



Federal Ministry
of Education
and Research

Research for Civil Security

Programme of the German Federal Government



HIGH-TECH STRATEGY

Igniting ideas!

Published by

Bundesministerium
für Bildung und Forschung /
Federal Ministry of Education and Research (BMBF)
Public Relations Division
11055 Berlin

Orders

In writing to the publisher
Postfach 30 02 35
53182 Bonn

Or by

Phone: +49 (0) 1805-262302
Fax: +49 (0) 1805-262303
(0.14 Euro/min. from the German fixed network)

E-mail: books@bmbf.bund.de
Internet: <http://www.bmbf.de>

Edited by, author illustrative stories

Dr. Mathias Schulenburg, Cologne

Layout

Suzy Coppens, Cologne
www.bergerhof-studios.de

Printed by

Druckhaus Locher GmbH, Cologne

Bonn, Berlin 2007

Photo credits

BergerhofStudios, Suzy Coppens

page(s) 06 top, center; 15
top; 20; 24; 27left; 29-31;
33; 35; 50

Bosch

front cover; page 19; 23; 25
top; 45 right; 48 bottom

California Inst. of Technology, Fei-Fei et al.
Deutsche Bahn AG

page 46
page 06 bottom; 12; 13
center; 21 bottom

Deutsche Telecom AG
EADS

page 14; 36
page 18 right; 21 top; 40
right; 42 bottom

ESA/DLR
Fraunhofer Inst. für Siliziumtechnologie, ISIT
Hamburg, Oberfinanzdirektion
Hafen Hamburg Marketing e.V., Achim Sperber
IKONOS, Space Imaging
Kölnarena GmbH
microdrones GmbH
Siemens AG

page 34
page 43
page 39 bottom
page 32
page 41
page 27 right
page 47
page 08; 10; 18 left; 26; 37; 38
left; 38 right; 42 top; 44; 45
left; 48 top

Technisches Hilfswerk

page 12 bottom; 13 right; 15
bottom; 17; 28; 40 left

University of California, Mark Hoemmen
U.S. Customs and Border Protection,
Gerald L. Nino
VDI TZ

page 39 center
page 22



Federal Ministry
of Education
and Research

Research for Civil Security

Programme of the German Federal Government

Preface



Germany is among the most secure countries in the world today and should continue to be so in the future. However, globally increasing terrorism and organized crime as well as natural disasters and major incidents confront us with entirely new challenges. Our modern, strongly networked society is highly susceptible to such threats. The security of people is not only threatened by direct attacks and natural disasters but also by failure of infrastructure networks. We are therefore investing in research to develop the advanced, intelligent solutions that we need to increase our security without interfering with our culture of personal freedom. We need new knowledge because we cannot just transfer the available solutions to new challenges. The Federal Government therefore presents its first programme on research for civil security.

Security research is one of the central fields of innovation of the comprehensive High-tech Strategy for Germany. The programme provides a platform for strategic cooperation between business and administration, research and application. It is addressed to the operators of security-relevant infrastructures in such fields as transport, water and energy as well as to companies which are developing innovative security solutions. The development of security products and systems is an important factor in a globally expanding market. German

companies' technological performance and their international competitiveness also depend on the availability of security technologies.

Security always means security of people. Dialogue and transparency are indispensable prerequisites for the success of the entire security research programme. From the outset, consideration must be given to the use of advanced security systems as well as the handling of security technologies and their acceptance. The humanities and social sciences are therefore as important for the development of innovative security solutions as the natural and engineering sciences. We must conduct a broad social dialogue to address the ethical, legal and social science aspects of security research. The aim of security research is to protect the population. We want to maintain security in our country while preserving the prosperity and freedom of people living here.

A handwritten signature in black ink, appearing to read 'Annette Schavan'.

Dr. Annette Schavan, Member of the German Parliament
Federal Minister of Education and Research

Contents

Summary	5
Part I: Strategic direction of security research	7
Objectives of the security research	8
Initial situation	9
Guidelines	10
Reinforcement of interdepartmental co-operation	10
Orientation to end users and markets	11
Link between technological and social issues	13
European co-operation and international research alliances	14
Ultra-wideband radio helps save human lives	15
Part II: Support programme	17
Objectives of the support	18
The agenda process for preparing the programme	20
Support programme lines	21
Programme line 1 “scenario-oriented security research“	21
Programme line 2 “technology interconnections“	21
Scenario-oriented security research	22
Protection and rescue of persons	22
Evacuation techniques	25
Detecting explosives	27
Protection against failure of the supply infrastructures	28
A false sense of security – how safe is safe?	31
Protection of transport infrastructures	32
Avoiding cascade effects	35
Securing the supply chains	36
Technology interconnections	38
Integrated protection systems for emergency and security services	38
The fire service of the future	39
Multi-sensor systems for cbrne risks	40
Nanotechnologies in the battle against bioterrorism	41
Pattern recognition	42
Biometry for personal identification	43
Reconnaissance robots	45
Biometrics	46
Implementation of the support programme	47
Support instruments	47
Duration of the programme and funding	47
Appendix	49
Ongoing activities of the federal government in relation to security research	49
Glossary	55



Summary

Germany is one of the safest countries in the world. The major confrontations of the Cold War are a thing of the past, Germany has been reunified and is surrounded by allies.

However, new threats have arisen, only some of which are attributable to possible external influences. Modern industrial society is thick with infrastructure networks that provide for mobility, energy and information flows and hence make efficient economies in Germany possible. These networks also reach critical points when they are operated at the limit of their capacity. Attacks using comparatively few resources could have a major impact on these.

Global mobility also comes at a price: viruses can now travel around the globe in just a few hours in aeroplanes, a situation that concerns epidemiologists. Even with the relatively limited transport of the time, the Spanish Flu of 1928 caused devastation. Increased mobility has resulted in a growing number of major events – world championships, youth gatherings – which, simply because of the huge numbers of people, bring their own risks and on which the world's television cameras are trained, which in turn makes these events attractive targets for attack.

Moreover, technological society has created not only convenience but also new ways of making highly-effective weapons available to small groups, which could use them to build up political pressure. Anthrax is one example – biological methods are widely available – and one legacy of the Cold War is the number of dubiously-secured radioactive substances that were left behind.

Natural catastrophes and major technical accidents can also trigger major consequential damage in a densely-networked world.

The Federal Government is launching this research programme to combat these and other threats to civil security. The programme is firmly incorporated into the high-tech strategy for Germany which, for the first time, is striving to achieve a common interdepartmental innovation policy. In addition, the security research programme is geared towards close collaboration with member states of the EU, and stra-

tegic research alliances with non-European states are being built up, which could build particular strengths in security issues.

The programme is expected to result in innovative solutions to improve citizens' security without restricting their freedom. Security cannot be achieved by technology alone. Technological and social issues are linked and new security solutions are accompanied by a social dialogue.

The programme is also market-oriented. The market for security technology and services was worth EUR 10 bn in Germany in 2005 and its global growth is 7 to 8% per annum. With its efficient, varied and contemporary research (microsystems technology, optical technologies, sensors etc.), Germany is very well equipped to serve this market. The close integration in Europe means the programme can create the conditions for economic success beyond Germany's borders.

The support is concentrated in two programme lines. Programme line 1 comprises „Scenario-oriented security research“ from the problem-solving perspectives of end users and is geared, among other things, to improving collaboration between the authorities and private operators of security-related infrastructures. The core elements of the support are the protection and rescue of people, protection of transport infrastructures, protection against failure of the supply infrastructures and securing the supply chains. The focus is not on individual technological results but on forming a community of players.

The goal of programme line 2 is to research inter-disciplinary technologies in “technology interconnections” that are required in many scenarios such as methods for rapid and reliable identification of persons, rapid identification of hazardous substances etc.

The initial support period for the programme from 2007 to 2010 will also form the basis for a long-term, targeted and flexible support policy. Around EUR 123m will be available for 2007 - 2010 in addition to the departments' budgets for security research.

Strategic direction of security research



In its second periodic security report of November 2006, the Federal Government noted the good security situation and the high level of safety in Germany. At the same time it noted that the threat from terrorism or extremist attacks is high.

Moreover, the main threats to modern society are the spread of weapons of mass destruction, regional conflicts, the collapse of states and organised crime, which are also cited in the European Union's security doctrine. The threats are mostly from small groups of ideologically or criminally motivated perpetrators but can affect many people. In extreme cases, attacks on vital infrastructures such as energy, logistics, information technology, telecommunications, transport, healthcare or the financial system could put the economic and social stability of a country in jeopardy. This is possible owing to the existence and availability of weapons and hazardous substances together with the complexity of the networked, globalised society which offers innumerable neuralgic points that can be targeted with limited resources to achieve a major effect. The key goals of (the) German security policy, therefore, are to protect the population, to reduce the country's vulnerability and to combat the causes of terrorism. The development of appropriate technologies and strategies as part of the civil security research is intended to help achieve these goals.

Security research also needs to develop solutions to minimise the effects on society of natural catastrophes or major incidents, whether they affect health and agriculture, drinking water and food, the energy sector or other vital infrastructures. The increasing concentration of the population in major conurbations, the growing interconnection of the most varied aspects of life and the development into a global information and service society result in a new type of vulnerability. The capacity of familiar methods and organisational forms to implement protection and security measures is therefore limited. New threats and risks, including those resulting from society's new vulnerabilities, require a new approach to security, new competences and qualifications and new technologies.

The Federal Government has laid down its security research programme as a focal point of the national high-tech strategy. This framework provides the ability, through research and innovation, to support the competitiveness of the participating companies and the marketability of the security solutions they develop, to establish security as a national location and economic factor and to open up organisational scope at the European level. The European Union has also accepted the challenge and launched its own security research programme.

Objectives of the security research

Research and innovation will provide the civil security policy with new tools to protect our democratic state and its people from threats. The purpose of security research is to analyse risks to our society and to develop new solutions to minimise or avoid them.

The security research programme centres on improving the protection of citizens in Germany against old and new dangers. Combating the new dangers, in particular, demands highly developed technologies in new security systems and associated new strategies.

The targeted innovative security solutions are intended to help increase people's security without restricting their freedoms. On the contrary: freedom of activity that has already been restricted by the threats can be regained through improved security systems e.g. by means of optimised and innovative detection technologies at airports.

The necessary considerations regarding the consequences of dealing with the new security systems and their acceptance can only be determined in a public dialogue in society. Another objective, therefore, is to initiate this dialogue.

Security research can only be effective in an international, or at least in a European context. International research alliances, European research collaboration and joint design of the European security architecture are therefore further objectives of the security research programme.

Reception in Munich airport: Complex establishments frequented by many people require elaborate security engineering, which should not constitute an intrusion.



Initial situation

The initial situation in Germany, which includes a wide variety of research support, intensive research activity in universities and non-university research institutes and strong traditions in natural and technical sciences as well as the humanities and social sciences, forms an excellent environment for security research.

The level of security in areas such as facilities and reactor safety, transport safety, food safety and chemicals safety is already exemplary but can be further optimised and refined through well-developed basic technologies.

However, security research for the new challenges that have been identified requires new qualities. Existing security solutions will not always be able to counter future threats. The many players active in the security sector (authorities, infrastructure operators, security and emergency services, providers of technical security solutions, researchers) do not currently have any common platforms to enable them to deal with questions about future threats and potential solutions systematically and in a co-ordinated fashion on a national basis. Therefore there is no adequate agreement on the priorities for research. So far it has not been possible to establish collaboration appropriate to the future challenges between the federal research institutes and other public research and development facilities and industrial research. The landscape of users and operators of security solutions is fragmented and lacks an agreed approach.

The list below summarises this situation and the resulting opportunities and risks.

Strengths: Strong basic technologies: good position in terms of microsystems technology, ICT, optical technologies, structural engineering, biotechnology and sensor technology. Varied research: wide-ranging research landscape, including in departmental research.

High level of security: high standard of incident and accident security (e.g. plant and reactor safety, transport safety).

Opportunities: Protection against dangers and crisis response capability: improvement of security technology and its interoperability, widespread distribution of civil security technologies through cost-effective solutions. Expansion of the market position: increased market shares and improved export opportunities for German companies. Reinforcement of core competences: support for national industrial companies with strategically important skills for security solutions. Technology transfer: tap high technology from other civil areas and the military for civil security applications. Reinforcement of synergies: employ common security solutions used by the authorities and private individuals, utilise European opportunities. Combine competences from technology, the humanities and social sciences.

Weaknesses: Innovative civil security technologies: no research programme for civil security that taps the basic technologies for system innovations. Some security technology obsolete: procurement insufficiently geared to innovations. Still little co-ordination: no platform that combines the players from research, industry and the authorities on a national basis and develops priorities for the research requirement for civil security. Co-operation in research: co-operation between departmental research facilities and other public R&D facilities and industrial research has not been specifically supported to date. Fragmentation: heterogeneous user landscape, too few players specialising in civil security.

Threats: Reasonable protection of classified information: limited dissemination of research results as a result of excessively rigid protection of classified information, flow of information to unauthorised parties as a result of insufficient protection of classified information. Societal agreement: lack of transparency of the planned activities as well as the effects of new technologies can lead to reservations amongst the population. Guarantee of civil rights: enhanced corollary research required to identify potential adverse effects on human rights and civil liberties at an early stage.

Guidelines

Reinforcement of interdepartmental co-operation

The security research programme is based on the analyses of causes and security (e.g. of radicalisation in Germany, of potential threats or of security gaps in infrastructures) carried out in the respective policy areas of the departments. It also allows new types of threats and causes and future security requirements to be dealt with in interdepartmental plans.

The Federal Government will gear the major research and development work in this context towards common goals in order to find ways of identifying and neutralising threats that have been deemed significant. Co-operation between security research and other research programmes in the Federal Ministry of Education and Research e.g. in technology research, life sciences, earth system research or the humanities and social sciences, will be strengthened and the co-operation between the research department and the department responsible for the policy area will be expanded. In particular, this applies to the Federal Ministry of the Interior, which is responsible for domestic security in relation to protection against terrorism and crime, protection of critical infrastructures, protection of the population and in the event of catastrophes, IT security and reinforcement of the security and emergency services, and the Federal Ministry of Transport, Building and Urban Affairs in relation to structural protection, the Galileo satellite navigation system and the se-

Contamination block against bird flu on Rügen – successful police and army co-operation in disaster prevention.



Supplying the country with millions of goods is largely achieved through night work. View from the signal box in Hamburg-Waltershof over the port track system of Deutsche Bahn AG.

curing of traffic and transport. Research into environmental protection and nature conservation and incident security will be supported jointly with the Federal Ministry of the Environment, Nature Conservation and Nuclear Safety and research into nuclear plant safety and air and space travel with the Federal Ministry of Economics and Technology. Co-operation will be intensified with the Federal Ministry of Health on bioterrorism, epidemics and pandemics and with the Federal Ministry of Food, Agriculture and Consumer Protection on



food safety, epidemics of animal diseases, pest management and plant health as well as agroterrorism.

The civil security research program is not concerned with military security research and is therefore not geared towards the goals of defence policy. The Federal Ministry of Defence's security research is geared to military tasks, intelligence, navigation, simulation, weapons, target approach, military networks, automatic and autonomous platforms, technical and medical ABC protection etc. Nevertheless, in principle the technological expertise acquired industrially in military projects can also be used for civil applications. Co-operation with the Federal Ministry of Defence will therefore relate in particular to the mutual transfer of knowledge and tapping of new applications that are significant for both the civil and military sectors.

Nowadays it is often no longer military but civil research that drives the development of new technologies. Innovative security technology will therefore benefit much more greatly, especially in terms of cost-effective solutions, from civilian high technology that can often be used for mass markets.



Crisis operations require the smooth co-operation of the various services

Orientation to end users and markets

In order to meet the need for security as accurately and as quickly as possible, end users are involved in the implementation of the projects. End users are authorities and state security and emergency services (e.g. police, Technisches Hilfswerk (Governmental disaster relief organization of the Federal Republic of Germany), fire brigade) as well as state and private operators of critical infrastructures (railways, energy and health sector, telecommunications, local public transport, airports, logistics etc.) Since around 80% of all infrastructures that are of interest for security are funded by the private sector, the Federal Government will use this programme to create additional incentives for the state and the private sector to work together and to minimise conflicts of goals as early as possible.

The demand for security creates assets and jobs. The market for security technology and services in Germany was worth EUR 10 bn in 2005 with growth rates of 7 to 8%. A market orientation for security research is advisable for the following reasons:



Deutsche Telekom AG Control Centre

- + **Only cost-effective security systems will become sufficiently widespread.**
- + **New security solutions can create new jobs and secure existing ones.**
- + **International competitiveness in security technology can only be guaranteed if core industrial skills in Germany are maintained and strengthened.**
- + **The state can generate demand for security solutions and thereby create a pioneering market and make it easier for providers in Germany to launch new technologies. This creates significant opportunities for new markets and exports specifically in terms of the security sector.**

Security technology is an increasingly important market for Germany. Security products and services are not only procured by public and private sector end users and infrastructure operators, there is also demand from all sorts of companies and, increasingly, from individual consumers. The demand is partly driven by state regulations (e.g. requirements for air

traffic safety), but is also fuelled by purely economic considerations (e.g. securing business processes, maximising availability, preventing a drain of expertise). Consumers demand security when travelling, or using ICT or in logistics.

New technologies are a necessary element of the security research programme, if not indeed sufficient in their own right. But when incorporated into well thought-out strategies, they are a key component of future security solutions.

- + **The latest security technologies can help the emergency and security services respond to new threats more quickly and effectively.**
- + **Our vital infrastructures are increasingly intertwined. Only if the progress in this area is accompanied by innovative security technologies can any new security gaps that may arise be bridged.**
- + **The introduction of new technologies can bring not only the desired effects but, occasionally, it can also bring about new vulnerabilities and even the risk of**



Flight luggage regulations are becoming ever stricter. Automatic detection processes for dangerous objects and materials will make the whole process quicker, safer and more pleasant.

abuse. Security research must therefore cover critical questions about potential side-effects in the run-up to the launch of new technologies – for instance in goods logistics, communications or deployment control technology.

Mobile control points depend on efficient communication media.



Link between technological and social issues

Security technologies are inter-disciplinary technologies requiring contributions from different technical and scientific disciplines. However, security cannot be achieved by technology alone as it always depends on human actions. The way those under threat behave, e.g. in panic situations, can actually be a potential for danger and quite often dangers only become acute as a result of human error - including and especially when dealing with technical systems. Security solutions that are not accepted by potential users and the citizens to be protected would have a limited effect or even be counter-productive. Thus in the same way that road safety is not achieved purely through technical precautions or legislation, but only if the road-users themselves agree with the measures, security solutions designed to protect against threats of any type must be accepted by each individual.

Technological and social issues must therefore be linked in security research. Contributions from research in the humanities and social sciences are expected especially in relation to

- + the need for and acceptance of security solutions and their effects and consequences
- + the risks of restrictions on freedom
- + the costs and benefits of security measures and strategies
- + the causes of threats including terrorism and extremism, the associated potential for radicalisation and the resulting new security demands
- + suggestions for improvements in crisis management i.e. in relation to the behaviour of individuals and social groups in the event of crises and catastrophes and how they deal with them, answering of legal questions and informing the population in case of a crisis or catastrophe
- + the options for the establishment and preservation of effective institutions to prevent and counter crises (systems-theory and organisational/sociological analyses)
- + the need to build up competences and skills of people handling innovative security solutions.

The security research programme should be accompanied by a social dialogue since its goal is to protect our freedoms, not to restrict them. It will be as transparent as possible and the public will be given detailed information about the topics being researched and the opportunities and risks of the new solutions.

European co-operation and international research alliances

The expected future threats do not respect national borders; they are global and must be viewed on a correspondingly large scale. In Europe, this requires close co-operation between the member states.

In its 7th framework research programme (duration from 2007 to 2013), the European Union will for the first time provide around EUR 200 m of funding annually for a European security research programme. It is geared to four "missions":

- + **Protection against terrorism and crime**
- + **Protection of critical infrastructures**
- + **Restoring security in case of a crisis**
- + **Border security.**

The Federal Government successfully argued that the European security research programme should be set up in line with national security research. Thus both the European and German security research programmes will concentrate exclusively on civil security solutions. Both programmes will involve private sector end users and will focus on strengthening competition.

As in many other fields of research, bridges must be built between national and European security research:

- + **Many future security solutions will only be effective if they are implemented on a Europe-wide basis in conjunction with EU member states.**
- + **Competitiveness can often only be achieved if critical mass is reached across Europe in the respective fields of research.**

- + **The deployment of new security solutions must be accompanied by European standardisation initiatives and legislation and regulations that are conducive to innovation.**
- + **The successful involvement of German players in the European security research programme requires intensive co-operation with the European partners and must be targeted through appropriate national consultation and support for the applicants.**

However, the European programme is not a substitute for member states' national programmes. Like other EU member states who are also planning their own security research programmes, or indeed have already launched them, the German programme has its own focus and concentrates on specific security requirements, standards and general conditions e.g. its central position in Europe, its highly-developed infrastructures, its cultural and social idiosyncrasies and its particular strengths in research. Both participation in the European programme and the active shaping of the European security architecture require individual strengths to be brought to the table. This will accommodate the market orientation of the national programme which is also useful for the country's own export efforts.

Germany will strive to play an active part in civil security research to develop solutions to global challenges such as international terrorism, including by means of international research alliances. These will allow knowledge that is available around the world to be used to the benefit of the national programme objectives. In particular, bilateral co-operations will be set up with states with specific strengths in civil security research.



Destruction following the earthquake in Bam, Southern Iran in December 2003. Signs of life (breathing, heartbeats) were distinguished beneath the rubble using UWB radar.

Ultra-wideband radio helps save human lives

Even technophobes have had to admit that over recent years, computer technology has not only become crucial but also has acquired a degree of elegance. We have flat multi-tasking notebooks with screens offering brilliant, natural colour, flatbed scanners that produce professional scans at amateur prices, tiny, fast hard disks for video editing. Only one thing detracts from workplace aesthetics and mobility, and that is the mare's nest of cables. But an end could be in sight, if new Bluetooth technologies such as WUSB become established. "Wireless USB" is radio link technology using ultra wide band (UWB) technology. UWB technology could fill the domestic atmosphere with a kind of electronic fog, into which every compatible appliance (notebooks, scanners, cameras, TV sets etc.) can dip with the aid of its radio interface, and via which they can automatically network and communicate. The electro-smog need give us no cause for concern, since it would be finely dispersed, with radiation levels of a mere fraction, perhaps one thousandth, of that emitted by a mobile phone. In the summer of 2006, functioning WUSB chips and applications were presented in the USA. At 480 Mbit/sec., the data transmission speeds are so high that it is even possible to transmit High Definition TV, albeit at limited range.

There is no alternative to this limitation to its range, because UWB is a radio technology that uses a very broad band of frequencies, including those already used by other applications. However, the UWB signals are so weak that they do not disturb other applications (although some dispute this). As a result, UWB is designed to act as unlicensed radio technology, for example in WLAN systems. The technology could relieve the industry of its problems associated with the shortage of frequencies, and its speed and functionality is so attractive that it is bound to become a part of everyday life. The networks clamouring to establish it include the giants of entertainment electronics.



Rescued and treated, for now.

UWB is a typical example of technologies whose groundbreaking possible uses and potential risks represent two sides of the same coin. Already trialled 60 years ago on warships to achieve low-interference radiotelephony technology, UWB technology may now become an important component of many applications in our immediate environment. Using RFID tags (radio labels), three-dimensional locating systems can for example be produced, using which the positions of thousands of different radio labels can be located simultaneously to an accuracy of ten centimetres. If these labels are attached to tools, for example in a large aircraft maintenance hangar, then there will no longer be any need to look for things. In hospitals, patient and staff whereabouts can be tracked, in refineries, the location of staff can be established in the event of a disaster.

The US military has since developed a kind of UWB radar, using which movements can be detected, even behind thick walls. Rescue teams could use the radar to find people buried beneath the rubble of an earthquake or under the snow following an avalanche. The UWB radar is capable of detecting breathing or even heartbeats through walls.

In addition to monitoring and safety engineering in the building industry, the food industry, environmental protection, production monitoring and control, transport and vehicle engineering, UWB sensors can also be used in humanitarian mine detection. In the EU RADIOTECT programme, the usability of a UWB-based ground radar to detect mines is one of the uses under investigation.

The UWB radar is likely to initially find a mass market in civil automotive engineering, as a distance radar to maintain safe distances on motorways.

Support programme





The Federal Government's security research program for the first time puts research into civil security into an overall context. The purpose of the support is to develop innovative solutions – including procedures, products, strategies and networks - to increase the security of citizens. Issues such as standardisation and quality assurance, harmonisation of system solutions, development of yardsticks for uniform risk analysis and evaluation of the effectiveness of measures and technologies are just as important as the accompanying social dialogue and analysis of international developments.

Objectives of the support

The functional objectives centre on three areas in which significant success can be expected:

1. Innovative security solutions to reduce the vulnerability of vital infrastructures:

in particular these infrastructures include information and communication systems, transport systems, energy facilities and networks, facilities for the supply and distribution of food and goods, institutions in the financial sector and health and logistics facilities. These infrastructures are increasingly interdependent. Only if progress in this field includes innovative security solutions can we ensure that more benefits and comfort do not result in new vulnerabilities.

More than ever, security in this particular field requires co-operation between the state and the economy. In infrastructures in particular, sovereign responsibilities have been largely privatised in the past. German industry, as a global leader in exports, is particularly reliant on these infrastructures functioning. Its geographical position in the centre of Europe makes Germany the location of choice for international logistics companies and major transnational service providers. The security research programme contains incentives for improved research co-operation between the authorities and private-sector infrastructure operators. In this way, protection against terrorism, sabotage and organised crime should be added to the given high technical security against failure of key German infrastructure.

Whereas in the event of attacks on a coal-fired power station (RWE AG, Weisweiler) the damage would be limited to a localised area, attacks on a nuclear power station could have very far-reaching consequences.

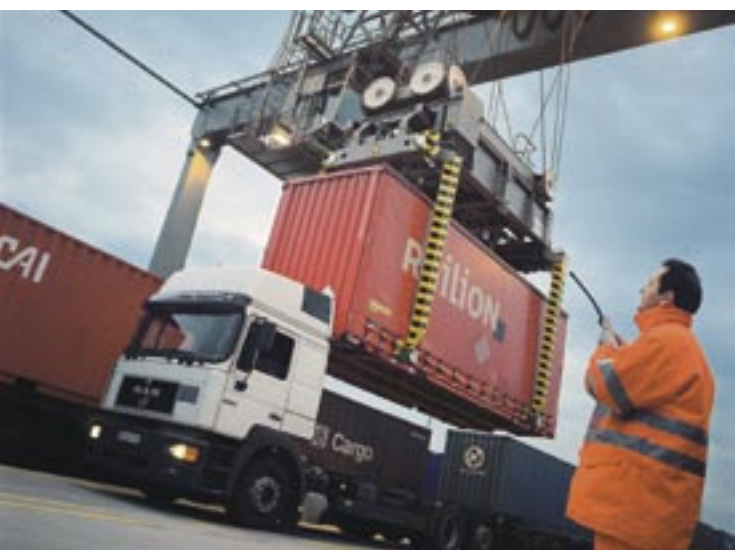




The modern communication possibilities of “digital police radio” are essential for effective policing.

2. Innovative security solutions to strengthen the emergency and security services:

these organisations (police, fire brigade, medical relief organisations, Technical Relief etc.) will work with universities, institutes and industry to develop solutions to effectively counter future threats by means of prevention and response. Given the



current acceleration in the speed at which threats change and the technical progress, it is not enough to equip the emergency and security services with more modern technology from time to time. The security research will create the conditions for delivering appropriate innovative solutions for technical equipment, organisation and handling strategies.

3. To tap the market for security solutions:

the security research programme will promote the competitiveness of the companies involved as well as the marketability of security technology in general. Demand for security also creates added value and jobs. The market potential of new security solutions should also be tapped to keep highly qualified jobs and owners of industrial expertise in Germany. There is a broad spectrum of industrial core competencies in security-related technologies (e.g. ICT technologies, biometrics, robotics, space travel) in Germany with roots in both defence and civilian areas. This strategically important industry will be given incentives, as part of the security research, to build on its competitive position. The security research programme will also ensure that players from Germany achieve an advantageous competitive position in research co-operations at European level. The support for the national security research programme will select projects to ensure that appropriate solutions that are representative at European level are developed. A national contact point for security research will be set up to support German players with advisory services.

Frankfurt am Main container handling station. The number of containers currently in use in transport facilities around the world is estimated at around 100 million.

The agenda process for preparing the programme

The direction of the security research programme, its objectives and content have been defined jointly with science and business.

As part of the preparations, a comprehensive dialogue of experts, the „agenda process” was carried out. In this process, three experts’ workshops held between April and June 2006 brought some 250 experts together from all areas of relevance to the security research. The purpose of the agenda process was to define topics, form strategies and set up the experts’ scene. The following were represented:

- + **Scientists from universities, non-university research institutes, departmental research facilities, companies and consumers**
- + **Scientists from engineering, natural sciences, the humanities and social sciences**

- + **End users (private-sector infrastructure operators, public-sector consumers at both national and regional level)**
- + **Providers of security technology (industrial companies).**

As part of the agenda process, the research requirement was ascertained by end users and the focus for the research and development of future security solutions was identified. The top priority security research scenarios were developed by combining requirement and solution perspectives. These scenarios outline the future requirement for innovative security solutions and describe areas in which new solutions can be expected based on more intensive research. The result of the workshops was a collection of research topics in technology, the humanities and social sciences on which focus needs to be centred.

The security research programme has been prepared in a comprehensive agenda process.



Support programme lines

Programme line 1 “Scenario-oriented security research“

In this programme line, the research will focus on solutions for complex security scenarios to incorporate the end users’ problem-solving perspectives into the research from the outset. Using the scenarios guarantees that all the technology, science, humanities and social sciences disciplines that are needed to develop viable security solutions are involved and geared towards common goals. The scenarios also provide a platform for the authorities and private sector players to collaborate as operators and providers of security technology. The use of scenarios ensures that appropriate system innovations are favoured over isolated individual questions and solutions. These system innovations integrate both existing and new technologies. They are based on threat analyses and take

For human and environmental security, there are now various burglar and fire alarm points available – from Bosch – with numerous interfaces.

account of cost-benefit analyses as well as the attitudes and behaviour of both individuals and groups and their dynamic. How can citizens make a greater contribution to reducing or even totally avoiding potential dangers in a crisis? How can errors be avoided in, for example, panic situations? In this way, scenario-oriented security research not only satisfies the actual security requirement but is also geared to a rapid implementation of the results.

Programme line 2 “Technology interconnections“

Certain security technologies are required in many or all scenarios. These include technologies for rapid and reliable identification of persons, rapid and mobile identification of hazardous substances, pattern detection and boosting deployments of security and emergency services. The technology interconnections tap basic technological knowledge that is important for security research and develop innovative technology systems from existing and new basic technologies. They work at application level by involving the entire innovation chain from the research via industry to the end users.

In the technology interconnections, reasonable accompanying research will address ethical questions, perform innovation analyses and examine legal or technical consequences in order to prepare any corrections or additional measures that may be needed.

Both programme lines will give high priority to issues such as the acceptance of technological developments, sources or threats, data protection or the impact on human rights and civil liberties as part of accompanying research. The accompanying research will place particular value on the transfer of knowledge to the public domain. Publications, workshops and discourses among the participants will reinforce awareness of security-related issues and support research-policy decision-making. Dialogue and transparency are regarded as an important pre-requisite for the success of the whole.



Scenario-oriented security research

Protection and rescue of persons

The showcases of major events, as well as busy public areas, are neuralgic points at which minor and even unintentional incidents can have a catastrophic impact. This makes protection against terrorism even more urgent in such situations, especially if the attackers want to be sure of achieving media coverage since the amplification of the horror by the media is generally part of the terrorists' calculations. Innovative solutions for prevention and crisis management of such events also increase the security of more everyday situations such as accidents, medical emergencies or criminal activities. It can also be assumed that the global increase in mobility will make critical densities such as major international events more and more probable. The population can nearly double in such situations, even in large cities.

In this scenario, therefore, a large number of people need to be protected in a small space. This requires innovative solutions to identify incidents at an early stage to either prevent or minimise a crisis. An effective response to a crisis also has a preventive effect. If the probability of factors that exacerbate a crisis, such as mass panic, can be reduced, major events become less attractive to attackers from the outset. Therefore solutions to manage and combat crises at major events act as a general indicator in terms of protecting the population in public places. The objective of security research in this scenario is the early identification of attempted incidents, the prompt initiation of rescue and combat measures and effective provision of emergency services on site.

Christmas markets – here in Cologne – are often mentioned as a target for attacks.





Relevant research topics:

- Sensor systems, detection, robotics

- + Image analysis systems for near-real time initiation of response measures
- + Algorithms for automated decision-making procedures
- + Standardised situation reports e.g. based on Galileo technology
- + Automatic personal identification procedures
- + Surveillance and sensor technology for unmanned aircraft

Image left: successful crime prevention and solving using video surveillance at the Munich Oktoberfest. Using 12 Bosch AutoDome cameras it was possible to solve a total of 89 crimes.

Image below: The World Youth Day of 2005 was also a challenge for the rescue and security forces.



- Simulation, pattern detection and data input

- + Identification of dangers supported by risk analysis and simulation tools and databases
- + Automated analysis based on scenario methods
- + Systems for modelling and automatic identification of social dynamic



Allianz-Arena Munich (below). In the background, security engineering – access control (on the right, with RFIDs, Siemens AG) security, building and information management – ensures smooth running of the events.





Evacuation techniques

The band “Brings” was still playing its evergreen hit “Superjeile Zick” (Beautiful Time) when the third bomb warning was received and the police decided to evacuate the Cologne arena, in which 8000 revellers were celebrating the local carnival. In the Cologne dialect, the announcer relocated “Brings” and invited the audience to create the longest conga line in the world, for the Guinness Book of Records, causing the crowd to flow out into the open, laughing and dancing, with Mayor Jupp Müller at their head.

This achievement on 20 February 2003, which was marvelled at even by security specialists, would perhaps not have been possible anywhere other than Cologne. In fact the bomb threat was a hoax, but there was no way of knowing this at the time. All the same, security specialists are extremely interested in ideas like this, since the evacuation of large crowds of people is a delicate issue. When a crowd develops agoraphobia, there can sometimes be no stopping them because, as Michael Schreckenberg, Professor of “Physics of transport and movement” at Duisburg University maintains, ancient behavioural patterns kick in automatically when people are under extreme pressure. If they are on in an empty field, they simply climb the nearest tree, but if they are in a football stadium, it can have disastrous consequences. He therefore investigated on a computer the patterns adopted by large crowds of people, in order for example to enable emergency exits to be better designed and to determine how to evacuate large cruise ships. According to Michael Schreckenberg, people always push one another away when they are bunched together, but draw together when they are far apart. “This is known as the herd instinct, which means that people follow others on the assumption that they know where they’re going, but then try unsuccessfully to push their way out of the crowd when they get into an enclosed space.”

Patterns emerge if such rules are fed into a computer. What is particularly impressive is the flocking behaviour of birds, which can be perfectly simulated. There are three simple rules: every bird first flies as fast as it can, then secondly tries to reach the protective centre of the flock without, thirdly, colliding with another bird. Based on these rules, a computer can generate a convincing flock of starlings.

The Cologne arena. Known as the “Laughing Cologne Arena”, the building was the scene of an exemplary evacuation in 2003.

Crowds of people also form patterns: department store owners know this and group their products in such a way as to create a positive atmosphere as people wander through. With the aid of a computer simulation (the specialist term is “Pedestrian and Evacuation Dynamics”), it is possible to break up avoidable bottlenecks, for example in front of a stadium exit. Undirected pedestrians tend to pause for air and look around at the exit, which brings the crowd behind them to a standstill. This problem can be solved by adding an additional pillar at the exit, which blocks the view and causes the flow of people to fan out, i.e. it adds an additional obstacle.

The annual pilgrimage to Mecca is an especially explosive subject of study amongst specialists. The Technical University in Dresden describes the situation as follows: “The Koran requires every Muslim to make a pilgrimage to Mecca at least once in their lifetime, in order to complete a precisely defined religious ritual (Hajj). Quite specifically, seven stones must be thrown at each of three pillars (Jamarahs) symbolising temptation by the Devil. The pilgrims may undertake this ritual at ground level or on the Jamarat Bridge. Up to 200,000 pilgrims swarm onto the 80 metre wide bridge in peak times. In past years, this has led repeatedly to tragic accidents, frequently involving over 100 deaths. In the most serious accident, over 1,400 pilgrims died.

Scientists in Dresden are now investigating how the area in which the throwing takes place can be geometrically configured in order to relieve the situation. “How effectively could the pressure within the crowd be avoided by creating a kind of breakwater set up along the elliptical throwing area, i.e. not against the direction of flow? Or how effective would zig-zag or S-shaped handrails be, to deflect the pressure of the volume of people and therefore create space behind those affected?” The findings obtained can of course also be applied to football stadia. The entertainment industry also benefits from this type of research. The crowds of Orks in “The Lord of the Rings” could not have been hand-drawn, they are computer-generated with a certain degree of autonomy, and they move according to the rules applicable to flocks of birds, which is why they are so convincing.

- Information and communication technology

- + Communications systems for mission control centres and positioning information
- + Mobile terminals with flexible access to positioning and deployment data
- + Systems to suppress radio-controlled trigger devices
- + Common semantic basis for management systems

- Prevention and response strategies and organisational forms

- + Mobility and speed of logistic systems for the relief units and emergency services.
- + Role of the media in the perception of threats and handling of crises
- + Investigation of potential for panic
- + Concepts to convey action perspectives for perilous and catastrophic situations
- + Situational behaviour according to CBRNE attacks

Floods – here in Baden-Württemberg in 2006 – are expected to be more frequent in future and require preparation accordingly.



*Explosives can be hidden in luggage.
New sensors are needed
to detect them.*



Detecting explosives

On 7 July 2005, the message displayed by the traffic signals on the M25 around London was apocalyptic: AVOID LONDON – AREA CLOSED – TURN ON RADIO. In the rush hour, at 8.50 a.m., terrorists had set off a series of bombs in quick succession on the transport system. Four underground trains and a double-decker bus were targeted. The bombs killed 52 passengers and the four suicide bombers themselves, and temporarily disabled London's entire transport and communications infrastructure. The horror was itself horrific: terrorism caused by freely available everyday substances, found in every ladies' hairdressers: nail varnish remover and bleach. With just a little knowledge, a highly effective explosive, triacetone peroxide (TATP), can be manufactured from their chemical components, although it can detonate unexpectedly.

As usual, modern industrial companies have a whole range of substances and techniques at their disposal, which can be used by determined people without proper scientific knowledge to wreak devastation, or at the very least to shock the media. The number of such opportunities is proliferating. It is seldom possible to withdraw potentially hazardous materials from circulation, as many of them, such as artificial fertilisers, are indispensable. However, it was precisely an improvised explosive device made of artificial fertiliser and an engine fuel additive that was used during the attack on the Murrah Federal Building in Oklahoma City in April 1995, killing 168 people.

If government security bodies are to cope with threats of this kind, then the technology accessible to them needs to be tightened up. The most important new tools needing to be developed in this context would be detectors, which are capable of discovering different kinds of explosives beneath clothing, in luggage, cars and lorries etc. Some such detectors do already exist, with one especially sophisticated design being based on the principle of x-ray backscatter ("Z Backscatter®").

A thin x-ray beam scans the suspicious area, whilst a detector with a large and hence highly efficient surface area, registers the x-ray radiation scattered back from the object being scanned. This method also allows objects to be recorded that are only accessible from one side, and also produces high

definition real-time images. On its website, the only manufacturer of such equipment to date shows a delivery van carrying the equipment being driven slowly along a line of parked cars, whilst the passenger looks at their contents on a screen. Contrary to conventional x-ray equipment, explosives made of light elements such as carbon, nitrogen and oxygen appear bright, as do a box of chocolates and also people. The manufacturer maintains that when scanning humans, the radiation load is negligible. The technology is also capable of picking up mines buried in the ground.

Spectroscopic methods may be useful when spotting explosives in the open, amongst a crowd of people. During baggage checks at airports, wiped specimens are taken from items that appear suspicious, such as Notebooks. These samples give off vapour when heated in an analysis device, which can be investigated on the spot for traces of explosives. However the procedure must be conducted at the same location, contrary to the method recently devised by the Technical University of Dusseldorf and the Fraunhofer-Institut für Chemische Technologien to provide evidence of the typical terrorist explosive TATP, which is theoretically able to detect traces of the material in the air wafting above the heads of people in a market. "Fourier Transformation Infrared Spectroscopy" (FTIR) permits measurement of a whole range of different types of air contamination using radiated heat, on a non-contact basis, over measurement distances of several hundred metres. TATP, which begins to vaporise at below room temperature, can also be detected in this way, although the concept requires further research and development work.

So who in the crowd is wearing the explosives belt? It will be possible in the future, using what is known as Terahertz Radiation, to find out using electromagnetic radiation from the as yet technically undeveloped frequency range between microwave (oven) and infrared (remote control). A Terahertz "radar" can be worn beneath the clothing and can even pick up ceramic knives that evade metal detectors. Such a sophisticated device could even undertake a kind of chemical analysis at a distance. The radiation is non-ionising and is therefore safe.

Protection of transport infrastructures

In a modern society, the various means of transport – road, rail, air, water – can, without exaggeration, be called its lifeblood. Their use has now become so finely balanced that even minor disruptions can have a far-reaching impact and cause considerable damage. If transport is cut off, it can become a disaster and destabilise society and business. The nodes in the transport system, such as airports, railway stations, dammed rivers and canals, bridges, tunnels, high-speed routes, are particularly vulnerable. It is absolutely vital to protect these neuralgic points. Furthermore, in an industrial society, large quantities of potentially hazardous raw materials and smaller quantities of chemicals that are actually toxic are transported. Attacks on such transports – in towns, on bridges, in tunnels – could have devastating consequences. Rapid and simple analysis of the substances concerned can make the difference between life and death.

Therefore innovative solutions to secure transport infrastructures are a particularly important objective of the security research. The focus is on prevention, early identification, increasing redundancy (functionality in all possible crisis situations) and increasing the performance of the emergency services in a crisis. The security solutions should take account of efficiency, user and customer-friendliness, the involvement of individual and group behaviours and legal aspects.

Relevant research topics:

- Simulation, pattern detection and data input

- + Automatic access control with integrated biometric systems
- + Mass-sensor based monitoring of transport systems (e.g. for transport of hazardous cargos)
- + Surveillance robots and robots to combat dangers
- + Automatic identification of critical behaviour for security, systemrelated and individual-related

- Simulation, pattern detection and data input

- + Modelling of damage (e.g. spread of fire)
- + Simulation-supported risk analyses for decision-making
- + Early warning systems with real-time data transmission





Germany has a dense transport infrastructure, including approx. 232 thousand kilometres of regional roads (over half the distance to the moon), 44 thousand kilometres of rail (more than the circumference of the earth) and 7.5 thousand kilometres of waterways. 150 million people are transported over Germany by air every year (source: federal statistics office). If this infrastructure alone is threatened, efficient protection is impossible without new technologies.

- + **Inclusion of the “human factor” in simulations and modelling**
- Information and communication technology
 - + **Interoperable ICT systems for area-wide surveillance and security**
 - + **Simulation software solutions for crisis exercises**
- Strategies to increase the robustness of systems, procedures and processes
 - + **Structural measures and architecture that is conducive to security**

- + **Human-machine interfaces in detection and monitoring systems**
- + **Shielding of electronic devices against electromagnetic fields**

- Prevention and response strategies and organisational forms

- + **Networked crisis management systems**
- + **Non-discriminatory procedure for checks on people**
- + **Concepts for crisis-related public relations**
- + **Concepts for involving citizens and customers in crisis prevention and response**

Containers in the port of Hamburg. In 2004 over 11 million standard containers were handled in German ports; annual growth is at 30% (source: federal statistics office).





A false sense of security – how safe is safe?

Picking up the keys at the car hire firm in Valetta, Malta, was an unforgettable experience. When asked what rules had to be observed in relation to rights of way etc., apart from driving on the left, the man raised his eyes heavenwards, threw his arms open and replied “No rules, absolutely no rules!!” If in doubt, stop. Something that sounds so comical - these Southern Europeans - has now also become the norm in Northern Europe. In the municipality of Bohmte in Lower Saxony, the centre has been redesigned by Hans Modernmann, a Dutchman who wants just two rules to apply: driving on the right and giving way to traffic from the right (as a concession to the Northerners, one rule more than in Malta). Bohmte has rediscovered the concept of shared space, under which the uncertainties of the colourful mix of participants mean that the traffic slows down to the extent that people can see the whites of one another’s eyes. Enough to reach an understanding. The accident figures are falling, the signs have been removed, people can breathe. As part of an EU project, seven European cities are currently trialling the concept of “greater security through greater insecurity”.

The principles applied by Social Sciences and the Humanities confirm Modernmann’s experiences. An unconscious risk limit clearly exists, and it differs from one individual to another. The increase in security achieved through the introduction of technical systems is often offset by more risky behaviour, the technical term for this being risk homeostasis, or “the sum of all loads remains equal”. In contrast, taking greater risks generates more cautious behaviour.

An in-depth psychological pilot study has also demonstrated, in relation to IT jobs, that excessive security concerns can

be counter-productive. In the words of an expert, a computer network that is absolutely secure behaves like an entirely sealed new building. If no air penetrates, mould begins to form. This means that too much concern for security, for example constant monitoring of the content of the computer by managers, or even the possibility of such monitoring, demotivates people.

Insurance specialists such as Rudolf Kreutzer at Allianz Zentrum für Technik GmbH, confirm the premise that “the better the brakes, the closer people drive” and “protecting something from a source of risk [...] does not always result in low risk in the long term. For example, the construction of dams along riverbanks does reduce the frequency of claims. But after building them, the flood materials carried by the water are heavily deposited on the river bed. This results in the water level rising, making it necessary to increase the level of the dyke still further and constantly increasing the potential risk associated with the size of the claim. This was experienced during the last spectacular flood disasters on the Oder, Elbe, Po and Mississippi, and can be expected in the future on the Rhine, Danube and Inn.”

The general public’s perception of risk occasionally becomes irrational, and is also fuelled by the media’s compulsion to provide interesting news. As an example, people were so scared that they even stopped consuming milk and cheese during the last BSE crisis, but they happily continued smoking. The risk of smoking is known to be high but is familiar, the risk of BSE was uncertain but was new.

Protection against failure of the supply infrastructures

The supply of energy, water, information and communications, financial and health services and food to households, companies and public facilities is based on complex networked infrastructures, some of which are Europe-wide. The supply infrastructures are becoming increasingly complex, increasingly intertwined and dependent on one another. The domino effect of an incident in a central infrastructure element, such as a network node, can affect many people and extend beyond national borders and have a knock-on effect on other infrastructures. Electricity is the elixir of modern life – and its Achilles' heel. A power failure of long duration would have disastrous consequences. The railways would come to a halt, as would air traffic, and cars would not be on the road for long either – petrol stations cannot operate without power. Even power generation itself could suffer permanent damage. Communications networks would fail, the Internet, gas pipelines would transport no more gas and gas central heating in houses, even if the gas supply were intact, would not provide any more heat, refrigeration units would no longer cool – nothing would work. There may be various reasons for a supply infrastructure to fail: targeted terror attacks, criminal activity, industrial accidents or natural disasters (earthquake, flood, hurricane, heavy snow etc.). Since the networks are extremely widespread, the protection of major infrastructures must be put in place where multiple dependencies mean that particularly high levels of damage could occur.

The large number of factors that could cause an incident makes it clear that a wide range of different technologies and strategies is required to protect supply infrastructures. It is not enough simply to build on what already exists; true innovations are needed. The efforts to protect the public from terrorism and crime will therefore pay for themselves because they also improve the stability of the community in relation to natural catastrophes and accidents.

Increased ICT security plays an important role in this context. The security of all infrastructures – not just the ICT infrastructures (telephone, Internet, cable and radio) themselves – is increasingly dependent on the security of the information and communications technology. Specific research tasks can be derived from this. Provision must be made to ensure that, for example, the expected penetration of Internet technologies into areas outside communications technologies, such as

process control systems and financial systems, does not lead to a new type of vulnerability. Since the Internet is a unique and increasingly significant supply infrastructure, it must be specially protected against attacks in which its failure could destabilise society or business. The objectives of the security research in this scenario are prevention, early detection, isolation and intelligent delivery of emergency reserves, securing basic provision in a crisis and rapid restoration of the original supply status.

Europe by night. The light reflects the population density and illuminates the European-wide network.



Power networks are the lifeblood of industrial society; it is essential that they function smoothly. Eighty percent of this type of infrastructure is operated privately.





Deutsche Telekom AG switching centre. Communication hubs such as this one require special protection.

Relevant research topics:

- Sensor systems, detection and robotics

- + **Mobile autonomous multi-sensor platforms and low-power sensor systems**
- + **Distributed sensor networks, wireless sensor systems and robust sensor software for extensive surveillance**
- + **Systematic status recording of factors that could lead to a area-wide failure of supply structures**
- + **Standardised interoperable carrier systems (e.g. robots, unmanned aircraft, satellites)**

- Simulation, pattern detection and data input

- + **Use of geo-information systems to generate a “risk atlas”**
- + **Modelling of damage scenarios, in particular IT risk profiles**
- + **Tools for ongoing systematic recording of the security situation**
- + **Systematic risk analysis and evaluation for damage prediction**
- + **Early warning system integrated into critical infrastructures**
- + **Automatic exchange of Operational Pictures**

- Information and communication technology

- + **Robust process control systems and corresponding test tools**
- + **Ad hoc networks for disaster and emergency management**
- + **Secure basic platforms and operating systems for process control technology**

- Strategies to increase the robustness of systems, procedures and processes

- + **Research into interdependencies and systematic analyses of vulnerability**
- + **Failure planning and management**
- + **Management systems to support decision-making in a crisis**

- Prevention and response strategies and organisational forms

- + **Improved methods to co-ordinate responsibilities**
- + **Interaction of new technologies and organisational structures**
- + **Analysis of future vulnerability of infrastructures in terms of security**



A vast infrastructure network is needed to supply a major city like Berlin.

Avoiding cascade effects

An important element in the failure of complex systems can be studied in any canteen, simply by walking through with a cup of coffee full to the brim and the firm intention not to spill any. If you look down at the surface of the coffee, you will attempt to offset any swishing motion by a counter-movement, which often goes wrong. If the counter-movement is a little too energetic, then the coffee swishes around even more, causing you to increase the counter-movement, your hand starts to shake and the coffee spills over the brim. In technical language, the person/coffee cup system has fallen victim to self-excitation through positive feedback. The principal cause may be a tiny disturbance, although the background is obvious: the cup was too full!

Similar mechanisms, the build-up of problems in a network at the very limits of its efficiency, may possibly be the cause of many blackouts, such as the loss of power in Europe on the evening of 4 November 2006 that affected millions of Europeans. The superficial cause was the cruise ship, the “Norwegian Pearl”, travelling from the Meyer shipyard and passing beneath two high voltage lines, which were temporarily turned off for this purpose. The load was automatically taken over by other lines, whose sensors reported an overload, which caused these lines to also automatically switch off, and so on. The power returned after 30 minutes. The company responsible claimed failures on the part of two employees, who should have assessed the consequences of switching off the lines above the Norwegian Pearl in advance, via a computer simulation, but who failed to do so. However, these lines could also have failed for other unpredictable reasons, which should not under normal circumstances lead to the breakdown of the entire system.

Industrial nations are now disturbingly dependent on the constant availability of electrical power. In the words of the Bundesamt für Bevölkerungsschutz und Katastrophenhilfe [German Federal Office for Civil Protection and Disaster Assistance], BBK: “Without electricity, the cities and conurbations of modern societies are suddenly laid low, since virtually every element of their infrastructure is directly or indirectly dependent on the availability of electrical power.

Even extremely brief failures can have serious effects on other parts of the infrastructure, such as Electronic Data Processing (computer crashes), traffic management (traffic light control) and other sensitive electronic systems.”

Even modern private households would be seriously affected by a lengthy power cut.

“Without electricity, nothing works in many households. In a worst case scenario, this means no light, no heating, no hot water, no cooking facilities and no information and communication systems such as television, radio, telephone and computer.”

Mains faults can also originate in highly sensitive plants such as nuclear power stations. On 25.7.2006, a short-circuit in an outdoor substation upstream of the Swedish nuclear power station Forsmark 1 resulted in the automatic removal of the station from the main grid. The switchover to the necessary emergency supply did not go to plan. Two diesel emergency generators failed to come online because, as can be deduced from a report from the Reactor Safety Association, their regulators were fed from the very power sources that had failed, whose failure they were designed to offset. An auxiliary gas turbine failed because of a defective processor. Vapour was emitted in the machine shop, which smoke alarms interpreted as smoke, triggering the order to evacuate the power station. This did not happen because the loudspeaker equipment had failed, and so on. The power station was brought back under control thanks to a capable operations team and pure luck.

Protection of the electricity grid is therefore extremely important. In the USA, pylons have now been fitted with wireless fault indicators, which have sensors for power, temperature and air moisture, plus a small camera equipped with software that reports large, sudden movements. The primary reason is to protect the USA’s 240,000 kilometres of mains power lines from terrorist attack. It would undoubtedly also make sense to further increase redundancy and expand capacities. It is also possible for the supply networks, under the burden of the terrorist threat, to assume a different, less vulnerable form.

Securing the supply chains

Secure production and transport of goods and guaranteeing the integrity of goods are vital to society and business. Terror attacks could affect the system in many places. An interruption in goods deliveries can cause considerable economic damage very quickly and can lead to companies collapsing. Counterfeiting, contamination or misappropriation of the goods themselves can substantially disrupt social and business life. Every citizen can be affected if the supply of food or medicines is impaired. Securing the supply chains is of increasing significance for Germany as an export and logistics location. Transport containers (such as letters, parcels, boxes, containers, tanks) may be misused for attacks or criminal purposes. The range of individual scenarios is very

Together with partners, Siemens has developed a comprehensive solution based on RFID for the seamless monitoring of donor blood. Using identification by radio chips, mixing of blood reserves is practically eliminated.



wide. Packaging and containers allow prohibited activities to be camouflaged, attacks to be disguised and illegal objects to be moved internationally. Production facilities can be deliberately destroyed or manipulated. The flow of goods also contains items whose manipulation or theft could pose a great threat. This makes large container transport systems and logistics centres highly significant. Innovative solutions for their security are therefore extremely important to secure the supply chains. The objectives of the security research in this scenario are prevention, early identification of threats without disrupting or slowing commercial transport and increasing the performance of the relief units in a crisis as well as minimising damage.

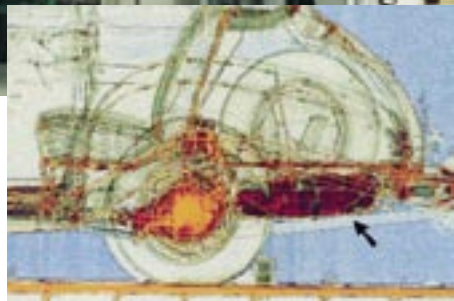
Relevant research topics:

- Sensor systems and detection

- + **Mobile scanning devices (e.g. container screening)**
- + **Mass sensor systems to detect contaminants and hazardous substances**
- + **Tracking of goods via sensor technology (including RFID and by satellite)**
- + **High-throughput detection**

Identification and tracking of goods in the logistics chain. Here, data are exchanged between the object and the RFID reader (Siemens AG). In order to avoid the possibility of interception and manipulation of the exchanged data, effective security measures are required.





- Simulation, pattern detection and data input
 - + Imaging procedure
 - + Integration of cost-effective monitoring systems into transport containers
- Information and communication technology
 - + Integrated security features in logistics ICT systems
 - + Energy-efficient cryptographic procedures for mobile systems
 - + Secure electronic key (token) to protect important data
- Strategies to increase the robustness of systems, procedures and processes
 - + Customer and user-oriented security features and systems combined with the qualification of the users
 - + Strategies for the secure co-ordination of business processes
 - + Interdependencies and systematic vulnerability analyses for key components and productions
 - + Failure planning and management

*Mobile radiographic x-ray equipment (above)
Below: The port of Hamburg customs are also equipped with container x-ray equipment. The x-ray image shows a classic car with narcotics in the tank, in a container on a lorry.*

- Prevention and response strategies and organisational forms
 - + Tapping solutions from the hazardous goods sector for general goods transports
 - + Security culture in the business environment
 - + Cost-benefit analysis including liability consequences and insurance burdens
 - + Preventive analyses of the spread of hazardous substances and warfare agents
 - + Modelling of damage situations to uncover structural and organisational deficits

Technology interconnections

Integrated protection systems for emergency and security services

Against a background of growing potential threats from terrorism, natural and technical disasters, as well as the increase in integrated assignments by various relief units, the range of deployment for civil defence and protection and the police has expanded significantly. First Responders in particular are faced with new communication and organisational challenges when combating and tackling incidents caused by



Practice with ABC protection suits

catastrophes or terrorism and are finding themselves exposed to increased psychological and physical burdens. Based on this changing threat situation development of integrated protection systems, equipment and organisational measures to improve the performance and security of first response forces in the long term will be required. In particular, there is a need for reliable, secure and compatible technologies and tools for communication and co-ordination and for equipment and resources to protect against chemical and biological agents and other hazardous substances. User-friendliness and human-machine interfaces in particular must be considered in the development of high-performance and robust security systems.

Helmet mounted IR-camera with head-up display and interface to a digital transmitter

Helmet integrated headset for digital transmission

Beacon with a digital interface

Digital transmitter, carried in a breastpocket, with large, glove-suited pushbuttons

Breath activity sensor with interfaces to a pressurized air container and a digital transmitter

Safety suit of the EADS fire brigade



The additional technology must not be at the expense of practicability.

The World Trade Center following the attack. The selfless contribution of the emergency and security services was a contributory factor in the surprisingly large number of survivors.



The fire service of the future

At around 8.45 a.m. on 11 September 2001, terrorists flew an aircraft and its passengers, with a full tank of fuel, into the North Tower of the New World Trade Center, followed a quarter of an hour later by a second aircraft, which was flown into the South Tower. Both 110-storey towers collapsed during the evacuation and rescue work. Around 3,000 people lost their lives, including 450 members of the emergency and security services.

Those involved in the rescue work were, quite rightly, hailed as heroes. It wasn't until later that specialists were able to examine in depth what went wrong: a great deal, according to a study by the RAND Corporation.

The ban on all commercial flights imposed immediately after the terrorist attacks meant that urgently needed materials and teams of specialists could not be flown in.

Communications were initially catastrophic. The mobile radio installation for the area of Manhattan affected had been located on the roof of the World Trade Center and had been lost along with the Tower; the fixed network was also demolished, because debris from the collapsed Towers had destroyed a hub. The remaining lines were blocked by huge volumes of telephone calls.

The spares for the equipment used by the rescue teams were not always interchangeable, which for example made supply of air filters for breathing equipment difficult. Most of the fire service equipment was not designed to cope with disasters, when equipment needs to be operated for hours at a time, so that after a while, members of the fire service took off their heavy helmets as frequently as they could. The breathing masks frequently restricted vision too badly, as visors prized as "anti-fogging" blinded their wearers in the sweaty inferno, and acoustic communication, shouted orders and warnings, was so bad that some men unscrewed the filters from their masks. Finally, even some heavy shoes failed to withstand the heat of the ground, and soles melted. Against the background of such difficulties, the achievements of those involved deserve even higher praise.

Security researchers from around the world have carefully noted the lessons learned from 9/11. The "fireman of the future", as a European technological group imagines him, should be spared most of the difficulties and risks that hap-

pened in Manhattan. Protective suits made of new materials would provide better protection from fire, heat and mechanical injuries and would also be more comfortable to wear. A helmet-mounted heat imaging camera with a head-up display would show the fireman and also the team leader a better, documentable picture of the risk location, for example, which would warn about glowing hot parts. The emergency services could place small transmitters and receivers around the site, which would automatically link up into a radio network. Someone working in situ would use this via a robust digital radio in his breast pocket, the large buttons of which would also make it usable whilst wearing gloves, providing a secure voice link to the other members of the team, the team leader and the control centre. An additional voice recognition function would allow hands-free use if necessary. Radio communication with colleagues would also be readily possible even when wearing a breathing mask. The compressed air supply would be precisely monitored and managed electronically. The transmission and reception units distributed could also serve as autonomous tracking devices and could also contain sensors to provide information about the current risk situation (e.g. temperatures), and in conjunction with a satellite navigation system, could enable virtual risk areas to be reconstructed for the people in situ.

The "fire service of the future" will keep security research teams busy for a long time. Where possible, they are also replacing the trusted wailing sirens of the fire engines, since although these are easy for car drivers to hear, they are difficult to locate, resulting in frequent accidents at road junctions. It would be better, insist acoustics specialists, to have an attention-grabbing sound sequence interrupted at regular intervals by noise pulses that the ear can readily locate. Tests using such sirens have demonstrated that their use significantly improves accident statistics. In tests, evacuation times for ships whose exits have been acoustically "marked" in this way are reduced by 70%. In the car parks at Munich Airport, such "sound alert" sound pulse generators are already providing greater safety. In the event of a fire, the generators can also be located through thick smoke and they can be understood by passengers, irrespective of their nationality.

Relevant research topics:

- + **Medical monitoring by sensors during deployment**
- + **Functional clothing for emergency services with integrated sensor and communications technology**
- + **Positioning and navigation systems**
- + **Digital communications systems for emergency and security services**
- + **Networked reporting, warning and information systems**
- + **Service robots for information, assistance and hazardous situations**
- + **Innovative NBC protection solutions**
- + **Effect of psychological factors and interaction of new technologies and mission conditions**

Multi-sensor systems for CBRNE risks

There is an increasing risk of abuse of chemical, biological, radiological, nuclear or explosive contaminants and hazardous substances (CBRNE substances) as these substances are becoming ever easier to obtain. Information on how to build weapons or parts of weapons can be found on the Internet, for example. The main technical pre-requisite for comprehensive preventive and reactive protection measures are highly-sensitive detector systems to detect all types of CBRNE substances. The threats range from the use of non-conventional explosives by terrorists to the risk of a large-scale contamination of agricultural output and spoiling of the food and water supply, to the use of “dirty bombs” that use conventional explosives to disperse radioactive material. Early detection, and the concomitant containment of such threats, requires the development of both new sensor concepts and new scanner technologies with integrated or mobile trace or volume detectors. The goal is to create early warning systems, e.g. during checks on people, baggage or goods, that can help to prevent CBRNE attacks or facilitate a rapid deployment of emergency

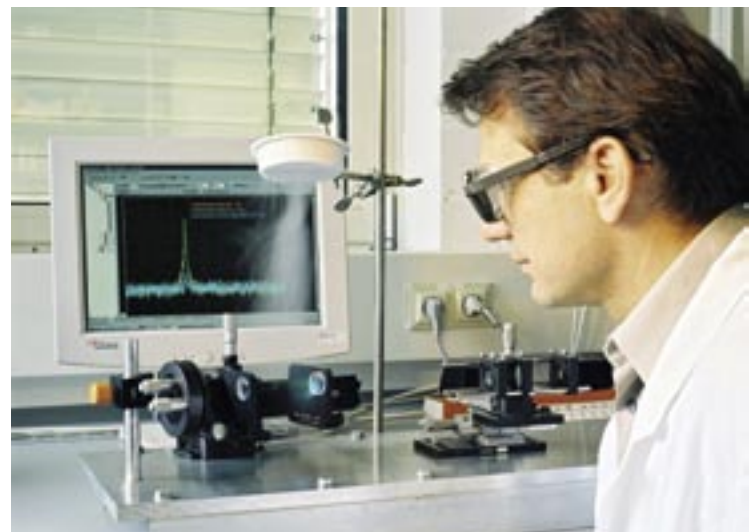
Image right: researchers from EADS in Munich have developed an innovative sensor based on an ion mobility spectrometer (here a laboratory assembly), which is 30 times more sensitive than the nose of a dog, for sniffing out narcotics and explosives. The artificial nose should make air travel safer and policing more effective.



RFID labels make the handling of goods quicker and above all safer. For goods with a high water content, which may interfere with the radio signals, flag tags are used: with flag tags, the transponder stands out from the packaging like a small pennant.

or evacuation measures in a crisis through early detection of warfare agents.

Against this background, the interdisciplinary topic of „multi-sensor systems for CBRNE risks” should preferably promote multi-modal and multi-functional detector platforms, new types of mobile sensor concepts as well as new types of sensor and data merge concepts and procedures to achieve a sustainable improvement in security at the point of deploy-



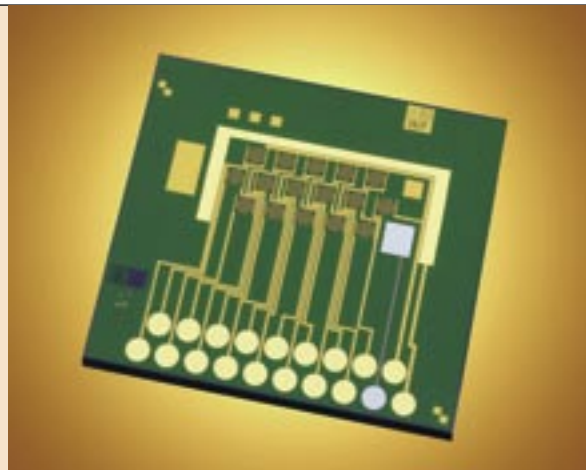
Nanotechnologies in the battle against bioterrorism

Most people associate “flu” with sneezing, coughing and a sore throat. Although this is generally true, there are some highly aggressive strains. The “Spanish flu” epidemic of 1918 killed 2.5 percent of all those infected between 1918 and 1919, including many young people. Some historians see the epidemic as a principal reason for the end of the First World War. Average life expectancy in the USA fell by ten years as a result. It is worrying that this particular deadly virus can be broadly-speaking reconstructed through genetic engineering, as proven a few years ago by an American military research group. Since then, vast resources have been spent on developing strategies to prevent the use of flu viruses as a biological weapon.

Risks of this kind can only be successfully combated provided they can be described quickly and accurately enough, as is possible using, amongst other things, new nanotechnological analysis equipment and sensors.

One particularly promising type of sensor uses nanowires made of a number of materials; these wires are only a few millionths of a millimetre in thickness. If a foreign substance binds to such thin wires, their electrical characteristics alter so drastically that in principle individual viruses, even individual molecules, can be detected. The coating of the nanowire determines what is measured: so if for example ammonia is to be detected, then the coating should preferably assimilate ammonia, if possible highly selectively. If certain viruses were to be detected, then the wires would have to be coated with antibodies, to which only these viruses adhere.

The nanosensor concept has become even more attractive thanks to a new class of substance. iMabs (industrial molecular affinity bodies) are biotechnologically tailored molecules that consist of a carrier to which an affinity point adheres, which can then be biotechnologically trimmed to bind with countless biological substances. These molecules are universal and highly stable, making them good candidates for nanowire sensors, which could detect pathogenic germs of all kinds. The food industry is also interested in such sensors,



With chips from the Fraunhofer Institut für Siliziumtechnologie, ISIT, rapid DNA sensors are being developed for the detection of pathogenic bacteria and other biogenic materials.

since once these can be cheaply mass-produced, they could bind to foodstuffs to provide information about its condition.

Fast, highly sensitive sensors would also be useful in preventing biological weapons attacks. However, new, fast, better and cheaper biosensor technology has already become a necessity, in the light of progressive globalisation. If the world is to become a global village as a result of fast mass travel opportunities, then the fast spread of epidemics will also become a possibility. Nanotechnological “labs-on-a-chip” could in the future assist the fast sensors in preventing this happening, since they would for example quickly enable the development of a new flu virus to be ascertained and its DNA sequence disseminated via the Internet more quickly than the virus itself can spread. At potentially affected locations, nanotechnological “fabs-on-a-chip” would synthesise vaccines at lightning speed, a remote, but not unrealistic goal. Many biotechnological procedures can now be accomplished in chip format; precisely temperature-controllable reaction vessels are needed for the polymerase chain reaction, or PCR, to proliferate the genetic material DNA, and these can now be produced at a scale of tenths of a millimetre using nanotechnologically manufactured thermoelectric cooling foils. This type of microsystems engineering is supported by ever more refined nanoelectronics, plus nanophotonic elements, which for example make the integration of spectroscopic analysis techniques possible on the tiniest scale.

Research in this field is being driven forward for commercial reasons, and the contribution made by security research helps to speed up success and to raise biochemical analysis to a new level, offering a real opportunity to avoid intentional and unintentional chemical, and especially biological threats.

An example is the EU project eBIOSENSE, which has brought together a number of companies to construct electrical bio sensor arrays for analyses of harmful micro organisms and microbial toxins; the German Fraunhofer Institute for Silicon Technology is contributing its expertise in bridging the gap between biology and electronics.

ment and to accelerate security checks. Essential criteria for the development and integration of multi-sensor components for both local and long-range detection of CBRNE substances include not only a high level of sensitivity, resolution and selectivity but, above all, ease of use, autonomy, a high level of automation, robustness as well as low susceptibility to false alarms and real-time capability. The key support points addressed include not only detection processes (e.g. based on terahertz technology) and sensor types (e.g. self-reporting sensors) but also multi-sensor system solutions based on a link between new and existing CBRNE sensors or application-related use of existing detector technologies (e.g. biochips or clinical diagnostic procedures).

Relevant research topics:

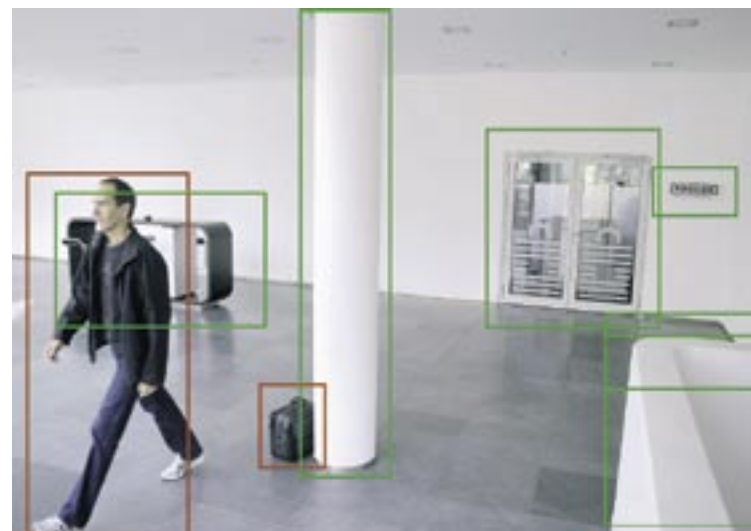
- + **Wireless or distributed sensor networks**
- + **Low-cost portable sensor systems with low power consumption and lab-on-a-chip systems**
- + **Sensor communication with mass-data and real-time capability, data transfer and data merge with decision-making function**
- + **Systems for rapid automatic long-range detection**
- + **Marker systems, identification and detection methods for new classes of explosive substance, toxins or pathogens**
- + **Hyperspectral sensors and multispectral imaging sensor systems.**

Pattern recognition

The ability to analyse information, images or data, which where possible originate from many different sources, by means of intelligent and automated pattern recognition and to make them available promptly to the responsible persons, facilities or authorities is an essential element of future security systems. In a case of a crisis, this ability will make it easier to plan and manage deployments and to gather information. Key applications include automatic protection of busy locations, identification of forged documents, automated support for border checks or monitoring of objects classified as being hazardous or in jeopardy.

There is still plenty of room for development in surveillance and early warning systems for automated analysis of multi-sensor data, such as image data, in conjunction with results of detection procedures geared, for example, towards hazardous substances. The foundations for implementing improved pattern recognition systems and new data analysis and visualisation methods will include extremely high-performance hardware and software developments based on database and Internet technology. There will also be information, visualisation and sensor technology developments from other fields of research. For instance, pattern recognition algorithms that were originally developed to detect tumours on computer tomography images can be modified to track movements of people or abandoned luggage at railway stations and airports via video surveillance. Results from the humanities and social sciences, such as the behaviour and organisational structures of terrorists, will also be incorporated into pattern recognition.

Thanks to sophisticated software, intelligent security cameras automatically recognise that an item of luggage has been left and abandoned.





3D facial recognition: 3D object recognition using colour strips offers many fields of application.

Biometry for personal identification

Generally speaking, people are very sensitive when it comes to faces; just a few differences result in failure to recognise a well-known face.

Computers are less sensitive in this regard, but they still have a real need to compare a real face against a passport photograph. It is not surprising as far as two-dimensional pictures are concerned, since the way people look in their passport photograph depends all too much on the way the light falls when the photograph is taken or on the inclination of their head. Or even on someone's form on a particular day – sometimes people don't even recognise themselves. Methods of recording a face or a head in three dimensions promise to be more secure. The European Union has therefore invested 12 million Euro in the "3D Face" project. People from the Bundesdruckerei [Federal printing plant], Cognitec Systems from Dresden and the French defence electronics manufacturer Sagem Défense Sécurité are working on the project alongside researchers from the Fraunhofer Institute. The project builds on experiences in production engineering, in which three-dimensional shapes must also be recorded as accurately as possible by means of an optical scan. When applied to the human face, this technology also covers details such as the curve of the cheeks, the creasing of the ears, the thrust of the chin. Bad lighting is no longer a problem when using 3D, and even ageing does not make a face unrecognisable to the machine, because of the many new reference points.

Over two years ago, the Hamburg Chaos Computer Club publicly disclosed how simply plastic casts could be made that are capable of outwitting fingerprint scanners, indicating that fingerprints as a security feature leave something to be desired. One possibility is recording the vein pattern on the back of the hand using an infrared camera. The benefits of this lie in the fact that the personalised pattern is located inside the body and emits heat. In order to copy it, one would have to produce a kind of infrared-active toupee for the back of the hand, which while not impossible, is certainly difficult. At schools in the Scottish town of Paisley, pupils pay for their school meals on a cashless basis by displaying the backs of their hands. One positive side-effect is the fact that less well-off students, who are not required to pay, previously had to



Bosch security systems have installed a facial recognition system, which works anonymously, for the casino in Bad Homburg. It reliably recognises persons whose facial images are saved due to a voluntary self-block. This enables surveillance personnel to discreetly refuse entry to gambling addicts.

identify themselves by means of a cord hung around their necks, before the back of the hand scanner was introduced, thereby distinguishing them from their richer counterparts and making them a target for bullying. Everyone is equal as far as the computer-based back-of-the-hand scanner is concerned, and the kids enjoy the "007" effect.

Her Majesty's secret agent James Bond was also involved in an adventure in which biometric features played a part, in "Never Say Die", the availability of atomic weapons was decided by means of a scan of the iris. Things went badly (although they turned out fine in the end) because they should have scanned the retina as well. And the back of the hand, and the shape of the face, and so on and so forth. Methods used for unequivocal identification of those with authorised access are now 98 percent accurate. However, they need to be practical as well. Lufthansa for example tested vein pattern recording on the back of the hand at Johannesburg airport. A check-in system generated a barcode from the vein lines, which was affixed to the boarding card and was intended to check the identity of the passengers when boarding. But the procedure was just too much for the passengers.

However, the future lies in biometric methods. The casino in Bad Homburg for example has stored biometric data on gambling addicts, at their own request. When they enter the casino, the hapless individuals are filmed like everyone else and their faces compared against a biometric database. If they are recognised, the computer sends a photograph by radio to the palmtop of the security guard, without giving the name, and the person concerned is escorted from the premises in his own interests. Shoplifters can be scared off in the same way.



Test image, compiled by L. Fei-Fei, R. Fergus and P. Perona. (California Institute of Technology), on the machine that is to learn classification: what is an insect, what is an aeroplane, what is a person, what is a motorcycle?

Relevant research topics:

- + Automatic image, data and text analysis processes and web search technologies
- + Artificial neural or self-learning networks
- + Automated information and data fusion with mass-data and real-time capability, VR technologies
- + Data exchange technologies
- + Machine translation and voice recognition technologies
- + Tracing and screening of radar and radio signals.



Left: micro-aerial vehicle md4-200...

Right... and its builder, friends and pilot, photographed from the MAV. In order to prevent equipment of this type from entering the private sector, the accompanying security research will establish regulations for its use.

Reconnaissance robots

The computer used for the Apollo spaceship, which took three astronauts to the moon in 1969, had a rewritable memory (4 kilobytes of RAM) and ran at 1 megahertz. Today's average laptop has a memory 250,000 times larger and runs 1,000 times more quickly. This comparison gives us an idea of what modern electronics and sensor technology make possible today: For example, a "UFO" the size of a cartwheel that remains in the air of its own accord if you put down the remote control unit – even if it is battered by gusts of wind.

This UFO, manufactured by microdrones GmbH, near Siegen, is called md4-200. It weighs just 680 grams and has a load capacity of up to 200 grams for carrying items such as electronic cameras. "md" stands for microdrone, "4" is the number of rotors, and "200" is the load capacity.

Unlike the model helicopters that have been around for a while already, the developer, Udo Jürss, assures us that even complete beginners will be able to control the md4-200 after only a short amount of time. This is made possible by the fact that the four rotors are driven by sophisticated electric motors which power an advanced computer system which, in its turn, is supported by numerous sensors. These include a GPS receiver, atmospheric pressure, temperature, and magnetic field sensors, tri-axial accelerometer, and other features. The energy required to power and control the device is provided by a lithium polymer battery which can keep it in the air for around 20 minutes.

The md4-200 is normally used to carry a digital camera for taking videos or photos. The camera is controlled by remote control and the signals are returned to the operator in the same way. This system allows the person controlling the device to put on a pair of video glasses and control the drone as if he or she were sitting directly behind the camera.. In this way, the operator can investigate sites which are simply out of sight to the naked eye. For example, the drone can travel to heights of up to 1,500 meters. This means that you could fly up to the sphere on top of the television tower at Alexanderplatz,

Berlin, and take a look through a window to see what they're serving in the tower restaurant.

The md4-200 is only one of many drones currently on the market. However, this particular drone is characterized by a series of unusual features such as its low weight, which allows it to be operated without registration. The 200 gram load capacity is sufficient for cameras capable of producing professional-quality photos.

This means that this type of drone could be extremely useful to public services such as the police force, fire brigade, and disaster relief organizations as well as to companies responsible for security at airports, power stations, and company sites. Since a satellite navigation system such as GPS (soon GALILEO) reports the position of the drone to the operator, you can program a computer to send the drone on fully automatic patrols. An image evaluation system allows it to report suspicious movements. The device's ability to hover at a particular location in the air makes it ideal for watching the action at large events such as football matches. Motorway police could send out the md4-200 when accidents and related traffic jams occur in order to assess the need for a rescue helicopter or other heavy equipment. The fire brigade could use it to obtain a precise overview of the situation when fires occur in high-rise buildings – without risking the lives of fire fighting personnel. Bridges could be easily inspected to look for cracks and large buildings could be examined for structural damage.

Obviously, the paparazzi will also be interested in using the drones to take pictures. A more important drawback is the possibility of terrorists using these freely available drones as a potential instrument of terror. The possibilities for both good and evil are endless. For this reason, the Government will have to consider whether or not to restrict the use of this technology. Security research can help the Government to reach the right decision by means of providing intelligent technical solutions and accompanying research.

Biometrics

Authentication or identification of persons using biometric features can be used for example to protect against terrorism, at border security or in law enforcement by the police. However, the technology is also becoming increasingly significant in e-commerce and access control. Among other things, biometric systems must be developed in such a way that their use at border checks, for example, facilitates high-performance, reliable, rapid and convenient authentication. In addition to ease of use, accuracy of identification and robustness of biometric systems, it is also important to minimise rejection and false acceptance rates. Protection of the stored reference data and data transmission in the biometric system are essential for the further development and integration of biometric components into security systems.

Relevant research topics:

- + **Integrated biometric sensor systems**
- + **Multi-modal biometrics**
- + **3D facial recognition**
- + **Decentralised trust models and technologies.**

In cooperation with Siemens, Lufthansa has successfully tested a biometric check-in and boarding procedure at Frankfurt airport. The system used identifies passengers via fingerprint by transforming the characteristic patterns into a two dimensional point code that is printed on the boarding card.



Together with partners, Bosch constructed the pilot project for the automated, biometrics-based border control at Frankfurt airport.

Implementation of the support programme

Support instruments

The focus of the support is not on individual technological results but on forming a community of players and implementing agreed innovation strategies and objectives. The co-operation of end users with their practical experience is vital to security research.

Priority for funding will go to joint projects which will essentially be measured against the following criteria:

- + **How they help increase security**
- + **Level of innovation and increase of knowledge**
- + **Uniformity and breadth of impact of the solution including social goals and effects**
- + **Practical suitability or marketability of the intended solution and its optimised economic leverage.**

The joint projects should be led by end users or industry and include all the necessary research disciplines.

The joint projects in programme line 1 aim to develop system solutions for security scenarios; those in programme line 2 aim to develop cross-scenario technology systems. Joint projects are of particular benefit to SMEs. On the one hand they bring SMEs into direct contact with excellent research facilities, and on the other hand they gain access, via the major enterprises co-operating in the project, to key users and markets and hence the opportunity to become a sub-contractor.

The funding will be granted on a competitive basis i.e. there will generally be a public announcement of the topics in question and other special criteria. Given the breadth of the security research field, the announcements may be made in conjunction with other research programmes and over multiple policy areas.

In order to accommodate the breadth of security research, the plan is to set up innovation platforms building on thematically-related joint projects. The goal of these innovation platforms is to bring all the players involved to one table, thereby allowing synergies between related research projects

to be utilised. This also means that the information transfer that is important for later decisions, such as in procurement, begins at an early stage of the research and development. The innovation platforms create the conditions for rapid implementation of the results. Efficiency will be increased even further if the players undertake to increase the proportion of their own research activities and evolve greater and more binding applications than has been usual hitherto in normal funding plans in Location Germany.

The security research programme will be accompanied and directed by a programme committee comprising research experts, the federal government departments, industry and operators of infrastructures of relevance to security. This programme committee will ensure that the security research measures interlock closely with the Federal Government's security policy activities and that the results can be implemented as seamlessly as possible. The programme committee is also responsible for evaluating goal-orientation on an ongoing basis, suggesting new research topics and more innovation steps (e.g. standardisation, regulations, procurement) and tracking the transfer of results into practice.

Programme duration and funding

Long-term funding is required to track promising security solutions and technology developments and to ensure a lasting build-up of skills and trust among the players. The support programme provides the framework for such a long-term, flexible funding policy. It is designed as a learning programme. One of the goals of the tools described above, the innovation platforms and the programme committee, is continuous optimisation and updating of the support.

For the time being, the Federal Government's security research programme will be planned on the basis of an initial support period running to the year 2010 and will be evaluated at the end of the initial programme period. Continuation of the programme beyond 2010 will require new medium-term operational goals to be defined.

The Federal Government will provide a budget of around EUR 123 m for this in the years 2007 to 2010 inclusive, subject to the approval of Parliament. This budget will be in addition to the security research funding already included in the federal departments and in corresponding specialist programmes.



After terrible disputes and aberrations, harsh conflicts within Europe are a thing of the past. However, in place of large external threats, there are now small-scale, but potentially very effective threats, which the community must combat with intelligence in order to preserve the freedom of Europe's things of beauty both past and present – like St Mark's Square in Venice, seen from the campanile.

Appendix

Ongoing activities of the Federal Government in relation to security research

Federal Foreign Office

- Web site www.auswaertiges-amt.de covering topics such as disarmament, arms control, peace policy, security policy, non-proliferation of weapons of mass destruction, civil crisis prevention, conflict resolution and peace consolidation, humanitarian international law, co-operation in the EU, NATO, OSCE and UN.
- Sicherheit und Stabilität durch Krisenprävention gemeinsam stärken – Federal Government report on the implementation of the Zivile Krisenprävention, Konfliktlösung und Friedenskonsolidierung action plan, May 2006
- Europäische Sicherheits- und Verteidigungspolitik, May 2004
- Jahresabrüstungsbericht, 2005
- EU-Strategie zur Verhinderung der Verbreitung von Massenvernichtungswaffen, December 2003
- EU-Strategie zur Bekämpfung der Anhäufung von Kleinwaffen und dazugehöriger Munition sowie des unerlaubten Handels damit, December 2005

Federal Chancellor

- Web site www.bundestkanzlerin.de
- G8-Erklärung zur Terrorismusbekämpfung of 16 July 2006

Authorities and research institutions under the umbrella of the Federal Chancellor

Stiftung Wissenschaft und Politik (SWP)

- Web site: www.swp-berlin.org
- Research groups on EU integration, EU external relations, security policy, America, Russia/CIS, Middle East and Africa, global issues
- Numerous studies, periodicals and series of books on security issues

Federal Intelligence Service

- Web site: www.bundesnachrichtendienst.de
- Responsibilities including early detection of risks through intelligence on international terrorism, and organised crime
- Interface to foreign intelligence services

Federal Ministry of Finance

- Web site: www.bundesfinanzministerium.de, covering topics including customs and money laundering

Federal Ministry of Justice

- Web site: www.bmj.bund.de covering crime prevention
- Zweiter Periodischer Sicherheitsbericht der Bundesregierung, BMI and BMJ, November 2006

Federal Ministry of Defence

- Web site www.bmvg.de covering topics such as defence, prevention and combat of crises and conflict and the battle against international terrorism
- Weißbuch 2006 zur Sicherheitspolitik Deutschlands und zur Zukunft der Bundeswehr, October 2006 – published jointly with the Federal Foreign Office

Research institutes under the umbrella of the Ministry of Defence

Institut für Radiobiologie der Bundeswehr

- E-mail: Institutfuerradiologie@bundeswehr.org

Institut für Mikrobiologie der Bundeswehr

- E-mail: Institutfuermikrobiologie@bundeswehr.org

Institut für Pharmakologie und Toxikologie der Bundeswehr

- E-mail: Institutfuerpharmakologieundtoxikologie@bundeswehr.org

Flugmedizinisches Institut der Luftwaffe

- E-mail: FlMedInstLtr@bundeswehr.org

Schiffahrtsmedizinisches Institut der Marine; Forschungsanstalt der Bundeswehr für Wasserschall und Geophysik (FWG)

- Web site: www.bwb.org

Sozialwissenschaftliches Institut der Bundeswehr (SWInstBw)

- Web site: www.sowi-bundeswehr.de

Wehrwissenschaftliches Institut für Schutztechnologien**- ABC-Schutz (WIS)**

- Web site: www.bwb.org/wis

Wehrwissenschaftliches Institut für Werk-, Explosiv- und Betriebsstoffe (WIWEB)

- Web site: www.bwb.org/WIWEB

Amt für Geoinformationswesen der Bundeswehr (AGEoBW)

- E-mail: ageobweingang@bundewehr.org

Forschungsgesellschaft für Angewandte Naturwissenschaften e.V. (FGAN)

- Web site: www.fgan.de
- Application-oriented research in high-frequency physics and radar technology, optronics and pattern detection as well as ICT and robotics

Fraunhofer Institutes under the umbrella of the Ministry of Defence

- Web site: Fraunhofer Alliance for Defence and Security Research www.vvs.fraunhofer.de
- FhI for Technological Trend Analysis (INT)
- FhI for High-Speed Dynamics, Ernst-Mach-Institut (EMI)
- FhI for Chemical Technology (ICT)
- FhI for Applied Solid State Physics (IAF)

Federal Ministry of the Interior

- Web site www.bmi.bund.de covering topics such as civil protection and disaster assistance, data protection, crime and terrorism, IT security
- Zweiter Periodischer Sicherheitsbericht der Bundesregierung, BMI and BMJ, November 2006
- Nationaler Plan zum Schutz der Informationsinfrastrukturen, July 2005
- Schutz Kritischer Infrastrukturen – Basisschutzkonzept, Empfehlungen für Unternehmen, August 2006

Authorities under the Federal Ministry of the Interior

Federal Office for Information Security (BSI)

- Web site www.bsi.bund.de covering topics such as application security, critical infrastructures and the Internet, cryptography and protection from eavesdropping, certification, approval and conformity tests, new technologies

and publication of technical guidelines

- Projects with research facilities in the innovation fields of early warning/Trojans, trusted computing and biometrics, passports, ID cards
- Lage der IT-Sicherheit in Deutschland, July 2005
- IT-Grundschrutskataloge und Leitfaden IT-Sicherheit - IT-Grundschrut kompakt, March 2006
- Risiken und Chancen des Einsatzes von RFID-Systemen, 2005
- Sicherheit von Webanwendungen - Maßnahmenkatalog und Best Practices, Version 1, August 2006
- VoIPSEC - Studie zur Sicherheit von Voice over Internet Protocol, 2005
- Studie Pervasive Computing – Entwicklungen und Auswirkungen (PerCENTA), October 2006
- Studie Integration und IT-Revision von Netzübergängen, October 2006
- Tomcat-Sicherheitsuntersuchung, 2006
- Mobile Endgeräte und mobile Applikationen – Sicherheitsgefährdungen und Schutzmaßnahmen, 2006
- Sample guidelines and location check for critical infrastructures

Federal Office of Civil Protection and Disaster Assistance (BBK)

- Web site www.bbk.bund.de covering areas such as protection of critical infrastructures, NBC protection, crisis management, civil protection research & development projects
- Rahmenkonzept zur Dekontamination (verletzter) Personen, National – Regional government working party, September 2006
- Biologische Gefahren - Beiträge zum Bevölkerungsschutz, 2005

The Governmental disaster relief organisation of the Federal Republic of Germany (THW)

- Web site: www.thw.bund.de
- Responsibilities in the area of disaster relief organisation, provision of disaster relief at home and humanitarian aid abroad

Federal Criminal Police Office (BKA)

- Web site: www.bka.de. Responsibilities in the area of coordination of crime fighting at national and international level, national point of contact for Interpol, Europol and the Schengen information system.
- Research into criminal investigation and criminology in the Institute of Law Enforcement Studies and Training with research centres for terrorism/extremism, police crime statistics, violent crime and ICT crime, organised and white-collar crime, legal policy and crime prevention
- Participation in research projects such as facial recognition and detection methods

Federal Police (BPOL)

- Web site: www.bundespolizei.de
- Responsibilities include border security, railway police, air safety and protection of federal bodies and application abroad

Federal Ministry for Education and Research

- Web site www.bmbf.de covering topics such as institutional research support and applied project research support

Research organisations under the Federal Ministry for Education and Research

Helmholtz-Gemeinschaft Deutscher Forschungszentren (HGF)

- Web site www.helmholtz.de. Work that fundamentally relates to security research is carried out in the following HGF centres under the Federal Ministry for Education and Research:
- Alfred Wegner Institute for Polar and Marine Research, Bremerhaven
- GKSS-Forschungszentrum, Geesthacht
- Helmholtz Centre for Infection Research, Braunschweig
- Research Centre Jülich
- Forschungszentrum Karlsruhe
- GeoForschungsZentrum Potsdam
- GSF National Research Centre for Environment and Health, Neuherberg
- Helmholtz Centre for Environmental Research - UFZ, Leipzig-Halle

Max-Planck-Gesellschaft (MPG)

- Web site www.mpg.de. Work that fundamentally relates to security research is carried out in the following Max Planck Institutes:
- MPI for Ethnological Research
- MPI for Informatics
- MPI for Biological Cybernetics
- MPI for Microstructure Physics
- MPI for Software Systems
- MPI for Foreign and International Criminal Law

Wissenschaftsgemeinschaft Gottfried Wilhelm Leibniz (WGL)

- Web site: www.wgl.de. Work that fundamentally relates to security research is carried out in the following WGL institutes:
- German Research Centre for Food Chemistry, Garching - DFA
- German Institute for Economic Research, Berlin - DIW
- Ferdinand-Braun-Institut für Höchstfrequenztechnik, Berlin - FBH
- Research Center Borstel, Leibniz for Medicine and Biosciences - FZB
- Forschungszentrum Rossendorf, Dresden – FZR (Institut für Sicherheitsforschung am FZR)
- Heinrich Pette Institute for Experimental Virology and Immunology - HPI
- IHP GmbH Innovations for High Performance Microelectronics, Frankfurt (Oder) - IHP
- Institute for Applied Geosciences, Hannover - GGA
- Leibniz Institute for Age Research - Fritz-Lipmann-Institut, Jena - FLI
- Leibniz Institute for Natural Product Research and Infection Biology - Hans-Knöll-Institut, Jena - HKI
- Max-Born-Institut für Non-linear Optics and Short Pulse Spectroscopy, Berlin - MBI
- Paul Drude Institute for Solid State Electronics, Berlin - PDI
- Social Science Research Centre, Berlin – WZB
- Leibniz Institute of Plant Genetics and Crop Plant Research, Gatersleben - IPK

Fraunhofer-Gesellschaft (FhG)

- Strategische Studie zur Aufstellung der FhG Fraunhofer-Gesellschaft in der Sicherheitsforschung, March 2005
- Web site www.fraunhofer.de Work that fundamentally

relates to security research is carried out in the following Fraunhofer-Gesellschaft Institutes under the Federal Ministry for Education and Research:

- FhI for Open Communication Systems (FOKUS)
- FhI for Applied Polymer Research (IAP)
- FhI for Digital Media Technology (IDMT)
- FhI for Experimental Software Engineering (IESE)
- FhI for Factory Operation and Automation (IFF)
- FhI for Interfacial Engineering and Biotechnology (IGB)
- FhI for Computer Graphics Research (IGD)
- FhI for Integrated Circuits (IIS)
- FhI for Information and Data Processing (IITB)
- FhI for Ceramic Technologies and Systems (IKTS)
- FhI for Laser Technology (ILT)
- FhI for Molecular Biology and Applied Ecology (IME)
- FhI for Microelectronic Circuits and Systems (IMS)
- FhI for Manufacturing Engineering and Automation (IPA)
- FhI for Production Systems and Design Technology (IPK)
- FhI for Physical Measurement Techniques (IPM)
- FhI for Silicon Technology (ISIT)
- FhI for Software and Systems Engineering (ISST)
- FhI for Toxicology and Experimental Medicine (ITEM)
- FhI for Industrial Mathematics (ITWM)
- FhI for Cell Therapy and Immunology (IZI)
- FhI for Non-Destructive Testing (IZFP)
- FhI for Reliability and Microintegration (IZM)
- FhI for Secure Information Technology (SIT)

Specialist programmes in the Federal Ministry of Education and Research relating to security research:

Framework programme “Materials innovations for industry and business, WING”

- www.bmbf.de/pub/rahmenprogramm_wing.pdf

“Research for the production of tomorrow” programme

- www.bmbf.de/pub/produktionsforschung.pdf
- Support measure “Innovations against product piracy”

“Optical technologies” programme

- www.bmbf.de/pub/foerderprogramm_optische_technologien.pdf
- Support for terahertz systems etc.

Framework programme “Microsystems 2004-2009”

- www.bmbf.de/pub/mikrosysteme.pdf
- Support for sensor systems and RFID etc.

“IT Research 2006” programme

- www.bmbf.de/pub/it-forschung_2006.pdf
- Support for security and reliability of ICT systems
- The IT Research 2006 programme will be superseded in 2007 by the ICT 2020 programme

“Health research” programme

- www.bmbf.de/pub/gesundheitsforschung.pdf
- Support for key areas including infection research

Support measure “Landmine detection technologies for humanitarian landmine clearance”

- www.bmbf.de/pub/hintergrundpapier_bekanntmachung_030327.pdf

Research project support by the German peace research institute

- www.bundesstiftung-friedensforschung.de

Framework programme “Research for sustainability”

- www.bmbf.de/pub/forschung_nachhaltigkeit.pdf
- Support for areas such as climate protection strategies, flood management, risk prevention strategies

Framework programme “Habitat Earth”

- Publication planned in 2007
- Support for system earth research covering areas such as early warning systems, earth and climate observation, risks of global change The ongoing commitment to the tsunami early warning system can be seen in this context

“Innovative core regional growth” programme

- Projects on “Maritime Safety Assistance” to develop security solutions along the maritime transport chain

Federal Ministry of Food, Agriculture and Consumer Protection

- Web site www.bmelv.de covering topics such as animal and plant health, consumer protection, emergency food supply (www.ernaehrungsvorsorge.de) and prevention of

biological terrorist attacks

- Vulnerabilität von Logistikstrukturen im Lebensmitteleinzelhandel, BMELV Applied Science Volume 512, October 2005

Authorities and research institutes under the Federal Ministry of Food, Agriculture and Consumer Protection

FLI (Friedrich-Loeffler-Institut)

- Web site: www.fli.bund.de
- Research into infectious diseases in agricultural animals

Federal Institute for Risk Assessment (BfR)

- Web site: www.bfr.bund.de
- Research into food safety, consumer health protection, risk assessment as part of biological security, exposure estimates and concepts to identify and prevent deliberate food contamination

Federal Office of Consumer Protection and Food Safety (BVL)

- Web site: www.bvl.bund.de

Federal Biological Research Centre for Agriculture and Forestry (BBA)

- Web site: www.bba.de
- Responsibilities include plant protection, plant health and biological security

Federal Ministry of Health

- Web site: www.bmg.bund.de covering topics such as health care and disease control, risk and security research in areas such as resistance to antibiotics and infectious diseases

Research institutes under the Federal Ministry of Health

Robert Koch-Institut (RKI)

- Web site: www.rki.de
- Research into the detection, prevention and control of diseases, collecting and preparing health data and assessing risks of genetic engineering

Paul-Ehrlich-Institut (PEI)

- Web site: www.pei.de
- Research into vaccine provision and the safety of biomedical drugs

Federal Ministry for the Environment, Nature Conservation and Nuclear Safety

- Web site www.bmu.de covering areas such as nuclear plant safety, chemical safety, radiation protection and emergency radiological protection
- Vollzugshilfe zur Störfall-Verordnung, 2003
- Guidelines Maßnahmen gegen Eingriffe Unbefugter, Incident committee, 2002
- Reaktorsicherheit und Strahlenschutz, series of journals
- Berichte der Strahlenschutzkommission, series of journals
- Radiologische Grundlagen für Entscheidungen über Maßnahmen zum Schutz der Bevölkerung bei unfallbedingten Freisetzungen von Radionukliden, 1999
- Rahmenempfehlungen für den Katastrophenschutz in der Umgebung kerntechnischer Anlagen, 1999

Authorities and research institutes under the Federal Ministry for the Environment, Nature Conservation and Nuclear Safety

Federal Office for Radiation Protection

- Web site: www.bfs.de
- Research including radiation protection for health, physical and technical radiation protection and the Nuclear Test Ban Treaty

Federal Environment Agency

- Web site www.umweltbundesamt.de
- Responsibilities including nuclear plant safety, security management, risk communication

Federal Ministry of Transport, Building and Urban Affairs

- Web site: www.bmvbs.de covering topics such as road safety and structural protection
- Air traffic initiative for Germany
- Galileo European satellite navigation system

Federal Ministry for Economic Co-operation and Development (BMZ)

- Web site www.bmz.de covering areas such as building peace, reducing poverty and human rights
- Krisenprävention, Konfliktbearbeitung Friedensförderung in der deutschen Entwicklungszusammenarbeit, BMZ concepts 131, 2005
- Recht - Demokratie - Frieden - Politik für Entwicklung, BMZ brochure, 2003

- Katastrophenvorsorge - Beiträge der deutschen Entwicklungszusammenarbeit, BMZ materials 135, Dezember 2004
- Der Millennium+5-Gipfel: Weichenstellungen für unsere globale Zukunft - Ein Diskussionspapier des BMZ, BMZ discourse, June 2005

Research institutes under the BMZ

German Development Institute (DIE)

- Web site www.die-gdi.de
- Department III "Governance, Statehood, Security"

Federal Ministry of Economics and Technology

- Web site: www.bmwi.de covering areas such as IT security, geo-information technology, export controls, classified information in the economy
- Online platform Sicherheit in der Wirtschaft, bmwi-sicherheitsforum.de
- Geheimschutzhandbuch - Handbuch für den Geheimschutz in der Wirtschaft, November 2004
- iD2010 - Innovationsstrategie für die Informationsgesellschaft Deutschland 2010, November 2006
- Security in medium-sized businesses – e-Business
- European initiative on Global Monitoring for Environment and Security, GMES
- The Federal Ministry of Economics and technology supports security-related space projects (earth survey missions TerraSAR-X and Tandem-X, optical communications systems, environment satellite Envisat) as part of the national space programme and the German contribution to the European Space Agency ESA.

Authorities and research institutes under the Federal Ministry of Economics and Technology

Federal Institute for Materials Research and Testing (BAM)

- Web site: www.bam.de
- Research into technical safety including hazardous substances, dangerous goods and explosives law, non-destructive testing and analytical chemistry
- Specialist portal: public/technical safety – hazardous substances/dangerous goods TES

Federal Network Agency

- Web site: www.bundesnetzagentur.de
- Responsibilities including telecommunications secrecy, basic provision of telecommunications and postal services, electricity and gas, ensuring efficient and uninterrupted use of frequencies, protecting the interests of public safety including in the railways network

Helmholtz Centre under the Federal Ministry of Economics and Technology

- Web sites www.helmholtz.de and www.dlr.de
- German Aerospace Centre

Federal Institute for Geosciences and Natural Resources

- Web site: www.bgr.bund.de
- Research including geological hazards, final storage measures for radioactive waste and the Nuclear Test Ban Treaty
- Seismological Data Centre

Glossary

3D Face: EU research project for the development of three-dimensional face recognition technology for automated border control systems (project runs to 31/03/2009).

ABC protection: Protection against atomic, biological, and chemical dangers such as ABC weapons.

Anthrax: Infectious disease that normally affects cloven hoofed animals but which can also be used as a biological warfare agent.

Biochip: Carrier device that allows a large amount of biological or biochemical information or checks to be stored in a small amount of space (also called a microarray).

Biometrics: Deals with tests made on animals and the related measurement and analysis procedures. In the field of human recognition: Automatic recognition of individuals based on their behavioural and biological characteristics.

Bioterror, bioterrorism: Variant of terrorism where biological weapons are used for attacks.

CBRNE agents: Chemical, biological, radiological, nuclear, and explosive substances that are dangerous and/or can be used as warfare agents.

Lab-on-a-chip, fab-on-a-chip: Also called microlab. Microfluidic system that enables all the functions of a large laboratory for analyzing or synthesizing chemical or biochemical substances to be housed on a synthetic substrate the size of a credit card.

FTIR (Fourier Transform Infrared Spectroscopy): Specific variant of infrared spectroscopy that uses Fourier transforms. **Galileo:** European satellite system designed for civil use which will be ready at the end of 2010.

Ion mobility spectrometer: Device used for chemical analysis. It is capable of detecting very low concentrations of chemicals, has short reaction times, and can detect different classes of chemical substances at ambient pressure.

Low power sensor technology: Energy-efficient/self-sustaining sensor technology or sensor networks with sensor nodes which use a very low amount of electricity or which obtain the electricity to power the sensor components by harvesting it directly from their environment.

Polymerase Chain Reaction (PCR): Method for replicating DNA without using a living organism. Among other things, it is used to detect hereditary diseases and viruses and to create and check genetic fingerprints.

RADIOTECT programme: EU research project for the development of ultra broadband technologies for the high-resolution detection of missing persons or unidentified objects.

RFID tags, radio frequency tags: Radio Frequency Identification. Small transponders that can be attached to objects. Their data content can be read without physical or visual contact.

(Risk) homeostasis: Self regulation. The ability of a system to keep itself stable within certain limits as a result of reaction to changes.

Dirty bomb: Radiological weapon. Conventional explosive device which scatters radioactive material when detonated. **Self-reporting sensors:** Autonomous, wireless, mostly passive sensors which actuate themselves if an incident occurs and return the detected signals to a central host or processing unit automatically.

TATP (Triacetone Triperoxide): A highly explosive fluid with the impact sensibility of priming explosive.

Terahertz radar (TADAR): Electromagnetic radiation at a frequency range between microwave and infrared radiation. Used to create images of objects through barriers such as paper or textiles.

Token: Hardware component (normally for connecting to the USB port of a computer) which generally contains a chip card from which data can be copied or manipulated.

VR technology: Virtual Reality technology: Human-machine interface which allows a user to interact with a computer-simulated audiovisual environment.

WLAN: Wireless Local Area Network.

WUSB (Wireless USB): Wireless variant of the Universal Serial Bus (USB).

Z Backscatter: Backscatter x-ray. Procedure for detecting and depicting concealed objects. Works by analyzing the material-specific backscattering properties in relation to the actively applied x-rays.

This publication is distributed free of charge by the German Federal Ministry of Education and Research as part of its public relations work. It is not intended for commercial sale. It may not be used by political parties, candidates or electoral assistants during an election campaign. This applies to parliamentary, state assembly and local government elections as well as to elections to the European Parliament.

In particular the distribution of this publication at election events and at the information stands of political parties, as well as the insertion, printing or affixing of party political information, are regarded as improper use. The distribution of this publication to third parties as a form of campaign publicity is also prohibited. Regardless of how recipients came into possession of this publication and how many copies of it they may have, it may not be used in a manner that may be considered as showing the partisanship of the Federal Government in favour of individual political groups, even if not within the context of an upcoming election.



Federal Ministry
of Education
and Research