackers in this field do not intend to cause the total

breakdown of information infrastructure; their intentions are more likely to be undetected personal enrichment or industrial espionage.

Future prospects

Extensive damage in ICT can be caused at relatively little effort and expense, as the internet attack on Estonia in April 2007 showed. Incidents of deliberate interference, both with terrorist and criminal motivations, are predicted to increase. Organised crime has recognised that IT attacks are profitable, meaning that increased activity and new methods of attack are to be expected in the next few years [see: Terrorism and organised crime, p. 28].

Levels of fault tolerance and security against attacks in the dominant systems in the economy and the administration are not satisfactory. It is already conceivable today that stock exchange computers and thus an entire financial centre could be paralysed, or that the process control technology of energy suppliers could be put out of action.

The level of dependency on ICT will continue to rise in the next few years, making malfunctions – especially of critical processes – increasingly less tolerable. At the same time, the ICT architecture used is becoming increasingly complex, making it even more vulnerable to faults and malfunctions. The challenge for coming decades will be to develop software, hardware and ICT architecture in such a way that they become, or remain, a reliable instrument of process support. At the same time, it is vital to ensure that ICT is able to continue functioning in spite of faults. Increased use of back-up systems might be necessary to achieve this. In addition, it is worth to consider to reactivate old proprietary technologies step by step if necessary.

³ Weak points usually occur when programming software, or designing and manufacturing hardware. However they then need to be identified which can take years.

⁴ For example, a software fault caused loss of control of the Ariane 5 rocket on 04 June 1996, making it necessary to blow it up.

3.2 BASIC ASSUMPTIONS

Electrical energy can only be stored in small quantities. In principle, it must be generated at the same moment as it is used and vice versa. When power stations unexpectedly go off-line, the supply network is interrupted at one point or the network control malfunctions, severe voltage fluctuations arise within seconds. If these fluctuations are not compensated immediately, a domino effect occurs and the power network collapses. The larger and more widespread the damage, the more difficult it is to restart the delicate balance of electricity generation and usage.

The starting point for the scenario is a power cut lasting several days or weeks, affecting several regions and caused by a serious malfunction in the German control areas. Emergency generators can only function part of the time, due to shortages in the fuel supply.

The "power cut" scenario would affect the whole country. The likelihood of such an event occurring in the medium or short term is strong. The risks entailed for the population, the state and the economy are high. A blackout on this scale would cause widespread damage, both direct material damage and follow-on effects such as supply breakdown and interruptions to deliveries. On current assessment scales, losses must be in the two-digit billion euro range to classify as disastrous. Losses would quickly amount to this sum if, for example, many large industrial enterprises and the financial sector are affected on a large scale. Power cuts also cause serious non-material damage, for example through a loss of confidence in the state and the economy.

The longer a power cut lasts, the more other electricity-dependent infrastructure elements collapse. It becomes more difficult if not impossible to restart sensitive technical installations. For example, a sudden power cut which cannot be sufficiently compensated by emergency generation can cause a blast furnace to overheat, leading to melt-down and fire. But even if the blackout can be

overcome without damage, it takes hours or days to restart production. In any case, production loss lasts longer than the event itself.

At present one can only make assumptions based on actual events on the level of damage caused by power cuts lasting days or weeks and affecting several regions.

- The one-day power cut on 14 August 2003 over the whole north-west of the US caused economic losses of between \$7 billion and \$10 billion⁵.
- The blackout lasting several days in thinly-populated Münsterland (Germany) in 2005 caused estimated losses of €130 million.
- An earthquake in Taiwan in 1999 which killed around 2,000 people also caused power cuts lasting up to three weeks in places. Among other effects, the industrial park Hsinchu, the heart of Taiwanese IT production, was completely cut off from the electricity supply. The earthquake did not destroy a single building there, but the power cut caused losses of €162 million. The primary damage due to the destruction of the electricity distribution installations was €2 million. Over all, the secondary damage, caused by loss of production, job losses and the partial collapse of some transport systems, was around 500 times the amount of the primary damage.
- An Austrian study in 2005 which calculated the economic costs of a one-hour nation-wide power cut concluded that each kilowatt-hour that is not supplied would cost six to ten times the price of the electricity.⁶

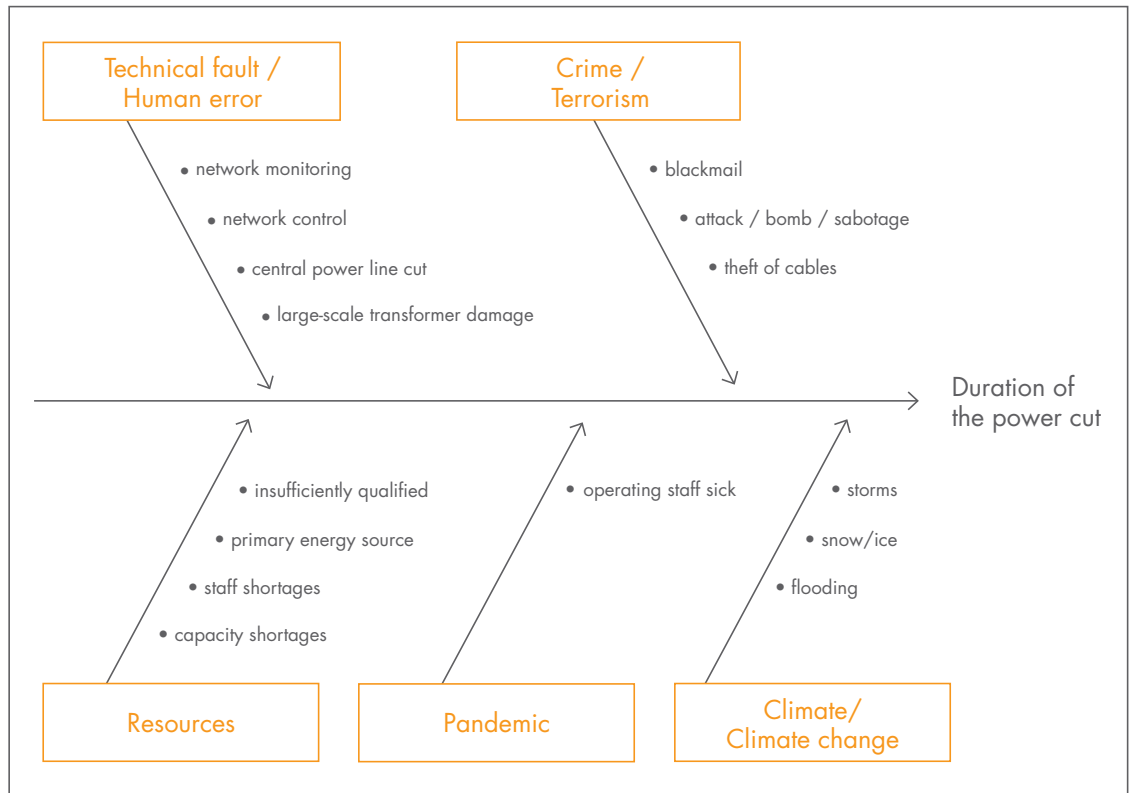
The "power cut" scenario would affect the whole country. The likelihood of such an event occurring in the medium or short term is strong.

⁵ Bansari Saha, Bill Moddy, The Economic Cost of the Blackout, An issue paper on the Northeastern Blackout, August 14, 2003, ICF-Consulting, Fairfax, USA.

⁶ Markus Bliem, Ein makroökonomischer Bewertungsansatz zu den Kosten eines Stromausfalls im österreichischen Versorgungsnetz [A macro-economic approach to evaluating the costs of a power cut in the Austrian supply network], IHSK DISCUSSION PAPER, 02/2005.

3.3 MANY POSSIBLE TRIGGERS

There are many possible causes for a long-term power cut affecting several regions:



Technical failure or human error can lead to cross-border blackouts.

Technical failure or human error can disrupt network control and monitoring processes and lead to cross-border blackouts. Problems in the control technology could also disrupt these processes and cause power cuts.

One example: On 4 November 2006, the power lines in Emsland, North Germany, were switched off in a planned action to permit a new cruise liner to pass safely from a dockyard in Papenburg along the River Ems to reach the North Sea. The result: An unforeseen chain reaction resulted in about ten million people in various regions of Europe losing power for ninety minutes. For a short time, it looked as if the event would escalate out of control and cause a long-term blackout throughout Europe.

Vital technical infrastructure in the distribution network could be so thoroughly destroyed or severely disrupted through criminal and/or terrorist activity that the electricity supply could be interrupted for up to several months in the affected areas.

Organised crime is capable of carrying out a variety of criminal activities in a professional manner: it is conceivable that the electricity supply might be targeted [see *Terrorism and organised crime: Information and communications technology and organised crime*, p. 28].

Destruction of technology and scarcity of resources can result in reduction of power station capacity or even its breakdown. One cause can be heat. Climate researchers anticipate a signifi-

cant increase in heat waves in parts of Germany, which can lead to disruption in the cooling water supply, either because the cooling water temperature is raised or because of low water levels. For example, during the heat wave in France in summer 2003, several power stations almost had to be switched off.

Severe natural events such as torrential rain, storms or freezing rain can also cause widespread power cuts, as happened in Münsterland on 25 November 2005. Temperatures around freezing point, heavy precipitation and storm-force winds resulted in a thick coating of ice settling on the pylons and overhead transmission line conductors. Wind and ice combined to produce the dreaded "power line galloping" effect. Sections of the power lines were switched off automatically for short periods and longer power cuts also ensued. The result: 250,000 people were without electricity for several days [see Background: Climate, p. 37].

Extremely high rates of illness resulting from a serious influenza epidemic can also lead to power cuts. 30 to 50% sickness rates would cause huge absences in the workforce. The situation would become worse because some people would stay at home to care for sick relatives [see Background: Influenza pandemic, p. 33].

The simultaneous occurrence of two or more events would be particularly critical. It is quite possible, for example, that a severe blizzard could take place during an influenza pandemic; after all, both events tend to happen more frequently during the late winter period. Serious staff shortages

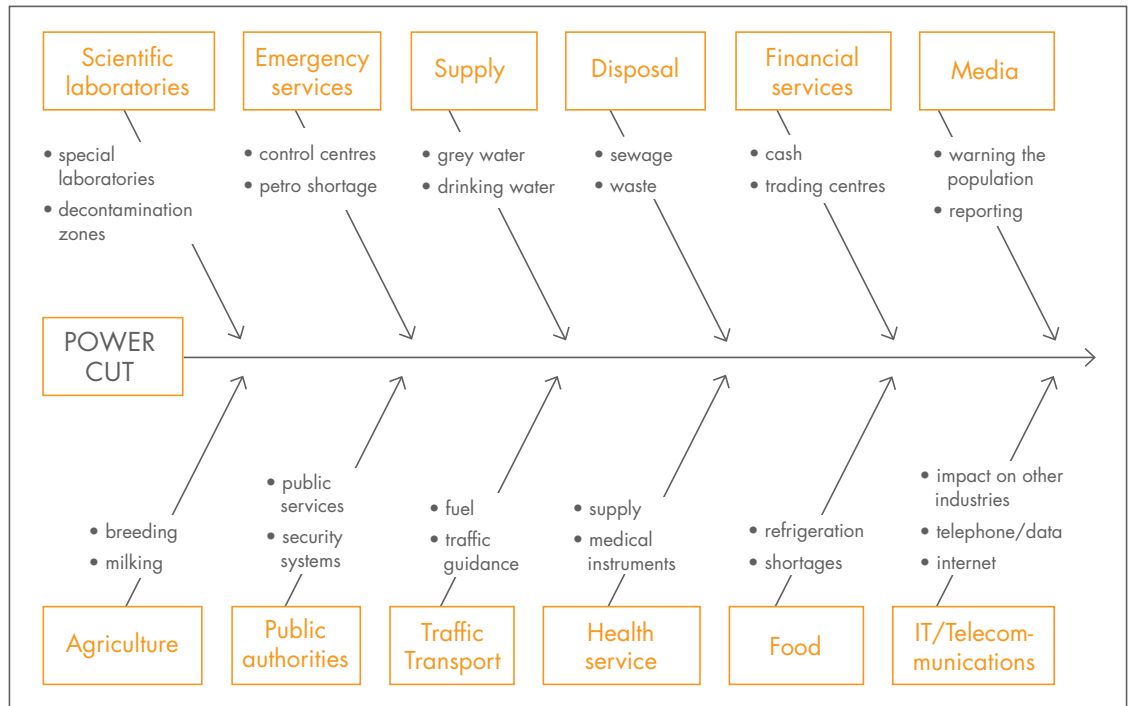
would then coincide with an emergency requiring the deployment of all personnel to cope with it. Under such circumstances, several large power stations may have to be switched off, depending on the extent to which the transmission network is affected. This would result in power cuts throughout Europe's power network and at worst, a blackout over the whole continent.

This scenario does not cover potential foreign trade problems resulting from Germany's increasing dependence on primary energy sources (oil, gas, uranium). The possibility of violent conflict in regions where oil or natural gas are found or through which they are transported is not included either. Problems in network stability are also excluded from detailed consideration. Network stability can be endangered by the dynamic load of the network, which can be caused, for example, by switching on and off large offshore wind power stations. Because these tend to be installed in weakly populated and scarcely industrialized areas, sufficient capacity to transfer large amounts of electricity to other regions is required. Present capacity is too limited to cope adequately with the demand. Increasing demands on the network due to further liberalisation of the electricity market and intensive electricity trading throughout Europe are not examined here. The same applies to the topic of nuclear power. At this point we merely want to point out that at present, Germany still has sufficient energy-generating capacity (power stations) of its own. If cut off from the European network by a malfunction, Germany could still supply its own needs.

Severe natural events can also cause widespread power cuts.

3.4 EFFECTS OF A POWER CUT

The effects of a large-scale power cut lasting several days on a modern technology-based society are serious and complex. Every part of society and all its players would be affected.



Even services where the dependency on electricity is not obvious at first will be affected relatively quickly, making them available in only limited form or not at all.

Massive consequences for all elements of critical infrastructure are inevitable due to their dependency on electricity. The following are particularly affected:

- Information and communications technology (ICT),
- transport and traffic, including all carriers,
- industry and manufacturing,
- the health service, including emergency and rescue services,
- the fresh and grey water supply,
- food supplies, including transport logistics,
- disposal of sewage, normal and hazardous waste,
- public authorities and administration,
- banks and financial systems, including the cash supply,
- (large) research centres,
- the media,
- energy generation and supply.

Even services where the dependency on electricity is not obvious at first will be affected relatively quickly, making them available in only limited form or not at all. This applies for example to the water supply and sewage disposal, which depend on electrical pumping systems and electronic management, control and monitoring systems. Banks and financial institutions will also be affected. Furthermore electricity is vital for cash machines, electronic till systems, electronic payment systems and international security trading. The manufacturing industry is forced to reduce or cease production during power cuts. In some sectors, the unplanned and uncontrolled reduction or shut down of processes can cause direct physical damage.

The enormous range of intra- and interdependencies in the event of a power cut in individual sectors and industries has not yet been thoroughly investigated, so we must assume that further unforeseen consequences will ensue.

Effects on the population

People will feel the effects in every aspect of their lives; the effects on basic supplies, family life and leisure time will impact their private lives, and consequences at work and in relation to services will be immediate and drastic. The most severe direct effects will be loss of heating in winter or cooling in summer, electric light, telephone, internet, radio and TV reception, food storage in fridges and freezers and possibly the lack of drinking water. The disposal of faeces by flushing the toilet may no longer function. Within a short time, high-rise buildings, for example, would have to be completely evacuated because of the danger of disease, meaning that an enormous amount of emergency accommodation would be required. This will be a particular problem in urban areas.

The failure of vital information and communication systems will cause uncertainty. Fear and panic will spread through the population.

Public transport will only be available in very limited form, if at all. The same applies to local and long-distance rail transport. Private transport in cities will also come to a standstill because traffic lights and street lighting will not work and in the medium term, it might be restricted by fuel shortages.

Shops will stay closed because the tills are not working, there is no lighting, heating or cooling and the electric doors are not working. Computer-controlled logistic systems operating on the just-in-time principle will fail, so local stocks will soon be used up and shortages of every-day goods, especially food, will arise. If the authorities do not provide sufficient support, people will find their own ways of supplying their needs by methods which will not necessarily be legal.

In urban areas with a high population density, people's ability to help themselves will probably be less than in the country. On the other hand, the capabilities of public assistance are higher in the city. However, it is conceivable that people might flee to more self-sufficient rural areas - if transport is available.

Effects on public authorities, emergency services and police risk aversion

Public authorities, emergency and rescue services and the police forces are themselves elements of critical infrastructure and extremely dependent on electricity supply. Modern control centres which direct emergency warning systems for whole regions, computer-supported executive information systems, crisis management systems, getting an overview of the situation – all these functions are dependent on the availability of electricity for information and communications technology [see Background: Information and communications technology, p.16].

Emergency blackout provision varies greatly according to which public authority is responsible. In most cases, emergency generators will enable the crisis management groups to operate. Whether and to what extent the crisis management groups can call on the administration varies from case to case. The Münsterland power cut showed that the staff available at district level was in part incapable to provide a 24-hour administration and operations team. The availability of means of communication is vital for the coordination of public authorities. It can be assumed that a long-term widespread blackout will disrupt public communications systems – mobile phones, land lines and data networks – on a large scale. To what extent public authorities are provided with alternatives, such as satellite telephones, varies from place to place. At present, no unified standards for the resources and organisation of public crisis management have been implemented. It will be some time before the decision to introduce the new digital radio system for public authorities and organisations involved in security/safety (BOS) is put into practice, making it available in every area and to all relevant players. Even this will only solve a small part of the problem on a purely technical level.

For the new BOS digital radio system it is planned that in case of a power cut, the system will be fed through batteries with a capacity of three hours. After that, an emergency electricity supply needs to be organised.

Public authorities, emergency and rescue services and the police forces are themselves elements of critical infrastructure and extremely dependent on electricity supply.

Out-patient care systems would suffer bottle-necks much earlier than hospitals.

The emergency services would be hit in several ways. First, citizens would not be able to make any emergency calls once the telephone and mobile networks cease to function. Second, emergency services could only be coordinated to the extent that they can fall back on back-up systems of communication, such as the BOS communication system on emergency generators or satellite phones. Fuel shortages due to insufficient emergency electricity at the petrol stations could lead to a breakdown of the emergency transport after two days.

However, it is vital that the security authorities and the authorities responsible for law and order do not cease to function. At the very least, fuel reserves, an adequate emergency electricity supply and a functioning communications network must be available for the police, fire and rescue services.

Effects on public health services

Hospitals have an emergency electricity supply to ensure critical areas including operating theatres, intensive care wards, x-raying and laboratories can continue to function in case of a power cut. How far normal hospital operation is possible and how long the emergency energy supply can be maintained varies from case to case.

Most hospitals have an emergency plan which involves the early discharge of as many patients as possible. However, it will not be possible to implement this in a situation where large-scale power cuts have left patients' homes without light, drinking water, heating, cooling or telephones.

A power cut lasting one or more weeks would affect the following health care structures particularly severely:

- All areas with controlled ventilation systems such as operating theatres and isolation wards would suffer additional basic functional problems.
- Problems would arise due to the breakdown of lifts, making it difficult to move patients, of emergency alarms, cooling systems and heat sterilisation. It will not be possible to maintain the energy-intensive heat sterilisation of medical instruments, so operations could no longer be carried out.
- Diagnosis in laboratories or using image-crea-

ting techniques would break down to a large extent. Only basic diagnosis methods would be possible.

- Specialised units could no longer be relied on; this would include neo-natal intensive care wards or units which require special air controlling systems, such as bone marrow transplant units or special isolation wards, which operate with regulated low-pressure systems to prevent the spread of highly infectious pathogens.
- Hospital laundry services are usually outsourced. The external companies do not have emergency electricity supplies and will cease to function during a blackout.

Health care professionals would try to cope with the situation by improvising and relaxing standards. In some areas of in-patient care this would succeed, but a large-scale power cut would be a serious threat to medical provision especially in intensive care wards. This would affect 21,000 intensive care beds in Germany. There are no substitutes for these complex and sensitive systems and doing without them for a time is not an option. In particular, if ventilation equipment failed, patients would die or suffer serious damage to their health.

Doctor's surgeries and out-patient care

Out-patient care systems would suffer bottle-necks much earlier than hospitals. The usual risk groups would be affected most: babies, small children, the old and the sick.

Doctors' surgeries do not have emergency electricity supplies. Apart from the basic functions, a continuous electricity supply is also required for diagnosis, heat sterilisation and therapeutic treatments. In addition, medical practitioners in private practice will probably only be able to work to a limited extent because patients can not reach them.

Dialysis centres are an example of a particularly electricity-dependent type of out-patient care. Power cuts here could affect tens of thousands of people. The breakdown or limited operation of blood banks would also soon lead to supply problems and after eight weeks, the supply of blood-based products would break down completely. Victims of accidents, tumour patients, etc., would be affected [see Appendix 2.1. "Medical care during power cuts"].

The same applies to welfare centres and other charitable establishments. Nursing homes are particularly badly affected by the breakdown in washing and dishwashing capacity for the equipment essential to care provision. House alarm systems and medical apparatus will not be usable because nursing homes do not usually have a full-scale emergency electricity supply. Private homes with chronically ill patients, for example those requiring home dialysis or breathing apparatus, would suffer particularly in a power cut.

Effects on commerce, trade and industry

Most industrial and commercial companies will close down. In some industries there will be a great deal of damage, for example in certain manufacturing processes where an uncontrolled shut-down can be disastrous.

Large agricultural enterprises will suffer severely under power cuts. Mass animal mortality is to be expected on poultry and pig farms, because without electricity, the animals cannot be supplied with heating, cooling and food. Electric milking machines will not function and there will not be enough staff to milk by hand. The consequences for dairy farming will be a considerable drop in production and the loss of many animals.

The impact on finance and the stock markets will be huge. It is possible that entire trading centres in Germany will close down because many transactions can not be carried out. Public institutions will close if no electric or electronic systems are working: lifts in residential and commercial buildings will not work; department stores and shops must close.

Waste disposal companies will be particularly badly affected. On the one hand, they can no longer function: sewage treatment plants will cease their treatment processes, hazardous waste will no longer be correctly sorted and checked, household waste will no longer be collected and processed. On the other hand, they will be inundated with huge amounts of new waste, for example, frozen goods, particularly meat, which have thawed and spoiled.

Fuel and emergency electricity supplies

Shortages of fuel and emergency generators can arise very quickly. In a survey of oil companies,

one company told us that about 15 of their 2,200 petrol stations across the country were equipped with an emergency electricity supply as standard. The company informed us that if a power cut occurred, the other petrol stations could order emergency generators via an internal logistics service provider. These would be available throughout Germany in a very short time. The question of whether the majority of existing pumping systems are already designed for emergency electricity supplies remains open. It may therefore be necessary to fall back on manual pumps, for which technical apparatus is also necessary [see Appendix 2.2 "Emergency electricity supply for petrol stations"].

Emergency generators and back-up installations are available in a variety of sizes and capacities. Fuel reserves for most of the existing installations cover a period of 12 to 48 hours. In the past, this was sufficient for everyday requirements. There are no general binding federal requirements for the extent of emergency generating capacity for companies and other establishments.

During the power cut in Münsterland, there was a lack of precise information about available resources. In the end, nearly 300 emergency generators of different capacities were used and around 4,000 helpers were deployed.

Shortages of fuel and emergency generators can arise very quickly.

BACKGROUND

Communication influences the course of a crisis

The vital importance of good risk and crisis communication to public security and safety is still underestimated. Communication unfolds on four levels: 1: in advance (preventative), 2: in case of a crisis (reactive), 3: internally, with the players in risk aversion and 4: externally, with the population. The media play a key role here. They can

make crises worse or mitigate them. It is indisputable that inadequate or no communication exacerbates crises. Communication itself can become a scarce resource, for example during a power cut or a failure of information and communications technology. Every other shortage of necessary resources, however, can also lead to the need for additional communication, which have to be provided by the existing facilities.

3.5 SUSTAINABLE RISK AND CRISIS MANAGEMENT

The level of preparation for a "power cut" scenario in Germany is very varied. Many players still assume that a long-term blackout affecting several regions will never occur. Clearly they do not know about or are not really aware of the complexity of a power cut of this type or the intra- and interdependency of elements of the infrastructure. Above all, the residential population in Germany is not prepared for a scenario like this: there are no adequate capacities for self-protection or self-help. Industry and the public authorities also show varying levels of preparedness.

Technical, organisational and planning capabilities would be the first requirements for rapidly getting to grips with a scenario of this kind. It would be necessary to have a precise knowledge of the critical infrastructure so generators could be put into action where they are most needed to supply the minimum necessities for everyday life. These include, first and foremost, communications systems, police, fire services, hospitals, control centres, selected shops, petrol stations and banks. Generators would have to start operating at once in places which have been precisely defined in advance. Supplying the people with food and fuel is one of the greatest challenges for public safety and security in such a crisis.

In the medium term, the electricity supply would need to be reinstated as soon as possible through alternative cable systems, integrated networks and detour circuits. A plan should be set up for this purpose to alert immediately deployable repair teams and technical systems. The electricity companies are responsible for restoring electricity supply. The responsibility for supply by generators, on the other hand, is divided among various players: the fire services, the Federal Agency for Technical Relief (THW), the Bundeswehr, Federal and Länder police forces, aid organisations, industry and commerce. Public safety and order might also be under threat in a blackout. The police must be prepared for looting. It might even be necessary to restrict freedom of movement. Further measures could include closing public institutions such as schools, libraries and some public authorities and the assignment of regional supply centres.

In principle, sustainable risk and crisis management which prioritises prevention is required. Interfaces must be defined: crisis management must be based on the best possible communication structures and include all players. Both risk control and crisis management must progress from a sectoral approach to a process-oriented, all-inclusive approach; they must follow standardised rules and be practised in regular training exercises.

3.6 CONCLUSION

The "power cut" scenario is a key scenario. It is interdependent with other essential elements of infrastructure and affects almost all areas of life and business. If such a long-term, large-scale blackout occurs, it will lead to considerable restrictions for the population and enormous economic damage. The public institutions and private aid organisations would not be able to maintain public safety or meet the population's basic needs.

Germany would become the focus of critical international debate as a business location with a doubtful level of security. At present, there is no perceptible unified risk or crisis management on the part of companies, the government or other players. The level of awareness is low, the population's capacity for self-help limited. A power cut on this scale would be a national disaster with damaging short, medium and long-term consequences for the whole of society.

At present, there is no perceptible unified risk or crisis management on the part of companies, the government or other players. The level of awareness is low, the population's capacity for self-help limited.

4. SECURITY THREATS IN GERMANY FROM TERRORISM AND ORGANISED CRIME

One of the most immediate threats to Germany's security is considered to be international terrorism. This threat is growing. At present, German authorities are working on more than 200 preliminary investigations in cases with an Islamist-terrorist background. In addition, there are proceedings to ban Islamist organisations in Germany such as the "Kalifatstaat" or the already banned Hizb-ut-Tahrir party. These are just the tip of the iceberg in relation to the increasing radicalisation of a growing proportion of Germany's Muslim population.

The public is less aware of organised crime and tends to underestimate the threats it represents, especially through its symbiosis with terrorism. A common definition states that "organised crime is the carrying out of planned crimes which are of considerable significance either individually or taken together, with the aim of gaining power or profit [...]". There are no distinct boundaries between organised crime and economic crime, money laundering and tax evasion. Organised crime is highly professional and often operates internationally. Its preferred methods are conspiracy, corruption and intimidation. Some networks could be called "organised crime on demand": these are often temporary groups which form in response to the "market". Their range is increasingly global and very flexible, and they often act in cyberspace. When the task is completed, these networks often disband and reconvene when required with different members [see Appendix 3.1, "Threats from terrorism and organised crime"].

Terrorism and organised crime are often closely connected with global phenomena which present potential threats to Germany's security. In particular, these include:

- Demographics, illegal migration and integration problems,
- arms proliferation and the increasing build-up of weaponry,
- the collapse of states in parts of Africa and Asia and other regional conflicts,
- conflicts over resources and energy security,
- malfunctions of critical infrastructure,

- natural disasters and the
- changing role of states in a globalised world.

4.1 THE INTERNET: A NEW CHALLENGE

Modern communications technology plays a vital role in worldwide networked asymmetric warfare, both for internal and external communication. The decentralised structure of the internet, lacking a central authority, provides terrorists and organised criminals with a platform for communications, recruitment and propaganda. Terrorists seek to dominate the media and gain worldwide public attention rather than military dominance. So they make intensive use of internet forums and chat rooms, mobile and internet telephony. Sometimes they also deploy modern encryption and concealment tactics.

The internet itself also provides the opportunity to attack the state, the economy and society. For example, botnet attacks and denial-of-service actions can paralyse entire IT systems. An increase in activities like this and new methods must be expected in the coming years [see Background "Information and communication technology", p.16].

4.2 SYMBIOSIS DESPITE DIFFERENT AIMS

International terrorism and organised crime have entirely different motivations and aims. Terrorism of the Al-Qaeda type is politically or ideologically motivated. A core element of the terrorist approach is carrying out spectacular attacks with large numbers of victims, to gain public attention. The aim is to terrify their enemies and to motivate their potential supporters. Organised crime, on the other hand, primarily seeks to maximise profits. It acts in secret, trying to avoid all forms of attention in order to preserve its illegal business; it also attempts to make its activities appear legal. Although their aims are different, organised crime and terrorism have certain similarities in methods and organisation and there are many cross-con-

The public is less aware of organised crime and tends to underestimate the threats it represents, especially through its symbiosis with terrorism.

nections. Terrorists also need to act undercover up to the final point in the chain of their activities, the actual attack. They often use the methods or the established structures and supply networks of organised crime, for example to obtain false identities, money and resources, which are then used to prepare attacks or maintain terrorist structures such as training and indoctrination camps. Alongside donations and profits from legal business, terrorism is financed by trade in drugs, arms and diamonds. And, vice versa, terrorism also supports organised crime: regional conflicts in the Balkans, in the CIS region and in the Middle East have strengthened the structures of organised crime and created new ones. Although, in Germany, the figure for reported crime has recently decreased, unreported criminal offences have probably remained at the same level or even increased.

One possible scenario is that perpetrators defraud an insurance company, then use the money to acquire arms, vehicles, explosives, information and, above all, radioactive material in order to carry out an attack with a dirty bomb. In 2007 Ibrahim Mohamed K., a German resident, was sentenced to seven years in prison for membership of a terrorist organisation and attempted fraud as part of a criminal group in 28 cases. K. and his accomplices planned an insurance fraud with the intention of using the money to finance terrorist attacks. They intended first to take out dozens of life insurance policies for several million euros and then to collect the premiums after a simulated car crash in Egypt [see Appendix 3.2 Scenarios “Terrorism and organised crime”, scenario 1].

4.3 PRECIPITATING AND AGGRAVATING CRISES

International terrorism uses the structures of organised crime as a means of financing its activities. At the same time, organised crime in itself damages society in many ways, largely unnoticed, by giving incentives to corruption and by property and economic crime. Organised crime can trigger crises in the long

term, but it can also use and exacerbate existing crises for its own purposes.

Drug trafficking is the best known field of activity of organised crime and one of the most profitable sectors of the underground economy, with a total global turnover estimated at between \$500 billion and \$800 billion. The social and economic consequences are enormous; in Germany alone they are estimated at €147 billion. Drug trafficking is an important source of income for terrorist and organised crime groups and so contributes indirectly to the financing of covert and asymmetric warfare.

The long and difficult journey of heroin and cocaine from the harvest to the end user, via production, transport and distribution, requires a complex network in terms of organisation, logistics, personnel and information. These illegal structures are also used for other criminal purposes by terrorist groups, who often take a share of the profits and use the logistic capabilities of organised international drug trafficking. This clearly shows the dangerous symbiosis of these two phenomena [see Appendix 3.2 Scenarios “Terrorism and organised crime”, scenario 2].

The illegal structures of drug trafficking also generate corruption, property and economic crime and procurement crime, as well as violent crime in battles for territory. The latter is significantly responsible for increasing the overall crime rate.

Property and economic crime rank second in the list of criminal activities in Germany after drug-related crime. Money laundering, tax and customs fraud (smuggling), forgery and bribery cause the erosion of state structures, not only in fragile states but also in Germany. Trade under false names and the setting up of fake companies, so-called shell companies and, increasingly, e-crime, such as so-called phishing, all come into this category.

Theft of exceptionally valuable or essential goods is another lucrative field of activity for organised crime. The stolen articles are either transported together or concealed individually in a load or store

Organised crime can trigger crises in the long term, but it can also use and exacerbate existing crises for its own purposes.

of legitimate goods. Some well-known examples include well-organised mass theft of sensitive medical technical instruments from doctors' surgeries, of non-ferrous heavy metals, of valuable goods such as electronics and microchips, or of special equipment from building sites.

It is quite plausible that such thefts could result in shortages or worsen an existing shortage. Theft of non-ferrous heavy metals and the resulting damage could be the direct cause of supply breakdowns, for example in communications, rail transport or safety of loads or on building sites. Shortages of medical instruments or theft of vaccines could cause problems or aggravate difficulties in times of crisis [see Scenarios "Power cuts", p. 16, and "Epidemics", p. 32].

Human trafficking is estimated to have a global market volume of \$7 billion. The crime of facilitating the entry of illegal immigrants has increased markedly in recent years. Prostitution is predicted to be one of the growth markets of the future. The lower echelons of drugs cartels are often connected in gangs to organised criminal structures which have prostitution or drug trafficking operations. Hundreds of thousands of illegal immigrants reach western states annually via these structures.

Protection rackets, kidnapping and piracy are linked in many ways to asymmetric conflicts. Organised crime and terrorism in turn fuel the **arms trade**, another important pillar of the illegal economy which is also booming.

Elaborate financial structures, whose complexity and suitability for adaptation to finance terrorism is still underestimated, often lie behind economic crime. Some examples are the founding of companies where the source of capital is questionable, or the import of stolen or embezzled cars and other goods from EU countries. Organised criminals make use of various cover-up activities, shell companies, product piracy and plagiarism. The proceeds and products from these almost industrially organised criminal activities are invested profitably under other names or offered directly to the consumer.

The aim is often to invest illegal profits in the legal economy. After committing their crimes, organised criminals need exchange facilities and the chance to reinvest in luxury goods, in order to conceal their activities and launder their money. It is known that non-participants are encouraged, for example, to use accounts or to buy luxury goods or property in return for a reward [see Appendix 3.2, Scenario "Terrorism and organised crime", scenario 3].

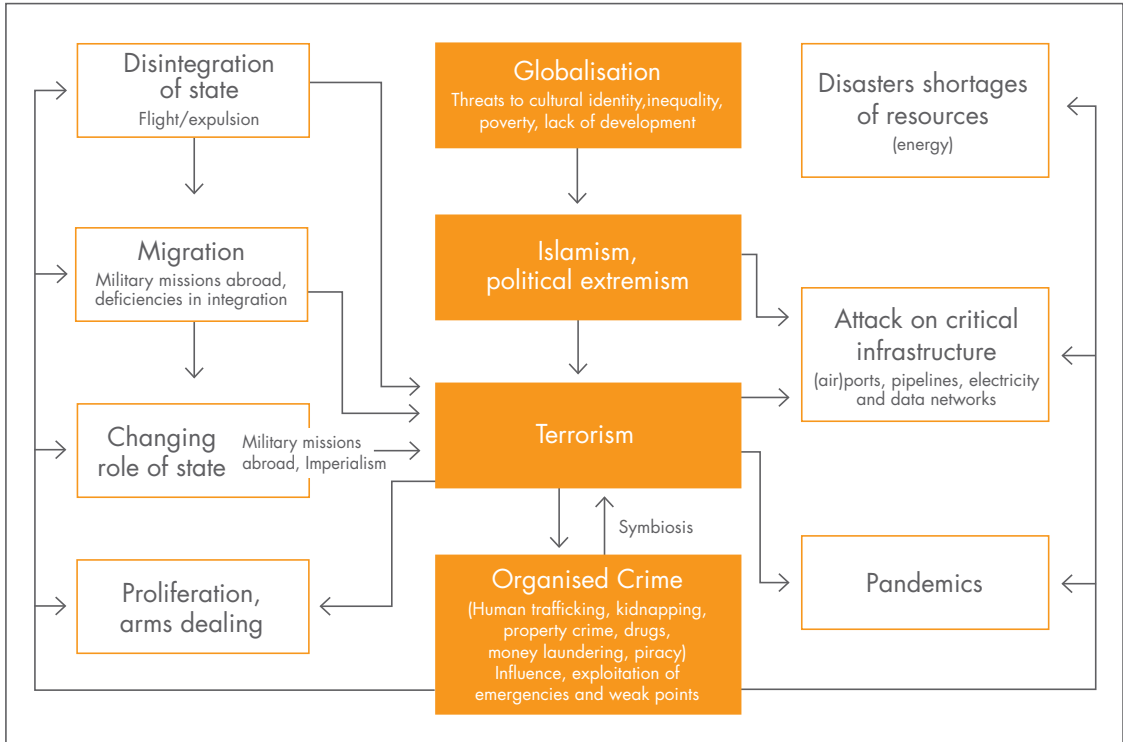
Statistically, the crimes listed are mass phenomena with a large number of unreported cases. Their potential to damage society is enormous and the percentage of cases solved is very low. The incidence of fraud has tripled over the last 20 years and the number of suspects has doubled. A large number of such cases go undetected⁷. Most of these criminals remain undiscovered and the state lacks penalties. An approach to property crime based solely on reported cases is not very effective. Analysis across all categories of crime and the involvement of different players from the economy, police crime statistics and prosecution statistics are necessary to avoid the risk of making seriously inaccurate assessments of the situation.

The currently available decentralised annual reports of the situation in the Länder vary in quality and quantity. They do not enable an adequate analysis of the complex economic relationships and cross-connections between crimes typical of organised crime and possible financing of terrorism, and so are unsuitable as a basis for evaluation and especially for rapid decision-making in crises.

Combating transnational terrorism will only succeed when organised crime and its environment have been cut back effectively.

⁷ On threat assessment for Germany, see the annual Federal Organised Crime threat assessment from the Federal and Länder Criminal Police Offices (BKA and LKAs), Federal Police and the Customs Criminological Office at www.bka.de; for the situation in the EU, see www.europol.europa.eu/publications/OCTA2007.pdf.

CONNECTIONS BETWEEN AREAS OF THREAT



4.4 CONCLUSION

Combating transnational terrorism will only succeed when organised crime and its environment in terms of economic crime, money laundering, tax and customs fraud have been cut back effectively. To deprive organised crime of its financial base, suspect assets must be confiscated with all available legal means. This requires the creation of cross-border bilateral regulations within the European Union to assist in recovering stolen assets. Data protection issues which might impede cooperation of the various players in crisis prevention and management should be scrutinised and practical strategies for action worked out. The challenges posed by terrorism and organised

crime can only be tackled successfully through close cooperation on a national and international level. Information exchange must be standardised and include an early warning system to help prevent crises and communication in response to specific events to act as a crisis-alert system. All authorities, institutions and organisations should cooperate even more closely than they have so far. The collaboration should have a legal basis which enables necessary - including confidential - information to be used within a security network as required to carry out these tasks for the good of the people, the economy and the state.

5. KEY SCENARIO "AN EPIDEMIC IN GERMANY"

The history of mankind is full of examples of epidemics which plunge states and societies into existential crisis. The tally of victims often exceeds that of severe natural disasters or wars. The influenza pandemic of 1918 to 1920 killed more people than the First World War; the plague in the 14th century probably wiped out one third of the population of central Europe, causing profound social upheavals.

Increased understanding of microbiology and progress in medical research and treatment give the illusion that these dangers are under control. New pathogens and epidemic outbreaks of known diseases in recent times have repeatedly shown that diseases and epidemics will remain a source of danger for German society, requiring government response.

First of all a re-emergence of smallpox, perhaps caused by a terrorist attack, or an influenza pandemic are to be mentioned. The Federal Republic of Germany has already taken precautions or is making preparations for these cases. This Green Paper therefore focuses on examples of diseases with the potential to have comparable consequences in Germany under unfavourable conditions.

Many diseases are not directly transmitted from human to human, unlike the above-mentioned smallpox and influenza. They require a vector which transmits the pathogen to the human victim. Mosquitoes are common vectors (malaria, dengue fever, Chikungunya fever) as are ticks (tick-borne encephalitis, borreliosis) and mammals such as mice (Hanta virus) and cats (pneumonic plague). Changing climatic conditions and global trade and travel can promote the spread of pathogens and vectors. Climate change has already resulted in both pathogens and vectors establishing permanently to new areas.

To make matters worse, a new disease occurring in an area not previously affected can have drastic consequences, since the population has not

yet built up a balance between pathogen and immunity. The speed with which the mosquito-borne West Nile Virus has spread in the US shows how fast a "foreign" pathogen can spread in the natural environment and then infect humans. This pathogen required only three years to migrate from the east to the west coast of the US, despite intensive efforts to prevent its spread.

BACKGROUND

Impact of an influenza pandemic

About 24 million cases of infection and 103,000 deaths within eight weeks – the Frankfurt am Main fire service has calculated that these could be the effects of an influenza pandemic with a medium infection rate. In the National Pandemic Plan (as of May 2007) it is assumed that around a third of the population would become infected. The current assumption is that all age groups would be equally affected. About half of those infected would consult a doctor and require treatment because of the severity of their illness.

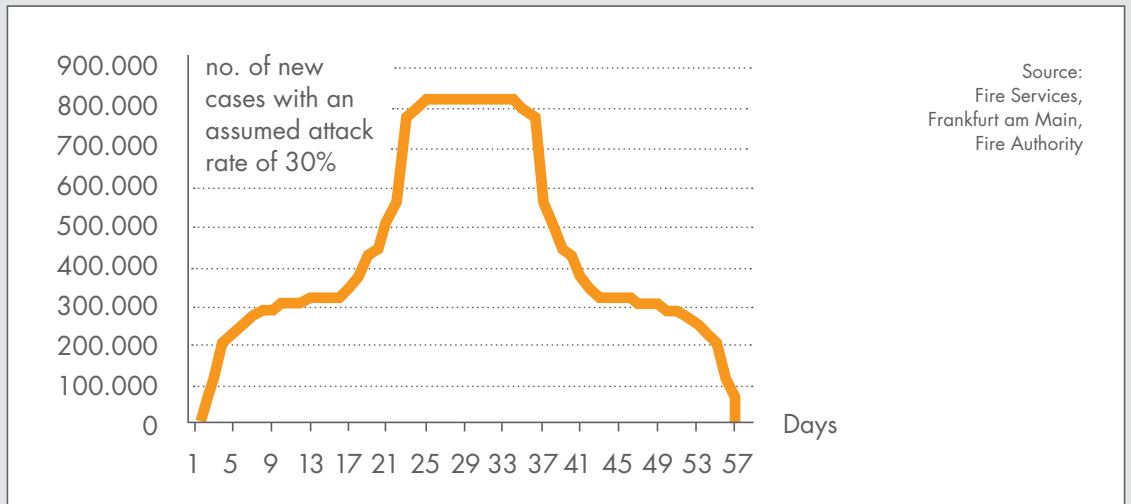
This would entail an estimated additional workload for doctors of 299,000 visits per day in total. Between the 21st and the 36th days of the epidemic, 820,000 new cases of infection could occur daily. This would not only affect the health system; it would also have significant negative effects on the economy.

Health care and economy particularly affected

A pandemic on this scale would cause dramatic shortages of personnel. Shortages in essential areas would occur in particular because key positions would remain vacant, affecting the police and fire services as well as logistics, transport and the electricity supply. State assistance would no longer be available to a sufficient degree, leaving people largely to look after themselves. In such a situation the natural human tendency to self-defence would be activated: many healthy people would not go to work, either because of fear of infection or in order to care for relatives. This would exacerbate the situation.

Staff shortages are particularly problematic when critical areas are affected such as doctors in private practice, hospital personnel and members of the police and non-police risk aversion bodies. The peak in numbers of doctor's visits, transports by ambulance services and in-patient treatments will coincide with the peak shortages of health professionals due to illness. The economy will continue to suffer staff shortages even when there are no more new infections, because the average duration of the illness from infection to recovery at the end of the pandemic wave is about 21 days.

NEW CASES OF INFECTION DURING AN EIGHT WEEKS INFLUENZA PANDEMIC



5.1 CHIKUNGUNYA FEVER

The Chikungunya virus⁸ is mostly transmitted by virus-carrying mosquitoes, principally the yellow fever mosquito (*Aedes aegypti*) but also other *Aedes* types, such as the Asian tiger mosquito (*Aedes albopictus*). Mosquitoes not of the *Aedes* type can also serve as vectors in particular areas. The main virus reservoirs are monkeys, rodents and birds. During an epidemic, humans are the main reservoirs. The human-mosquito-human transmission is the dominant factor during the outbreak. The disease is rarely fatal in humans. The incubation period is between three and twelve days, followed by high fever, intense headaches, conjunctival infection and severe pains in the muscles and joints. The joints become swollen and are often so sensitive to pain that even the simplest everyday tasks can no longer be carried out. There are no vaccines or specific treatments for the disease. Treatment consists of relieving the symptoms, which generally subside after one to three weeks. In about ten percent of cases, the arthritic joint pains last for several months, sometimes years.

Chikungunya fever was originally discovered in East Africa and currently occurs mainly around

the Indian Ocean in Asia, (including Malaysia, Thailand, Cambodia, Myanmar, Sri Lanka, India and Indonesia) and Africa (including Tanzania, Madagascar, Mauritius and the Seychelles). Other tropical regions in Asia and Africa are now also affected, including the Philippines, Gambia, Senegal and Guinea.

An outbreak of the disease on La Réunion in late 2005/early 2006 clearly demonstrated how quickly this virus can cause an unexpected and uncontrollable epidemic. On this island, located east of Madagascar and one of France's overseas Départements, one third of the population of nearly 800,000 was infected within only eight weeks.

This situation was caused by the simultaneous occurrence of two events: an extreme weather event and a mutation of the Chikungunya virus. The main vector for the virus, the yellow fever mosquito, is rarely found on La Réunion. However, a minute change in the virus's genetic make-up had adapted it to suit the locally common tiger mosquito. Weeks of torrential rain enabled this mosquito

⁸ Chikungunya [pron. chikungunja] is a word from the Bantu language family meaning "to double up".

to reproduce rapidly and prepared the way for the virus to spread at an explosive rate. At the peak of the outbreak, nearly 20 percent of the island's population was ill, including medical personnel. A total collapse of public life and health care was only averted by flying in medical experts from France.

The Chikungunya virus has now reached EU states bordering the Mediterranean. The virus occurred in North Italy in 2007, where people were infected by local mosquitoes, after the disease was probably introduced by a traveller from India. In Germany, tiger mosquito eggs were identified in an isolated case on the upper Rhine in spring 2008. However, there is no indication of an established population so far.

Rising temperatures in Central Europe are already bringing very mild winters, with frosts only rarely occurring on lowlands and tropical temperatures during the summers. One consequence of this development is that the *Aedes* types mentioned can spread from the tropics and subtropical areas to Germany and become established here. Additionally, mosquitoes are no longer dependent on natural expansion. They can "use" the high levels of mobility of goods and people; for example the transport of old tyres from the tropics to Europe, where they are recycled as valuable secondary raw materials. Mosquitoes in the tropics lay their eggs in rainwater which collects in the tyres, and thus embark on their journey around the world with the old tyres. Asian tiger mosquitoes have also been found in imported bamboo plants in the Netherlands.

Basic assumptions

Current climate models calculate that Germany will have a significant increase in the number of hot days and nights as well as more frequent and longer heat waves. The models also predict a change in rainfall patterns; there will be shorter, but heavier rainfalls in the summer. These are general trends, which will not necessarily be observed every year. Some years will be "average" whereas others will clearly show the changes in climate. These variations are not inconsistent with the overall long-term trend.

Based on the climatic calculations and the outbreak of Chikungunya fever in La Réunion, this

scenario is applied to Germany, especially the south and west of the country. It is true that the conditions in Germany are not present yet, but this scenario could take place within 10 to 20 years. The assumption is that daytime temperatures in the areas along the Rhine, the Alpine region and the Bavarian hills may exceed 30° Celsius over a period of weeks, accompanied by unprecedented numbers of "tropical nights", conditions similar to those of the 2003 summer heat wave. Frequent but brief torrential rain showers will also occur. Meteorological experts are already registering such changes in rainfall patterns and anticipate that this development will continue. Consecutive thunderstorms as they pass through can cause this type of heavy rain shower. A weather pattern of this type may last several days or weeks, bringing widespread rain overall and in some cases, resulting in flooding over a large area. Climate models project that these trends towards changed precipitation patterns will increase.

The following possible future trends also increase the chances of Chikungunya fever spreading:

- The climatic conditions have changed to such an extent that a stable population of tropical *Aedes* mosquitoes has established itself in south and west Germany. Tiger mosquitoes, with resistance to cold, have also spread from northern Italy into Germany.
- Chikungunya fever has become endemic at a low level in northern Italy and southern France and individual cases occasionally occur in Germany.
- The disease also continues to benefit from the transmission path provided by long-distance tourism to countries around the Indian Ocean. 57 cases of transmission in this category were registered in 2006.

The scenario

A heat wave and summer flooding permit the tiger mosquito to reproduce at explosive rates. This creates the basis for a massive spread of the virus. The usual methods of mosquito control are not as effective as hoped, because the *Aedes* mosquitoes are harder to combat than their local relations.

Experience in South Asia has shown that these insects have adapted very successfully to the urban environment. They can reproduce in tiny amounts of water such as small puddles in flower pots,

It is true that the conditions in Germany are not present yet, but this scenario could take place within 10 to 20 years.

drink cans or similar. Unlike France, for example, Germany has little medical entomological expertise and facilities for combating mosquitoes.

An additional problem is that *Aedes* mosquitoes are active in the daytime, which makes a great difference to the frequency of their bites: it is easier to protect oneself effectively against nocturnal insects than against those active in the daytime. Simple mosquito nets are adequate protection against the former, but repellents and adequate clothing are necessary to avoid mosquito bites of the latter. This results in much higher numbers of victims, as seen in the rapid spread of the outbreak on La Réunion.

At the peak of the epidemic in the scenario, the rate of new infections is eight percent of the population per week. This is the figure which actually occurred on La Réunion. The illness usually lasts from one to three weeks, so it will affect a significant proportion of the people needed to maintain basic supplies and public life. It is estimated that 15 to 25 percent of the population in the affected area will be ill at any one time, based on the figures from La Réunion. This means that several million people would require medical treatment simultaneously and are absent from work. Health care personnel will probably be affected at the same rate as the rest of the population.

This means that several million people would require medical treatment simultaneously and are absent from work.

The shortage of manpower will be exacerbated because:

- Health care professionals caring for the old and chronically ill, who are particularly vulnerable to the heat wave, are already overburdened.
- Disaster relief staff and the Bundeswehr staff called in to fight the flood are overburdened too.
- Employees and aid workers who are not ill themselves might not go to work, instead staying at home to care for relatives.
- Those helping to deal with the flood might stop helping for fear of being infected, because there is no vaccination or other protection against the disease.

The scenario will come to a head as soon as local mosquito types also start to transmit the disease

to humans. It is also assumed that many people will leave the affected area and try to reach areas which are still free of the disease. Flight movements like this exacerbate a crisis.

Public life will come to a standstill in the affected areas. Fear and even panic may arise within the population and this may be reinforced by media coverage.

Painkillers, other relieving medicines and repellents will soon be in short supply. It is conceivable that organised crime may use its well established structures to open a black market for medicines, including counterfeit drugs or those which are not permitted or not effective. This would further aggravate the situation [see: Terrorism and organised crime, p. 28].

BACKGROUND

Impact of climate change in Germany

Global climate change is also noticeable in Germany. In the last 100 years, the average annual temperature has risen by 0.8° Celsius. This trend has accelerated substantially during recent decades and has now doubled to a rate of 0.15° Celsius per decade. Looking at individual areas and seasons, it can be seen that precipitation has increased considerably in the west of Germany, especially in winter. In the east of the country, precipitation in summer has decreased. Extreme weather events such as heat waves and torrential rainfall occur more frequently, are longer and more intense. This trend is set to continue and has the potential to cause great damage to the economy [see Appendix 4.1 "Climate change"].

Institutions such as the Federal Environment Agency, the Federal Meteorological Institute (DWD) and climate research institutes have published the results of their regional climate models in recent years. They are all based on global climate models and identify possible climatic changes in Germany up to the year 2100. Comparison of the possible climate between 2071 and 2100 with the period between 1961 and 1990 shows that

- Temperatures in Germany could rise by between 1.5 and 3.7° Celsius – though to a different extent in different regions and with seasonal variations
- There will be fewer days of frost, but more hot days and more tropical nights
- Heat waves will occur more frequently and last longer
- Summer rainfall will decrease by an average of 30 percent and at the same time, torrential rainfall will occur more frequently
- Alpine glaciers and snow cover will continue to recede
- The sea level could rise by 60 to 80 centimetres.

The DWD has compared four regional climate models and has come to the following conclusions: experts anticipate an increase in average annual

temperature of between 1° and 2.25 ° Celsius by 2050. Over the whole century, the temperature could rise between 2° and 4° Celsius. The average annual rainfall total will probably be almost the same as it is today, but the rainfall cycle will change considerably. Summer precipitation will decrease by between 15 and 40 percent, depending on which projection is followed, whereas winter precipitation will increase. Only the east and south of the country will become generally somewhat drier by 2050: 5 to 15 percent less rain is anticipated there.

Regional effects of climate change

An examination of the different areas of Germany reveals the regional differences climate change and its effects will bring. By the end of the 21st century, a comparatively low rise in temperature is predicted for the coastal regions of the North Sea and the Baltic Sea, due to their proximity to the sea and the relatively temperate coastal climate. However, the number of so-called temperature marker days will change considerably; that is, "ice days", "frost days", "summer days", "hot days" and "tropical nights". The models predict an above-average increase in precipitation during the winter for the North Sea coast and the north-west German plain. A particularly marked decrease in summer precipitation is predicted for the Baltic coast and the north-east German plain, which could cause problems in the north-east region of the country, which already suffers from drought. Adaptation measures will need to be introduced – for example in the field of agriculture and water management.

The Central German Uplands and the Harz mountains are predicted to retain their cooler climate compared to the rest of Germany. There will be smaller changes in the number of "frost days" than in lower-lying areas. The number of "summer days", however, will more than double in places. These areas already have high levels of precipitation. The experts predict an above-average decrease in summer precipitation in the Harz and Harz foreland, whereas winter precipitation will increase at above-average rates.

BACKGROUND

The predictions for the Rhenish Uplands on the left and right banks of the Rhine show particularly striking changes in precipitation. The highest rate of increase in winter precipitation for the whole of Germany is projected for this area; summer precipitation, however, will only show a comparatively small decrease. The Uplands on the left bank of the Rhine will receive more precipitation altogether, which may have consequences for agriculture and forestry and for flood prevention. Climate change in the Rhine Rift will be marked by a substantial increase in hot days and nights and more frequent and longer heat waves. This increase will pose particular challenges for the health services.

In southern Germany, especially in the Alpine foreland, the Alps and the north Bavarian hills, temperatures will also rise steeply. Precipitation, in summer in particular, could also decrease significantly in south and south-west Germany. The higher summer temperatures would cause the remaining water to evaporate more quickly, increasing water management problems.

Climate change is also reflected in the increase in extreme weather events, such as heat waves and torrential rain. These episodes will occur more frequently, last longer and be more extreme. It is impossible to calculate in advance the damage such events may cause. Occurrences in the recent past, however, reveal the possible extent of the problem for Germany: for example, the floods on the River Elbe in 2002 caused total economic damage of €9.4 billion. Hurricanes Lothar and Martin in 1999 caused damage totalling over €14 billion. Statistics show that 7,000 more people died in the heat wave in the summer of 2003 than in normal summers.

Approach through double strategy: Adaptation and prevention

Although not all details of future climate changes and consequences are known, experts are developing a double strategy to cope with the effects:

- First, a long-term strategy to mitigate climate-changing gas emissions in the atmosphere, which will start to make a difference after several decades or even centuries. The aim of this

strategy is to protect the climate as a "common good".

- Second, forward-looking adaptation of natural and social systems to the current and anticipated climatic changes. Even if no more greenhouse gases entered the atmosphere from now on, the climate will continue to change in coming decades due to its thermal inertia.

Adaptation and mitigation are allocated equal importance at international level, particularly since the Climate Conference on Bali in December 2007. A European Green Paper on the topic was published in the summer of 2007, to be followed by a White Paper, probably in late 2008. The federal government is preparing a strategy to adapt to climate change at national level, and activities towards adaptation and climate protection are also taking place at regional and municipal level. Adaptation to climate change in the sense of making provisions for the future has, above all, a local and regional focus. Adaptation measures have been shown to bring the greatest benefit at this level.

Information on climate changes and vulnerability must be as precise as possible if successful instruments of adaptation to climate change are to be developed. It is also essential to increasingly adapt both established and new planning and regional planning instruments to flooding, storms, water shortages, heat waves, etc. The aim is to plan current and future land use in accordance with climatic conditions. For example, new buildings should not, where possible, be constructed in areas where repeated flooding occurs. Conflicts about future land use can be expected to increase. Land use in particular areas will lead to conflicts of interest at national, regional and municipal level.

Long-term sustainable development is required. This is the only way to reconcile climate protection, adaptation and further demands on land use. In recent years, the responsible authorities have considered new forms of taxation in the sense of climate governance, in addition to existing instruments.

5.2 THE SARS VIRUS

The Chikungunya virus is transmitted to humans by the vector *Aedes* mosquito. A pathogen such as SARS is spread by human-to-human transmission, leading to additional challenges.

A dollar bill-tracking investigation in the USA astonished scientists by revealing a huge increase in the mobility of people and goods in recent years. The conclusion is that pathogens can spread far faster today than previous model calculations assumed. Consequently future pandemics will spread according to different rules and much more quickly. New model calculations focus on air traffic hubs such as London, New York and Frankfurt am Main, which would be responsible for the rapid global spread of an epidemic, almost regardless of where the pathogen actually originates.

The spread of SARS provides convincing evidence of this. The first cases of an atypical form of pneumonia occurred in mid-November 2002 in the Chinese province Guangdong. The World Health Organisation gave it the name Severe Acute Respiratory Syndrome (SARS). In February 2003, the pathogen started its journey round the globe. SARS spread extremely fast and without exception only via infected air passengers. The highest numbers of patients occurred in cities with international airports. The classical methods of restricting the spread of epidemics and pandemics, such as quarantine for contact persons and isolation of patients, were the only possible means to end the pandemic. There was and is no therapy against this virus. Initially, hospitals were also unprepared for such a contagious form of pneumonia, so that tragically, initial infection rates among medical personnel were high.

SARS has an extremely high mortality rate of around 10 percent, compared with seasonal influenza which kills only 0.1 percent of its victims; an influenza pandemic would cause a mortality rate of 1 or at most 2 percent.

However, certain characteristics of this new virus, compared to other pathogens, have so far helped to prevent a pandemic on a disastrous scale:

- The virus can only be transmitted to other people after symptoms have appeared, unlike HIV, measles or influenza viruses which are infec-

tious before symptoms appear. The SARS virus is mainly present in the patient's lower respiratory tract. Only when symptoms are fully developed the virus is present in the upper respiratory tract in such numbers as to infect others by coughing or sneezing.

- The SARS virus is not particularly robust. Thorough hand washing can suffice to render the pathogen inactive.
- Because the disease is typically spread by infected droplets, wearing a surgical face mask can prevent transmission, similar to influenza.
- Children and young adults were only mildly infected and there were hardly any deaths among this age group. However, the mortality rate was over 50 percent in patients over 65.

The SARS virus only infected around 8,000 people world-wide, yet the global economic effects of the pandemic were remarkable. Although there were "only" 251 cases in Canada with 43 deaths, the economic damage was estimated to be nearly \$1 billion.

Assumptions and scenario

Viruses in general have a high mutation rate. Slight changes in the genetic material suffice to give the pathogen new characteristics, as in the Chikungunya fever epidemic on La Réunion where a slight mutation gave the virus the edge. A similar mutation of the SARS virus could make the virus more dangerous than influenza.

A mutation of the SARS virus could conceivably result in the following changes:

- that it can be transmitted before the symptoms appear,
- that it becomes more robust,
- that the disease takes a more aggressive form in younger patients,
- or a combination of those three factors.

The scenario assumes a mutation which enables the virus to appear in the upper respiratory tract before symptoms appear. The SARS virus is about as infectious as influenza and if it were to mutate as envisaged, it could be transmitted just as easily. The result would be a massive outbreak with the numbers of infected people comparable to those predicted for an influenza pandemic, but with a mortality rate between ten and one hundred times as high. The situation would be exacerbated by the lack of medicines to treat SARS and the lack

The SARS virus is about as infectious as influenza and if it were to mutate as envisaged, it could be transmitted just as easily.

of a vaccine. The effects are difficult to predict but would certainly be disastrous.

Extrapolating the figures of the SARS event from 2003 and applying them to a mutated virus and several million infected people, the economic effects would be on a scale which even a western economy would not be able to compensate.

5.3 EFFECTS OF THE SCENARIOS

The health service would be completely overloaded.

The Chikungunya virus is a serious threat to people's health and life and even more so is a highly infectious variant of the SARS virus. Fear and panic could spread among the population far more quickly than in the case of a blackout, because the latter is not immediately life-threatening for most people.

Effects on the population

The population's capacity for self-help is rather limited. First Aid courses are rarely promoted in Germany. This is a definite deficit in a crisis where the whole population would be required to care for the sick at home, in the family and in the neighbourhood. Healthy people who could go to work will stay at home to care for the sick. If public institutions such as schools and kindergartens close as part of quarantine measures, parents will also miss work to stay at home and look after their children.

Effects on public authorities, emergency and rescue services, police risk aversion and health services

When an epidemic occurs, the responsible authorities actions would have to be as targeted as possible in their response in order to ensure that at least basic supplies are maintained. They would have to focus on the care, treatment and transport of the sick and on controlling the spread of the virus.

The care, treatment and transport of the sick would require almost identical measures in both scenarios: mass casualties have to be treated within a very short period. Neither a vaccine nor effective medical treatment is available for either disease. The patients are in a weakened state and are treated with supporting measures such as infusions and artificial respiration. Treating SARS patients is much more difficult and dangerous because of the

risk of infection. There is no available vaccine to protect key medical staff for either disease.

The health service would be completely overloaded. The available resources are designed for a normal level of illness and local events. They could not begin to cope with a crisis on this scale. Rising economic pressure leading to the reduction in spare capacity in the health service structure and increasing privatisation are contributing to this situation.

To ensure basic care for the patients, the following would be required:

- Auxiliary hospitals, wards and care institutions, operated by aid organisations and the public health service.
- At-home emergency calls and home care reliably provided by the public health service, aid organisations and charities despite the additional burdens placed on them.
- An adequate supply of medicines, infusions, hygiene items and disinfectant provided by industry.

Another problem is the lack of stocks of medical supplies due to the currently prevalent just-in-time logistics: for example, hospitals only usually hold two days' worth of supplies of infusions. There is also a lack of reliable information on requirements of additional essential medical supplies in a crisis of this nature. There has never been a reliable inter-regional study of the quantities and types of additional material required during the heat wave in the summer of 2003, which killed about 70,000 people throughout Europe.

Measures to restrict the epidemic are different in each case:

- The main method of tackling Chikungunya fever would be to decimate the population of carrier mosquitoes. It may even be necessary to isolate the regions where the Tiger mosquito occurs.
- The highly contagious SARS variant would require more drastic measures, such as, isolating the areas where the outbreaks occur, reducing the rate of infection by use of surgical masks, setting up disinfection stations, imposing restrictions on freedom of movement.

Both scenarios would quickly lead to shortages of manpower. Healthy personnel who are also wil-

ling to work, despite the risk of infection, would be in short supply at all levels. The health and risk aversion services would require increased personnel. Finally, the lack of personnel would lead to the dreaded cascade and domino effects in all areas from emergency services to hospitals to essential energy and food providers.

Inevitably, medical personnel and volunteer helpers would be double-booked, leading to further shortages in the aid organisations. Shortages of irreplaceable specialists are to be anticipated.

In an outbreak of Chikungunya fever in Germany, comparable with that on La Réunion, attempts would be made to bring support into the crisis area from other regions of the country. However, if the weather conditions spread, other regions may also be affected which would greatly reduce the personnel available.

Besides, it is by no means certain that the Länder would be willing to make their resources available to each other. They are not legally obliged to do so and if they did, they would risk suffering shortages themselves, if the crisis spreaded. The floods on the Elbe showed that the Länder and districts tend to hoard their resources in case they need them themselves.

In the SARS scenario, the epidemic would get out of control so fast that the only sensible measures would be quarantine for all those who have come into contact with the disease, isolation of patients and other epidemic control measures such as closing schools and banning large public gatherings. As a last resort, banning movement of goods and people could be considered, resulting in isolating entire cities or regions. These measures would themselves exacerbate the crisis considerably and increase the effects of the disaster.

The SARS epidemic in Canada showed that it was not so much the disease itself as the measures necessary to combat it which turned the situation into a disaster.

Effects on commerce, trade and industry

The absence of large numbers of staff because they are sick, looking after relatives or afraid of infection will restrict economic activity in all areas. Even counter measures such as recalling all perso-

nnel from holidays would bring only limited improvements. If other elements of critical infrastructure apart from the health service are affected, cascade effects will result, aggravating the situation further.

5.4 PARALLELISM OF EFFECTS

Shortages of personnel in the energy industry, ICT, transport, logistics and all other elements of critical infrastructure could have similar results to those already described in the power cut scenario.

5.5 CONCLUSION

Epidemics pose risks and dangers for the people and society in Germany. Despite all medical progress, they still threaten the two most important factors of a community: the population's health and the basic food supply [see also animal foot and mouth disease in: Appendix 5.1 "Epidemic scenarios"]. This makes it essential that appropriate preparations for such events remain one of the core areas of the state's responsibility.

Germany already has basic documents on preparation for a large-scale epidemic: the "Federal/Länder conceptual framework for essential preparation and measures for disease control after a bio-terrorist attack - section on smallpox" and the national "Influenza pandemic plan". These could serve as examples for risk and crisis management. However, these documents only relate to an outbreak of these two epidemics. They are taking no account of comparable types of crises.

Germany's lack of a unified national emergency plan which includes a basic strategy for preventing an epidemic makes crisis management more difficult on all levels. Whether the current federal structure of the health and disaster aversion services is the most suitable instrument for dealing with a nationwide epidemic is an open question, especially if limited resources must be shared beyond Länder boundaries in the event of a crisis.

Germany's lack of a unified national emergency plan which includes a basic strategy for preventing an epidemic makes crisis management more difficult on all levels.

6. TOWARDS A MODERN DEFINITION OF SECURITY

The scenarios show that the really novel aspect of the information society is the increasingly complex global interconnectedness of systems with mega data streams. This has brought about a new level of vulnerability and risk. Security is increasingly dependent on availability of data and smooth communications. If these are disrupted, large-scale crises can occur, reaching dimensions previously only conceivable for a case of national defence.

In these circumstances, “public safety and security” means in the first place that complex processes and systems, on local, national and transnational levels, must function as smoothly as possible. The Green Paper indicates the points at which these functions are endangered and examines how system breakdowns and crises could be approached. The more resources society and the state can mobilise, the more resilient they are in times of crisis.

The central question is how the responsible authorities can impose and maintain this smooth functioning and, in the event of a crisis, how they can regain it as quickly as possible. How long and to what extent can individual functions break down before endangering the existence of society and the state? Which functional equivalents are necessary to bridge, bypass or compensate the breakdowns?

It is clear that material and conceptual determinations are required to maintain public safety and security:

- **Material determination** relates to the type and quantity of the functional equivalents: what is required in order to cover system failures and to maintain the functioning of the system as a whole?
- **Conceptual determination** refers to how safety and security are measured. How much loss of function – and to which function providers – will be acceptable? How much or how little can they afford in comparison to other function providers? Security costs money which must be earned, just like other goods. This also makes security a locational factor.

Safety and security in modern societies can no longer be defined in purely national or sectoral terms, nor be provided independently by a single state. This is shown by events like the SARS crisis or widespread power cuts. Security requires a global framework and monitoring instruments.

Climate research has revealed that long-term, gradual global changes demand entirely new processes of gaining information, for example models and simulations. New methods of reaction must also be introduced, such as long-term steering, avoidance, adaptation, acceptance and legitimation.

Civil protection is not solely a task for the state; business is also responsible, above all when it operates critical infrastructure. Each citizen also bears responsibility, whether in the will and ability to protect themselves or to assist others. This makes new ways of dealing with danger and risks necessary. Human resource management which regards the citizen as a potential partner is required. Only a common understanding of

collective security and safety will make the individual citizen willing to make a contribution and to accept restrictions in a serious situation. Security at no material or immaterial cost is impossible. However, freedom and security are not mutually exclusive.

6.1 KEY QUESTIONS: PHILOSOPHY AND AIMS OF SECURITY

- Are current **security philosophies** and the **security architectures** based on them still valid? What are the dangers which society and the state must prepare for? Which instruments could provide early identification of threats?
- Are special **rights** to “basic protection” (still to be defined) necessary, in addition to general human rights, international rights and basic rights?
- How can modern society’s need for information be fulfilled? How can both **basic civil rights** and the need for informational self-determination be guaranteed?
- What mediation instruments are necessary to ensure that future threats are perceived and adequately responded to? Are current forms of risk and crisis communication adequate?
- How many **crises** and how much **damage** can society and the state sustain and still survive? What resources and capabilities are required to survive this damage and to ensure long-term resilience? What contributions are required from the state, the business sector and the people? What protection do all participants expect from the state?
- How much resilience is expected from society, the state and the economy in the short, medium and long term? What should **critical infrastructure** deliver, especially the electricity supply and information and communications technologies?
- What forms of **international collaboration** are necessary to ensure that the management of transnational infrastructure is crisis resistant? And what types of international collaboration must be developed to overcome or avert cross-border risks?
- Is **standardisation of technologies, organisations and laws** required, in order to develop a transnational framework for global security?
- How must **communication and collaboration** be structured between the police and non-police risk aversion bodies, between private and state institutions, between national and international levels?
- In view of changing threats, especially events which develop gradually, **preventive measures and instruments** as well as reactive measures are necessary. How can these be implemented within Germany? And how can they be harmonised at international level, for example in case of a pandemic or in the face of climate change?
- Will the **national economy** be able to survive the anticipated effects of seriously threatening situations (climate change and shortages of resources)? Would the losses caused be acceptable?
- Are the effects of specific threats, for example organised crime, **on the national economy and society** sufficiently described and is the public aware of them? Do appropriate responses exist, such as the confiscation of illegal profits or social surveillance?

6.2 KEY QUESTIONS: RESOURCES AND MOBILISING THEM

- In principle, everything can be classed as a resource: nature, people, knowledge. What could cause a **serious scarcity** of resources; which resources are threatened under which conditions? How could the shortage be compensated, replaced or bypassed?
- Which **natural resources** require protection? Which must be stored to guarantee availability? And in which form: as minimum reserves or safeguarding laws? And which resources must be developed or created?
- Which resources are essential in the event of a crisis or disaster? How long can society and the state survive shortages which threaten their existence (material, physical and psychological **stamina**)?
- At what point does a shortage become life-threatening? How can resources be **mobilised and distributed** (for example in case of an influenza pandemic which could affect 24 million people)?
- What **reaction strategies** are available in a crisis and how can they be communicated and rehearsed?
- To what extent are society and the state ready to make capacities available for crises of this kind – for example, for observation, analysis, evaluation and **procurement**? How are these tasks allocated?
- Is it necessary to restructure and reallocate **responsibilities**?
- What medium and long-term **financial resources** must be secured for threats of this nature?
- What personnel and emotional resources have to be set up to ensure **efficient prevention**?
- What **leadership systems, equipment, training and exercise** scenarios are required?
- How significant are the players' **willingness and ability to cooperate** for effective crisis management?
- How can the **Bundeswehr** (in the frame of the subsidiarity principle) be included in the planning of official aid and what resources could it contribute (Civil Military Cooperation, CIMIC)? How do resource providers collaborate from regional up to EU level?
- Many elements of critical infrastructure are now privatised to a large extent; are the many **resource providing organisations** of all sectors sufficiently networked and able to cooperate?
- Are specific resource providers such as the public **health services** sufficiently integrated? Are hospitals equipped for a large-scale crisis such as a blackout or an epidemic? Could they cope with mass casualties? What resources are needed to deal with bottlenecks in capacity? What solutions could be found to compensate for an excessive demand for hospital treatment?

6.3 KEY QUESTIONS: CRITICAL INFRASTRUCTURE

- Is the definition of **“critical infrastructure”** adequate in the face of new threats? Are all elements systematically registered?
- Have the **interactions** between the different infrastructures been sufficiently modelled and tested in practice?
- Are currently available sensor systems and communications technology adequate

- to identify and ward off an **attack on critical infrastructure** early enough?
- Should industrial providers of critical infrastructure adhere to **minimum standards** in view of physical threats and should these be subject to official inspections?

6.4 KEY QUESTIONS: POPULATION AND CIVIL PROTECTION

- What **preventive measures and capabilities** are required for damage limitation in the case of large-scale long-term events?
- How can the population's **self-help capacity** be strengthened? Is it possible to create awareness of the importance of self-help?
- To what extent are **precautionary measures** needed and what risks must people be persuaded to accept?
- Are adequate **protective measures** and equipment available to the population in case of a large-scale danger, particularly an epidemic, a pandemic or the threat of radioactivity?
- What must be done to enable people to show **solidarity and resilience** in a crisis?
- Is any empirical data available on people's **risk acceptance** and resilience? Is such data sufficient to enable predictions of what behaviour could be expected in case of a large-scale threat such as an epidemic?
- What must be done to gain a **realistic estimate** of people's probable behaviour in a crisis of this nature?

6.5 KEY QUESTIONS: RISK AND EMERGENCY COMMUNICATION

- What kind of **communications concept** is needed in a crisis? How must information and data exchange be organised?
- What possible forms of communication are available? What **information and communications systems** need to be set up?
- How can an effective **warning system** be ensured and combined with information about the type of danger? How can it be ensured that the population is well-informed and aware?
- How can **helpers be coordinated** and resources pooled – even when communications systems have collapsed?
- How can the **media** communicate the need for prevention?

6.6 KEY QUESTIONS: INSTITUTIONAL REQUIREMENTS AND IMPLEMENTATION

- Is the **harmonisation of laws** on cooperation, coordination, establishment and distribution of depots **necessary** at the national level? Is this necessary at European and international level?
- Are Germany's **federal structures** appropriate for risk and crisis management?
- How can effective and essential **leadership and decision-making structures** for a nationwide crisis be created within a federal system?

- How can the **federal government, the Länder and the municipalities** ensure that new risks to public safety and security in their area of responsibility are identified at an early stage? How can they evaluate and possibly avert the threats? Which structures need to be institutionalised?
- How can a **holistic risk and crisis management system which takes the interdependencies into account** be established for the events described? What standards would have to be drafted and implemented? Which public and private players have to collaborate? What legislative foundation and institutional conditions need to be created? Which responsibilities and competencies have to be defined? Can the subsidiarity principle be maintained as a guideline?
- Are there suitable **overall operations planning and leadership systems**? Is an adequate and overall leadership capability available?
- How should a suitable **early warning system** be designed?

GLOSSARY

Asymmetric warfare: Conflicts with serious effects similar to war between two parties/players whose relative military power differs markedly (e.g. terrorists vs a state), sometimes using unequal means and/or methods.

Bi-polar world order: This term refers to the territorial situation during the cold war where the two alliances, NATO and the Warsaw Pact countries, opposed each other with a huge military presence.

Bill-tracking: Tracing the movements of particular bills for scientific purposes. A large number of marked dollar bills was put into circulation in 2005. Anyone who receives a marked bill can register online, enter their position and return the bill to circulation. The website is now so popular that approx. 50 million individual bills are registered.

Underground economy: All economic activity within the national economy whose value creation does not enter the gross national product. This usually means profits from illegal activities which are introduced into the legal economy without payment of tax or other dues, so distorting competition and avoiding responsibility towards society and obligations towards the state. Examples include money laundering, flight of capital, smuggling, transnational corruption, organised crime, proliferation of nuclear material, trafficking in drugs, diamonds and arms, unregulated trading points for goods (internet) and flight and migration movements (human trafficking).

Borreliosis: A tick-borne disease caused by the bacterium *Borrelia burgdorferi*. After infection, the borrelia bacteria migrate via the bloodstream into the body tissue and can affect the nervous system and joints. This can cause chronic and neurological infections, such as arthritis, meningitis and heart disease.

BOS: German abbreviation for public authorities and organisations involved in security/safety, including the Federal and Länder police forces,

customs authorities, the Federal Agency for Technical Relief (THW), the fire services, the disaster protection authorities, the civil protection and disaster prevention organisations and the supporting organisations for the rescue services.

Botnets / botnet attacks: A bot (short for robot) is a programme which works by remote control on a computer previously taken over by a Trojan horse, for example. Botnets are networks of compromised computers (some networks of hundreds of thousands of bots have been observed) which can carry out simultaneous remote-controlled activities such as sending spam emails or carrying out DDoS attacks.

Cascade effect: Term for an unforeseen chain of events proceeding in stages; if the stages reinforce each other the term avalanche effect can be used. In relation to damaging processes, these can start from very small causes and end up having very large-scale effects (as in an actual avalanche). Infrastructure processes can react in cascade fashion to certain events.

Critical infrastructure: Organisations and institutions which are essential for the functioning of a society, the loss or malfunction of which would cause long-term shortages, severe disruptions in public safety and security or other serious effects. (Definition by the working group KRITIS in the Federal Ministry of the Interior, 17/11/2003).

Dark figure (of crime): The sum of crimes which are not known to the authorities and so do not appear in police statistics. There is a large dark figure of crime in all fields of organised crime (e.g. drug trafficking, economic crime).

Dengue Fever: (Also known as breakbone or polka fever) An infectious disease transmitted by mosquitoes. The symptoms are often not specific; they can be similar to severe influenza, but sometimes internal bleeding also occurs.

Denial-of-service (DoS) attack: This occurs when a target IT system is saturated with data packets from other computers, in order to overload it and to prevent genuine users from accessing it. The victim system can often not handle the huge amount of packets and breaks down. A DDoS (Distributed Denial of Service) attack occurs when multiple attackers act simultaneously.

deNIS: Abbreviation for German emergency planning and information system, an electronic information system located in the Federal Office of Civil Protection and Disaster Assistance (BBK) in Bonn. It collects and processes information on civil protection and makes it available to certain clients (e.g. Federal and Länder authorities, aid organisations). An open internet portal, deNIS I, is available for public interest and interested experts. The closed platform deNIS IIplus is accessible to the assessment centres of Federal and Länder ministries and the aid organisations' control centres. It is mainly a geographical information system (GIS) which supports crisis management in particularly dangerous situations.

Digital communications: Modern digital technology-based broadcasting, radio, TV and the digital radio communication network of the BOS (public authorities and organisations involved in security/safety), currently being set up. Digital communications are more powerful and are now replacing analogue technology.

Dirty bomb: A bomb using conventional explosives to disperse radioactive material to contaminate the surrounding area. The explosion and contamination are much weaker than if using a nuclear device, but the manufacture is much easier by comparison.

DISMA: A software tool for early recognition of threats and damage limitation in cases of technical failure. DISMA has a modular structure, consisting mainly of the components data (collection, overview, research), threat evaluation, map (crisis management and links to data), planning and

tools for data administration and maintenance and to serve interfaces.

Domino effect: Sequence of events in which each event is the cause of the next and all can be traced back to the same initial event.

Epidemic: Spread of a known or new disease in a limited area (city, country, several countries) for a limited time, where the number of cases exceeds a previously defined seasonal "expected number" for this disease. The "expected number" for a new disease is zero, so a very small number of cases still counts as an epidemic.

GMLZ: German abbreviation for German Joint Information and Situation Centre, a joint crisis management institution of the federal government and the Länder. The GMLZ is located at the Federal Office of Civil Protection and Disaster Assistance (BBK) in Bonn and can be reached 24/7. Its tasks include (1) continuous observation of the situation (2) acquisition, analysis, preparation, coordination, passing on and exchange of communications and information and (3) making of prognoses about damage development in the event of a crisis (see www.bbk.bund.de). GMLZ is intended to provide nationwide information on experts and resources for the disaster relief agencies when disaster relief assistance is required. The assessment centre also acts as an international contact and liaison organisation in the EU Civil Protection Mechanism. Federal government, Länder and aid organisation staff is assigned to the GMLZ.

Hanta Virus: An infectious disease transmitted by mammals, which causes pulmonary infection, acute renal failure or severe haemorrhagic fever. Hanta viruses occur world-wide and are endemic in some regions of Lower Saxony, Hesse, Bavaria and Baden-Württemberg in Germany and in Steiermark in Austria.

LÜKEX: Abbreviation for a German nationwide crisis management exercise; LÜKEX is a biennial series of staff exercises by the federal government

and the Länder, commissioned by the Federal Ministry of the Interior, to test and practise the crisis management functions of Federal and Länder authorities, encompassing municipalities and the business sector.

Metadata streams: Streams of data which relate to primary data flows and are intended to clearly define, check and control them. Digitalised data require decoding data and reference data such as time, place, sender and recipient. Each entry in a database requires “identifying” (keyword) and “localising” metadata. The more data accumulate, the more important are the data about the data and the greater the danger of not being able to “read” the primary data if the metadata are damaged.

Pandemic: Spread of a known or new infectious disease during a limited period where the number of cases exceeds the previously defined seasonal “expected number”. In the case of new diseases, the “expected number” is zero, so a very small number of cases can be counted as a pandemic. The difference between epidemic and pandemic lies in the extent of the outbreak: a pandemic affects continents, or even the whole world.

Phishing: Word made up from password and fishing, meaning fraudulent means of obtaining and using access data for online banking and other internet payment systems.

Redundancy: Duplication or multiplication of identical structures and resources (back up) to improve the reliability of a system.

TBE: Abbreviation for tick-borne encephalitis, a disease transmitted by ticks and caused by the TBE virus. The disease produces flu-like symptoms such as fever and can cause meningoencephalitis, an inflammation of the brain and the membrane surrounding the brain and spinal cord.

Temperature marker days: For the German climate the marker days are defined as follows: Ice days: maximum temperature $\leq 0^{\circ}\text{C}$; frost days: minimum temperature $\leq 0^{\circ}\text{C}$; summer days: max. temperature $\geq 25^{\circ}\text{C}$; hot days: max. temperature $\geq 30^{\circ}\text{C}$; tropical nights: min. temperature $\geq 20^{\circ}\text{C}$.

Subsidiarity principle: A principle originating in Catholic social teaching, describing the ranking of responsibilities for assistance in a social system. According to this principle, the lowest level (ideally an individual) should take the necessary action; only if he/she is not able to do so, the next highest level takes on the responsibility. This concept views the responsibility of the state as subsidiary. At the same time, it ensures that decisions and action are made or carried out as closely as possible to the point of need. Disaster relief and civil protection in Germany are organised according to this principle. The German aid system is structured in this way from municipal up to Länder level: the federal government is only involved in cases of national defence. The EU’s civil protection mechanism is also based on this principle.

Vector: (Latin for “carrier”) Transmitters of pathogens. In the case of Chikungunya fever described above, the vectors are mosquitoes of the Aedes type.

Year 2000 problem (Y2K): Weakness in older computer systems which could have caused, and in a few cases did cause, undefined failures and system breakdowns at New Year 1999/2000. The problem was that in the older systems, the year was only shown as a two figure number, so there was no recognisable difference between the year 2000 and the year 1900.

PUBLISHING DETAILS:**Publisher:**

Gerold Reichenbach,
Ralf Göbel,
Hartfrid Wolff,
Silke Stokar von Neuforn

Publishing House:

ProPressVerlagsgesellschaft mbH,
Behörden Spiegel-Gruppe Berlin/Bonn

Editing Office and Layout:

Pleon GmbH, Berlin

Print:

Spree-Service- und Verlagsgesellschaft mbH, Berlin

Date/Edition:

September 2008, 1st edition /1,000

© Copyright for text and diagrams is held by the authors or editors, unless otherwise stated. With permission of the authors or editors other forms of publication are possible.

Bundestag eagle: © Prof. Ludwig Gies,
revised 1999 Studio Laies, Cologne.

ISBN 978-3-934401-18-8

www.zukunftsforum-oeffentliche-sicherheit.de