Federal Ministry
of Education
and Research

THE NEW
HIGH-TECH
STRATEGY
Innovations for Germany

Self-determined and secure in the digital world 2015-2020

The German Government's research framework programme on IT security

Federal Ministry
of Education
and Research

Self-determined and secure in the digital world 2015-2020

The German Government's research framework programme on IT security

Foreword

Information and communication technologies (ICT) are an integral part of our lives. Smart phones are with us day-in, day-out, while networked applications shape the way we work. Yet almost every day the media report security shortcomings, data thefts, and cyber attacks on bank accounts, industrial facilities and online services.

To fully exploit the opportunities digitalisation offers, it is essential that we take positive steps to improve IT security. Instead of constantly accelerating the race between attackers and security experts, we require new, holistic solutions. Technological developments must be identified at an early stage, and IT security solutions for tomorrow need to be researched and implemented today.

The Federal Government is rising to this challenge with its research framework programme "Self-determined and secure in the digital world 2015–2020". In this framework programme we bring together cross-cutting IT security research, concentrating on high-priority aspects.

This brochure presents the programme, its objectives and its four research focuses. These include research into new, high-tech tools and processes, together with the security of complex ICT systems with their wide-ranging dependencies and interactions. A further focus is the security of large application areas such as production, transport, medicine, and critical infrastructures, for example energy and water supply. In the context of privacy, the programme addresses the issues of how to restore public trust in the information technology employed, and the way individuals can be empowered to determine how their personal data is handled.

IT security research will provide innovative solutions to help us to use information technology safely in the future. We are consistently promoting collaboration between science and industry in order to ensure that the approaches developed are actually put into practice. We urgently need applications for improved IT security as progressive digitalisation in both the business world and public life is making vital infrastructures more vulnerable than ever before.

Johanna Wanka

Prof. Dr. Johanna Wanka
Federal Minister of Education and Research

Content

1 Self-determined and secure in the digital world

Information and communication technologies (ICT) now pervade every area of our society. Without ICT there would be no modern hospitals, no reliable supply of water and electricity, no up-to-date banking system, no competitive automotive or machinery sectors, and above all no Industry 4.0. The everyday use of smart phones, tablets, and smart TVs is taken for granted by most people.

It's now more important than ever that we can—at all times—rely on secure and stable ICT able to withstand cyber attacks. Increasing digitalisation and networking make today's vital infrastructures—in business and in public life—more open to attack than ever. The German telephone company, Deutsche Telekom, alone records up to one million attacks on its network every single day. Companies and states are exposed to growing dangers from cyber attacks. If for example the power supply were to go down over a wide area as the result of a hacker attack, there would be massive implications for traffic control systems, hospitals, logistics chains, and water supplies.

The Federal Office for Information Security (BSI) sees five targeted espionage attacks on the federal administration each day. Every month attempts to maliciously manipulate the government's website network result in some 30,000 attempted attacks being blocked. In 2013 the global number of attacks on companies' IT security reached 42.8 million, a rise of 48 % against the previous year. That's 117,330 attacks per day. The economic damage alone for 2013 is estimated to be as much as 575 billion dollars.

There is also the impact felt by citizens in their private lives, who time and again will find themselves in a quandary over their personal data. On the one hand, citizens want—and need—to disclose information to use products and services from the cyber world. On the other hand, however, this produces increasingly extensive profiles that can be cross-linked, sold on, and analysed. Facebook alone has over 1.3 billion users. Every 20 minutes, they share some million links and exchange approximately three million messages. Facebook gathers an estimated 500 terabytes (TB) of data every day. By comparison, the entire US Library of Congress comprises a mere 20 TB. Since almost no-one knows how their data is connected with other information, who makes use of it and what can be done with it, most citizens are largely at the mercy of the world of "big data" and are seriously limited in their ability to establish how their personal data is being used.

This is why we need IT security. However, since new protection mechanisms usually spawn new means of attack, IT security should primarily be understood as being a forward-looking process. The task of research is to develop innovative protection measures and reliable solutions which will continue to function into the future and can break the vicious circle of attack and response.

IT security research always also has in mind the needs of citizens, companies, and public institutions. In order for IT security to become a matter of course for everybody, we need solutions which right from the outset take into account the realities of usage—something possible only if all involved parties engage in ongoing dialogue with each other. Technological approaches and solutions for IT security standards are required

together with ethical, legal, and economic research contributions.

IT security is an important element of the government's public services provision, but one in which the state finds itself caught in a constant conflict—between citizens' entitlement to the protection of their data on the one hand, and the security demands of our society on the other.

A prerequisite for users to be able to trust the IT infrastructure is that the state must as far as possible guarantee IT security. Accordingly, effective IT security means above all protecting the IT infrastructure from attacks by unauthorized third parties. Laws and regulations apply equally in both the "real" and the virtual world. The web is not some lawless space which protects offenders from prosecution or from the security services.

The government is addressing the challenges of IT systems security and the protection of data as core research topics. With its research framework programme "Self-determined and secure in the digital world", the government is investing in the forward-looking design of technical systems and their general conditions for use in order to protect against cyber attacks and to safeguard the right of our citizens to determine what happens to their personal data. The programme is directed at universities and research facilities as well as at companies and users, and brings together the government's research activities on IT security. The research framework programme implements key objectives of the "The New High-Tech Strategy—Innovations for Germany" scheme, which enshrines innovative solutions for the digital economy and society as a priority task for the future. Because the demands of IT security change rapidly, the research framework programme is designed with flexibility in mind, allowing it to be adapted in line with changing prerequisites and new challenges.

With the research framework programme, the government is also addressing important interdisciplinary topics from the Digital Agenda 2014-2017: Without trust in the security and integrity of the digital world, we will not be able to tap the economic and social potential of the digital revolution.

Digital IT security technologies constitute a dynamic field of innovation with enormous value creation potential. The research framework programme "Self-determined and secure in the digital world" gives us the chance to make Germany a leading provider of IT security solutions. We are very well placed to achieve this. Germany is an international leader in data protection law, and with its excellent research landscape can really make its mark. Since data flows—particularly on the web—do not stop at national borders, the government is also promoting the development process at a European level.

2 Objectives and guidelines

The research topics highlighted in the research framework programme are orientated toward ten objectives and guidelines:

IT security is a public service

The rapid technological progress of information and communication technology, as well as changing user behaviour, constantly result in new threats. As a result IT security is a long-term task, and one which already requires us to provide solutions today for the challenges of tomorrow.

IT security creates trust

Trust and acceptance are indispensable prerequisites for the utilization of the diverse opportunities offered by the digitalization of society and the economy. IT products and services that are proven to be secure, reliable, and user-friendly must create the foundation for this trust.

IT security protects the privacy of our citizens

Citizens must be in a position where they can embrace their right to digital self-determination and decide for themselves which personal data can be collected and how this data can be used. In the digital world, citizens have the "right to be forgotten".

IT security strengthens Germany as an industrial location

The value creation chains of practically every economic area, as in Industry 4.0, change as digitalization progresses. IT security protects the new business models arising against this background, thus promoting economic growth. In parallel, the IT security industry is expanding its international position with the help of innovative technologies and processes.

IT security safeguards the operation of critical infrastructures

The failure of one or more critical infrastructures has serious effects for both the state and population of Germany. IT security should increase the protection afforded to critical infrastructures to ensure their availability and prevent chain reactions.

IT security is targeted at the needs of users

IT security solutions are only implemented if they can prove themselves in daily use. IT security solutions must therefore ensure the required level of protection and data transparency whilst being easy for the user to use and understand.

IT security is measurable

The measurability of IT security enables the assessment of social and technical IT security risks and of the corresponding solution approaches. IT security research develops the parameters and methods which are needed for this.

IT security is interdisciplinary

IT security requires networked thought and action across disciplinary borders and process chains—from research and development to the application of IT security solutions. This means that social, legal, and commercial issues are taken into consideration right from the start.

IT security is European

Europe's industrialized societies would find it hard to survive without powerful and safe information and communication systems. Along with its European partners, Germany will develop its own technological key competences in IT security in order to reduce dependency on entities outside Europe.

IT security is international

The challenges of the digital world cannot be overcome at a national or European level alone. IT security requires international solutions that provide the required legal bases and standards. Only in this way can new IT security solutions attain global effect.

3 Research focuses for the future

On the basis of the stated challenges and objectives, the research framework programme concentrates on four major research focuses which encompass technical, economic, and social aspects of IT security.

High-tech for IT security
One research focus emphasizes the technical prerequisites for future-proof and secure ICT, such as hardware-based security modules, effective cryptography processes, and digital identity management, together with quantum communication technologies.

Secure and trustworthy ICT systems
Because IT security is not only about individual elements but must function as an entirety, the second research focus lies on secure and trustworthy ICT systems. These include the transparent and user-friendly design of IT security, reliable protection against Internet attacks—including within heterogeneous system structures—and increased knowledge and product protection.

IT security in fields of application
The specific requirements of particularly complex and significant fields of application, such as networked production systems, critical infrastructures, medicine, and transport, are the subject of the third research focus.

Privacy and data protection
Privacy and the protection of personal data are fundamental prerequisites for the self-determination of the lives of each of our citizens. These issues form the subject of the fourth research focus, whose research includes cyberculture and the challenges of big data.

3.1 High-tech for IT security

To make information and communication technologies fit for the demands of the future, innovative and secure tools and components are a vital prerequisite.

3.1.1 Hardware-based trusted platform modules

Trusted Platform Modules are technical modules which prevent the reading and changing of specially protected areas, such as special security chips. These modules can be used to store sensitive data such as cryptography keys or certificates but are also suitable for use as launch points for integrity-critical processes such as system start-up. Trustworthy firmware employed in conjunction with hardware-based modules provides the basis for security-critical platforms and applications.

Reports of new analysis and attack technologies are published practically daily. As a result, there are ever more opportunities for attacking hardware modules. The research task is to develop security modules for security-critical systems and applications able to with-

”IT security creates trust.“

stand attacks in the long term and which can be efficiently and cost-effectively integrated into IT systems.

Key research topics include:

- Tamper-resistant hardware-based or hardware-related modules that in conjunction with verifiably trustworthy firmware are suitable for embedded and mobile systems as well as for server systems
- Cross-manufacturer aggregation of different trusted platform modules

- Validation of the security of trusted platform modules
- Prevention and detection of hardware manipulation

3.1.2 Digital identity management

Trust on the Internet can be created only if users can rely upon the secure and clearly attributable identity of persons. For objects equally—for example in the "Internet of Things"—it is important that identities cannot be easily bypassed, falsified, or stolen. The consequences of identity theft can be serious, ranging from cyber bullying to fraudulent purchases/sales and even industrial espionage. As Internet use intensifies, the number of cases of identity theft on the net is growing constantly. In 2014, some 16 million stolen digital identities were discovered in the analysis of botnets.

We need trust infrastructures with identities which can be safely and independently managed by users themselves while also contributing to protection in the "Internet of Things" and in the Industry 4.0 environment.

Key research topics include:

- User-centered identity management which protects individual users and their privacy
- Further development of the identity management of existing individual solutions to create standardized, comprehensive, and widely applicable solutions
- The combination of different forms of digital identities to achieve additional security
- Efficient implementation of digital identities for objects in order to ensure the "Internet of Things" is secure

3.1.3 Long-term secure and efficient cryptography

Making payments over the Internet, sending private messages, and logging onto Facebook—all these things are safe only where trustworthy cryptographic processes are in place.

The most widely used cryptographic processes are currently based on complex algorithms which cannot be cracked by normal computers within a reasonable amount of time.

Quantum computers, however, are able to compute using superimposed states, which could render many of today's cryptographic processes unusable. While theoretical approaches for alternative processes are already in existence, algorithms resistant to quantum computer hacking nonetheless remain a long way from practical application.

What is needed are practical cryptographic processes which are secure today and which will remain so once high-performance quantum computers become available.

Many applications call for cryptographic security features for individual components which are sometimes extremely small and low-cost, such as sensors. Components like this, however, often have low memory and computing resources available, meaning that implementation of current cryptographic processes can only be implemented in very restricted ways.

Key research topics include:

- Algorithms which are resistant to quantum computers and can demonstrably be implemented in today's popular applications safely and efficiently
- Processes which enable the encrypted data to be handled and can demonstrably be implemented in applications safely and efficiently
- Practical processes for secure communication where mutual distrust exists
- Lightweight yet demonstrably secure cryptographic processes which are particularly well-suited to use in systems with limited resources

3.1.4 Quantum communication

Quantum communication allows the transmission of sensitive information—such as cryptography keys and access data for bank accounts—in a way that protects its confidentiality. Any attempt by an attacker to listen in on the exchange of information can be detected by the recipient.

Quantum communication connections have to date been possible only over distances up to 150 km. Where transmission over longer distance is required, measures are needed to counteract the unavoidable weakening of the transmitted signal.

A traditional signal repeater receives, amplifies, and forwards the signal. In quantum mechanics, however, each measurement results in a change to the photons, with the result that the same fundamental principle which protects quantum communication from listening in also prevents amplification of the signal in the traditional sense. In quantum communication the role

of the "amplifier" is fulfilled by the "quantum repeater" which works with quantum-mechanically entangled photon pairs.

The task of research is to increase the performance of quantum repeaters to also enable quantum communication over long distances.

Key research topics include:

- Improvement of the performance of quantum repeaters by means of longer storage periods, higher efficiency, and improved signal sources
- Further development of individual technology concepts that have already proven successful in laboratory testing, and the combination of these into an application-ready state
- Theoretical bases for the transmission of information in quantum networks, in particular the development of optimal transmission and correction processes
- Analysis of the impact of targeted disturbances and side channel attacks against new technologies and the development of effective countermeasures against such attacks

„IT security is a public service."

3.1.5 New security technologies

IT security is an ongoing race against the attackers, with each new technological development providing new opportunities for attack. Anyone trying to hold on to a status quo that is secure today will become an easy target for cyber criminals tomorrow. After all, cyber criminals also make the most of progress and now are faster and more professional than ever. New communication channels are also used as a means to escape prosecution.

In order to block new attack scenarios right from the outset, and facilitate the resolution of IT security incidents, these developments are quickly brought within the remit of the new security technologies and projects are promoted to research and develop new technological approaches.

An initial topic for the new IT security technologies is research into new data-protection-compliant methods for the detection and resolution of IT security incidents. These open up opportunities to detect anomalies and abnormalities arising in connection with IT systems—even in real time—in a data-protection-compliant way, and determine whether a technically or legally significant event is occurring. Following an incident, forensic measures can be employed to reveal, analyse, and evaluate digital traces. Fast and efficient decision-making can help minimize damage. Further—and not yet foreseeable—security technologies research topics will also be quickly taken up.

3.2 Secure and trustworthy ICT systems

Trust on the part of citizens, consumers, and companies in the security of ICT systems has diminished greatly in view of criminal attacks, tracking and profiling by IT enterprises, and cyber and digital industrial espionage. Four out of five Internet users no longer believe their data to be secure.

Effective measures against cyber crime, sabotage, espionage, and other undesirable IT incidents, together with the fair and trustworthy handling of data and information, can help to build trust and so are key concerns of secure and trustworthy information processing. The self-determined and independent interaction of users with ICT systems requires users to have freedom of choice with regard to product selection and the configuration and use of ICT systems, and total control over these ICT systems.

This requires that not only individual components and applications be made secure, but that complex systems must be protected. Security should already be considered during the development of IT systems in the sense of "security by design". Trustworthy solutions that are also practical for users—for the protection of privacy, the safeguarding of mobile devices and business processes, and the protection of networked production and automation systems—contribute fundamentally to Germany's position as an ICT hub.

3.2.1 Transparency and user-friendliness

Defence against attack is usually the greatest concern in the development of IT security solutions today, with too little attention being paid to aspects of transparency, usability, and ease of understanding. The fact is however that IT security solutions which are overcomplicated or are not transparent will often be shunned or bypassed, or may inadvertently be incorrectly applied.

For example, all common e-mail clients and messaging applications support end-to-end encryption. But this encryption is not "on" by default, it needs to be activated subsequently. Most users fail to change default settings—one of the main reasons for the insufficient extension of insecure e-mail communication.

Security solutions are needed which both ensure the required level of IT security and are transparent enough to allow users to employ them intuitively and efficiently. Furthermore, these solutions must also be "transparent" in the sense that they can be fully verified by third parties such as certification authorities.

Key research topics include:

- Easily-understood and intuitive technologies (such as search engines), which take into account the issues of transparency, risk assessment, and control for users
- Technologies which allow the effects of human error, force majeure, and targeted attacks to be minimized
- Mechanisms for the safe and trustworthy control of individual and personal data stored on the Internet
- User-friendly control and trust infrastructures as the basis for the effective protection of personal data, especially with regard to end-to-end encryption

3.2.2 Protection against Internet attacks

The open structure and anonymity of the Internet contribute to the increasing number of Internet attacks. Attack tools and methods are easily and cheaply available, and there are many ways in which to obtain confidential information, perform sabotage, and make money from criminal transactions. Information on vulnerabilities, malware, and illegally acquired data are often traded on the global market ("malware as a service").

Amongst other things, targeted attacks penetrate networks to install custom malware which for a long time may remain undiscovered. The attack itself often takes place only some weeks—or months—later. To be able to counter these, analysis methods are required which enable early detection and allow the creation of an overview of the IT security situation, along with warning systems, strategies and methods for tracking and defending against web attacks.

Key research topics include:

- Comprehensive concepts and technologies which are less vulnerable and better protected against Internet attacks
- Efficient analytical methods able to identify anomalies in order to detect and analyse attacks, in real time and with a high level of reliability, and able to aggregate the data to create a full overview of the IT security situation.
- Models and assessment/forecasting processes for the derivation of preventative measures and required actions
- Prevention, early detection, and defence against targeted multi-stage attacks and malware, including on mobile devices

„User-need oriented IT security."

- Next-generation intrusion detection systems that go beyond the detection of anomalies in network traffic and are able to give early detection of new threats such as hardware Trojans and modern malware

3.2.3 Demonstrable IT security

Citizens, companies, and the public sector need to be assured that their data, knowledge, and products are protected in the digital age. Trust is created if ICT systems security is demonstrable and so is transparent and measurable for users.

Design flaws and implementation errors in hardware or software can result in serious IT security incidents. The "Heartbleed" vulnerability in the widely used OpenSSL security protocol—which remained undiscovered for more than two years—is the most serious example of this to date. One small bug affected hundreds of thousands of Websites and—potentially—hundreds of millions of users.

In future all parties involved—from developer to integrator and ultimately the user—should be in a position to evaluate ICT systems with respect to potential security gaps. IT security needs to be seen as a fundamental quality indicator throughout the process, beginning with the development of an IT product all the way to its manufacture. Of particular interest here are the business models for IT security solutions based on open standards and free software.

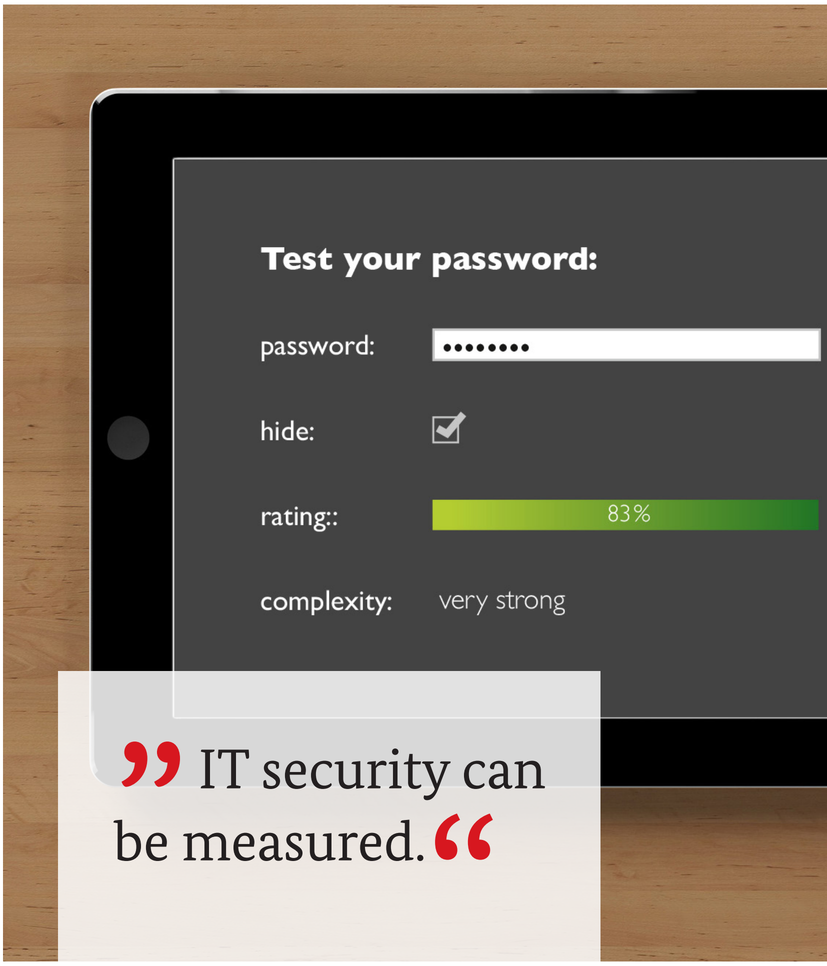
Key research topics include:

- Consideration of IT security and privacy during the development and manufacture of hardware and software products, systems, and services ("security and privacy by design")
- Static and dynamic software code analysis to maximise effectiveness and freedom from errors
- Quality assessment of the IT security of hardware and software and of analysis tools
- Quantification of the cost benefits of secure IT products from a business perspective

- Effective certification of IT products' security (hardware and software) and systems, taking into account ever shorter product life cycles and reducing budgets

3.2.4 IT security in heterogeneous system structures

From the "Internet of Things" and its associated autonomous networking, up to service-oriented platforms— ICT systems today comprise a multiplicity of components spanning national and sector borders. However, the use of products of unknown origin increases the risk of security gaps and hidden malicious functions which can—for example—be concealed in the control software or on a microchip. As a result, other IT products such as printers and IP telephones can also present considerable risks.



Test your password:

password: ••••••••

hide: ☑

rating:: 83%

complexity: very strong

> ,, IT security can be measured. ‘‘

It must be ensured that the required level of IT security can be guaranteed on a long-term sustainable basis even in complex, heterogeneous ICT systems and in non-trustworthy environments.

Key research topics include:

- Modelling and evaluation of the IT security of hardware and software, (mobile) devices, and of an entire system
- Models, architectures, and mechanisms which ensure the required IT security level of an overall system even if individual components are not trustworthy (for example, in the case of applications running on platforms or operating systems that are not secure)

- Protection of especially critical communication channels and components, for example in software-controlled structures such as software-defined networks (SDNs) or in new telecommunications protocols
- Physical—and also practical and cost-effective—access protection for ICT systems and components requiring special protection
- Demonstrable compliance with the required IT security level in supply chains, for integration into existing systems and where replacing or updating individual products or components

3.2.5 Protection of knowledge and product

Enormous economic damage is caused to Germany as the result of intellectual property loss and the dishonest counterfeiting of products. In 2013 alone losses to German machinery and plant engineering from product and brand piracy amounted to 7.9 billion Euros, and the situation is getting worse.

Chips for example contain programming code or process control software—information which can generally be read with relatively little effort. Chips that have been tampered with can be used to attack networked telecommunications systems, production systems, and even the electricity grid. Ultimately the use of a chip that has been hacked, or is a low-grade counterfeit, can endanger IT security and put at risk the reliability of infrastructures, networks, and applications. Accordingly it should be possible to at all times protect technical knowledge and products. On the other hand, such protection should not deny the true owner control over how their products are used.

Key research topics include:

- Practical and demonstrably effective processes for protecting software
- Preventing the reverse engineering of hardware and software products

- The combination and integration of different processes and measures for the protection of knowledge and products, for example with differing locations and severities of effect

3.3 IT security in fields of application

Almost one in three companies in Germany has had their ICT systems attacked in the past two years. 58 % of affected companies state that the attacks occurred "on site" and that e. g. targeted data was stolen or malware introduced to their systems via USB stick. 30 % relate that the attacks took place over the Internet.

Both existing and new business models such as "Industry 4.0", "Smart Home", and "Smart Services" (the blending of products and Internet-based services) are successful only where both citizens and companies are able to rely on the protection of their data and IT systems. IT security creates trust, contributing to the acceptance of innovations, and as a result is a strategic success factor for German companies.

Some fields of application nonetheless have extremely type-specific IT security requirements that cannot be met using standard solutions. Below are some particularly relevant fields of application for which even today the need for specific made-to-measure solutions is already clearly apparent. Further application fields such as Smart Home and Smart Services should also be considered here.

3.3.1 IT security for Industry 4.0

Industry 4.0 is the end-to-end comprehensive and global networking of products and processes in industrial value creation. Industry 4.0 machines, systems, and products become more intelligent and "talk" to each other—from ERP systems for order planning, via SCADA computers at the control level right down to sensors at the field level. As a result the threat from cyber attacks on IT systems now also extends to industrial machinery and control systems.

Industrial networks are not only an attractive target for cyber criminals—for competing machine builders as well, penetrating the network of a German competitor and inserting targeted malware can certainly pay dividends. Whether this disrupts production, or sets-up a back-door into the corporate network and to sensitive business data, significant financial losses can result for the attacked company. Industrial espionage costs the German economy around 4.2 billion Euros annually; one in three companies suffers financial losses due to espionage, and more than 50 % of material damages occur as a result of outages, theft, or damage to IT or telecommunications systems.

Affording protection against economic crime and industrial espionage requires new solutions for IT security and its comprehensive integration into the vertical and horizontal value creation chains. In the industrial environment, however, the wide variety of machines

and systems, and their long service lives, pose a major challenge. Operating cycles may stretch over months, with only limited windows available in which maintenance can be performed.

Security solutions should as far as possible be standardised or based on standard interfaces so that competition is unobstructed and cost-effective solutions are facilitated.

Key research topics include:

- Sustainable IT security over the entire life cycle of industrial machines and systems, taking into account special industrial features such as real-time requirements
- Integration of IT security solutions into existing systems, and new networked production environments, without incurring downtime
- Modular, standardised IT security solutions which are scalable by producers, integrators, and users—in particular for the secure connection of process control systems
- Quantification of IT security as the basis for cost-benefit estimates for IT security investments
- Legal (e. g. liability, data protection, and copyright) and sociological issues

3.3.2 IT security in critical infrastructures

As new digital technologies grow, so does the number of weak points. The higher the dependence of critical infrastructures on digital technologies, the more vulnerable they become. In Germany the Federal Ministry of the Interior has classified critical infrastructures into nine sectors: energy, transport and traffic, information technology and telecommunications, finance and insurance, health, the state and administration, water, media and culture, and nutrition. Averting these dangers requires both the state and the infrastructure facility operator to agree on protection concepts. In Germany responsibility for approximately four-fifths of critical infrastructures lies with the private sector.

For example, under the name "Dragonfly" hackers have recently attacked American and European utility companies. Internal tests by a public utility company in Germany have shown that a hacker—deliberately commissioned in this case—was able to penetrate the control network of the city facility in a mere two days. In a major metropolis such as Berlin, the cost for example of a one-hour power failure at midday resulting from a cyber attack is estimated at 23 million Euros. But it is not just the economic consequences that can be dramatic. Should a hacker attack on an energy company paralyse the power supply to hospitals, or malware take out the emergency power supply, human lives are also put at risk. More extended power outages can massively impact every aspect of life, including water supplies, the waste cycle, traffic, and availability of food.

❞ IT security strengthens Germany as a location. ❝

The energy transition itself is also bringing increased demand for information technology. Power supply is becoming increasingly innovative, decentralized, and computer-controlled—making power grids increasingly vulnerable.

The task for research is to work together with the operators of critical infrastructures to develop methods and tools for the reliable protection of essential IT systems, so that supply services delivered via these critical infrastructures can be permanently guaranteed.

Key research topics include:

- Analysis and assessment of the potential for attack of critical infrastructures, and any consequent domino and cascade effects
- Design of comprehensive protection concepts and high-quality, cost-effective IT infrastructures
- Early detection of disturbances and outages in critical infrastructures and solutions to minimise their effect
- Prompt and autonomous restoration of the supply service whilst ensuring required levels of IT security
- Recording and evaluation of security-relevant events to facilitate long-term continual improvement of protection levels, provision of an overview of IT security situation, and support for risk management
- Practical and cost-effective IT security solutions for the sustainable and continuous protection of critical infrastructures, and ensuring their integrity over the entire life cycle

3.3.3 Secure ICT applications in medicine

With the growth of computer-aided surgery, networking of medical imaging, and mobile solutions for real-time patient monitoring, ICT is also playing an increasingly important role in in healthcare.

Networking of devices is already quite advanced in medical technology. Mostly, however, this is delivered by manufacturer-specific end-to-end solutions. It would be preferable to be able to call up a patient's data via any device from any manufacturer, from the patient's arrival in the clinic or hospital right through until their release and—ideally—during further outpatient treatment as well. Before this vision can become reality, however, medical devices must fulfil high permit requirements. Proof of security is particularly hard to achieve where devices from different manufacturers are networked. Faced with an ever more elderly society, the question of providing ICT-supported medical care at home is also becoming increasingly important. Treatment at home can be considerably aided—and in some cases is only made possible—through the use of telemedicine and Smart Home technology.

Whether in a clinic, the home environment, or the care sector, the best possible care for patients should be guaranteed. The challenge lies in ensuring the protection of sensitive health data along with advanced digitalisation and manufacturer-independent networking of health management.

Key research topics include:

- Secure and dynamic networking of medical devices in planning, diagnostics, and treatment as well as in the clinical IT environment
- Secure integration of mobile devices, for example in the operating theatre and clinical IT environment

> ” IT security safeguards the operation of critical infrastructures. “

- Patient-oriented solutions for intelligent networking at home and in the care sector that comply with data protection regulations and legislation

3.3.4 IT security in transport and logistics

The extent of networking in vehicles today is vast: depending on the vehicle class, up to 50 networked components are controlled via microprocessors. More than 100 sensors and as many as 200 processors are at work in a modern car. In addition vehicles are networked into cooperative traffic and transport infrastructures, forming interconnected systems via vehicle-to-vehicle (Car2Car) and vehicle-to-infrastructure (Car2X) communication which increase traffic safety and transport efficiency. The efficient use of planes, buses, and trains, together with logistics services, are increasingly reliant on these new networked structures.

The new technologies of the so-called "connected cars" bring mobile communication to vehicles. The protection of systems of this type is just as important as the protection of servers and home PCs, particularly in view of the potentially serious consequences for drivers and other road users.

To enable the building of cooperative traffic infrastructures participants must be able to rely on the security of the information and data of their partners. The absence of an agreed approach to security will considerably reduce acceptance of the application—and procurement—of cooperative systems. On the other hand, security solutions must not impair competition and should accordingly be based on standardized interfaces.

The preconditions for IT security solutions for protection of the vehicle (in-vehicle security, embedded security), of the driver, and of other road users, as well as those for autonomous driving, must be established. Inter-vehicle communication channels also require special protection.

Key research topics include:

- Protection of vehicle communication (Car2X), vehicle control, and vehicle data

- Design of integrated privacy-respecting IT security solutions for intelligent traffic management and control, and the integration of these solutions into existing infrastructures

- Updating of IT security mechanisms throughout the entire product life cycle

3.4 Privacy and data protection

In 2013 Internet users in Germany were each online for an average of 169 minutes daily—up by more than 25 % against the previous year.

Users increasingly are having to "pay" with personal data for Internet services and social media use, a situation intensified by the use of mobile devices. Users on the whole no longer have any control over what ultimately happens to their data, how it is used, or to where or whom it may be sold on to. This brings new threats: for example, online visibility of a visitor's attendance at an event allows criminals to take advantage by breaking into the visitor's unoccupied home. In addition a wide range of activities are stored, gathered and aggregated into profiles—with the user often being totally unaware this is happening. This in particular affects every user of a mobile communication device, whether it be a smart phone, navigation aid, or wearable sports device used by an amateur athlete to record and store their vital data.

3.4.1 Privacy and self-determined living in the digital world

To allow citizens to embrace their right to self-determination and be able to protect their privacy requires on the one hand the establishment of technical preconditions. On the other hand, the individual media skills of users also need to be reinforced, on top of which it must be ensured that business models based on the evaluation of personal data allow for monitoring by users.

The challenge facing research is to establish technologies for the protection of privacy such that they can be used effectively, and with minimal extra effort, by the ordinary person. Digital services must be designed in a way that users retain full sovereignty and control over their data. Technology-supported data protection (privacy by design) should be further developed and improved.

Key research topics include:

- Challenges relating to the protection of personal data resulting from the increasing networking of different aspects of life (such as Smart Home, e-mobility, etc.)

- Mechanisms and opportunities for protecting personal data that are intuitive to use and whose protective effects are comprehensive, readily understood, and accountable, for example by providing a "quality seal"

- Procedures and infrastructures for trusted and anonymous communication on the Internet that can also be used by the ordinary person

> ”IT security protects the privacy of our citizens.“

- Technical, organizational, and legal bases which enable users to reliably delegate complex data protection tasks to service providers

- New types of online communication which enable the self-determination of information and the protection of privacy

3.4.2 Internet culture—life and value shift in the Internet age

Over the last 20 years, the Internet has developed into a universal communications platform. Increasingly, our professional and personal communication takes place in the digital world, and closed-in communities are being extended by open networks. Our everyday lives are supported and culturally enriched, but also accelerated, by digital services and products.

The constant global availability of digital services and products promotes socio-technological innovations and contributes to personal fulfilment, while at the same time new behaviours and cultural techniques are emerging. To date it has only partially been possible to understand and scientifically document the diverse effects the Internet has had on our lives, and the associated value shift—the Internet culture.

A central task of research is then to assess developments in Internet culture with regard to their social implications. This also includes support for innovations and social developments through appropriate norms and guiding principles. To enable a comprehensive approach such as this the social science, legal, ethical, and technology sectors must work together.

Key research topics include:

- Researching and interdisciplinary monitoring of the value shift and associated social practices occurring in the Internet age

- Overall societal assessment of the significance of norms and values in the digital world

- Researching and promotion of the cultural environment for new areas of business, such as smart services, arising from the coming together of the digital and "real" world and the challenges resulting from this with respect to protecting the self-determination of personal data

- Safe, secure and democratic shaping of opportunities for direct political and social participation

3.4.3 Privacy and big data

The use of social media such as Facebook and Twitter, and increasing networking of various systems such as traffic control cameras and car-sharing fleet vehicles, contribute to significant accumulation of data. Every Internet activity leaves behind data trails—whether using online services, visiting search portals or online stores, or using Web-supported sensor systems to monitor the heart rate or blood pressure of athletes.

The market for trading data is growing rapidly. The global turnover for big data products and services grew to around 73.5 billion Euros in 2014—that equates to growth of 66 % against the year 2013.

Many people regard the disclosure of certain personal details as harmless—or even useful if it means, for example, that on-demand products and services can be offered on the Internet customised to individual preferences. However, such information allows others to draw conclusions about your interests, lifestyle, and habits. Computer-based technologies are able to filter out the countless, often tiny data trails of individuals from a large set of data to build detailed profiles of groups and individuals.

These profiles can be used to categorize individuals, who may then be unable to either understand, or correct, such a categorization. This may have serious consequences if, for example, a potential employer declines an applicant due to his or her lifestyle choices, or where someone can only buy insurance under excessively stringent terms as a result of lifestyle information becoming known.

The task for this research is the creation of concepts which ensure the basic rights of citizens—the right to live one's life, to privacy, and to protection of the right to determine how one's personal data is used—also apply to big data applications.

Key research topics include:

- Design of big data services in accordance with the principle of data minimization; in particular to allow profiling, and business models that are based on this, to function without gathering individualized personal data

- Anonymization and pseudonymization of big data services
- Development of new legal and technical concepts for the protection of sensitive data in big data analyses
- Enforcing the purpose and contextual relationship, from a technical and legal perspective, of personal data in big data analyses
- Definition of privacy metrics
- Design of data mining processes and applications which preclude the profiling or disadvantaging of affected users

> ”IT security is international.“

4 Shaping IT security research

4.1 Developing national competences

Innovative IT security research gives us the opportunity not only to defend ourselves against cyber threats but also to develop secure IT products and services, making Germany a leading provider of IT security technology and strengthening its digital sovereignty.

Supporting and connecting research

Since 2006, in a cross-cutting approach, the Federal Government has been pulling together its research and innovation activities into its High-Tech Strategy in order to build on Germany's leading position in key technologies and accelerate the implementation of research results to create products and services.

Research support in the field of IT security contributes to achieving a high performance level in the international IT security research rankings, and to ensuring the prompt exploitation of research results. This takes place primarily as part of cooperative and individual projects relating to the named research focuses.

Collaborative projects are an important instrument of project support in which scientific institutions and companies work together on an interdisciplinary basis. Users and end users play an important part in these projects, ensuring transfer of results into applications. Specific funding measures are selected on the basis of the quality of the research approach, economic viability, and a proper balance between expenditure and benefits.

Centres of competence for IT security

Since 2011, the Federal Ministry of Education and Research has been sponsoring three centres of competence for IT security research which are developing new approaches to IT security research:

CISPA—Centre for IT Security, Privacy and Accountability in Saarbrücken;

EC SPRIDE—European Centre for Security and Privacy by Design in Darmstadt;

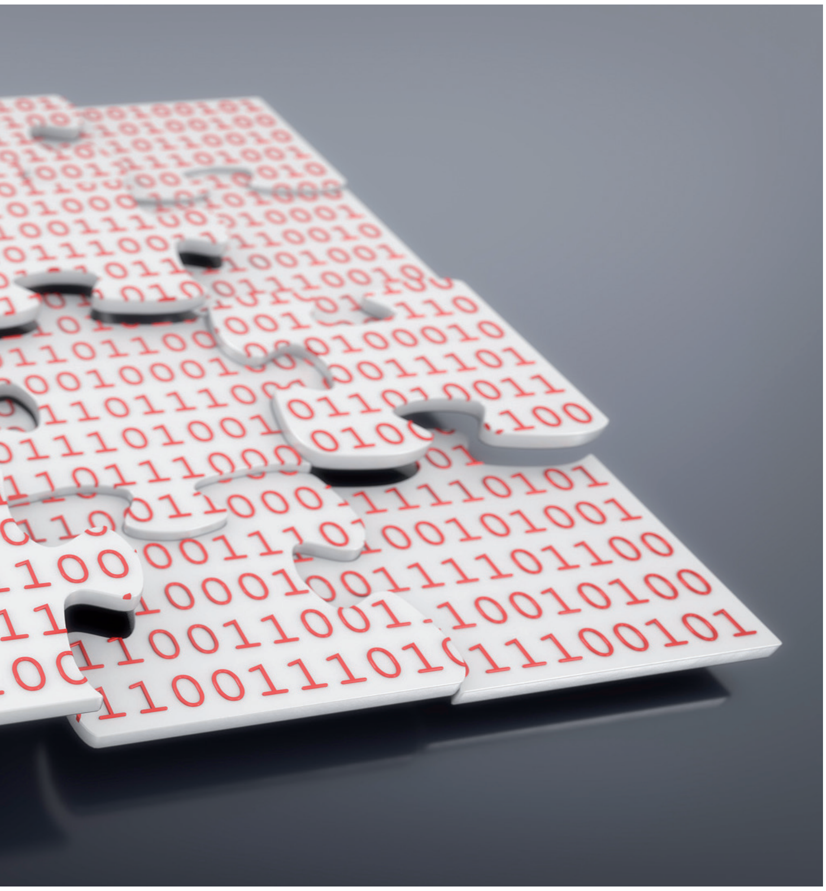
KASTEL—Centre of Competence for Applied Security Technology in Karlsruhe.

The centres of competence are outstanding locations for IT security research in Germany. The pulling-together of national research competences avoids expensive duplicate and parallel structures and facilitates the consolidation of research content as appropriate.

» IT security is interdisciplinary. «

The centres were established as regional hubs where expertise on IT security-related issues is brought together and interdisciplinary research is performed. They grapple continually with current and new research issues to formulate timely and flexible appraisals, recommendations for action, and solutions to new challenges. All three centres cover a broad spectrum of IT security research, and work in those fields of design, integration, and analysis largely corresponding to their profiles. These centres of competence are to be further reinforced in terms of their importance as a sustainable scientific base, and in order to strengthen the expertise of German research and industry in the field of cyber security.

www.kompetenz-it-sicherheit.de
(in German only)



forum
<privatheit>
selbstbestimmtes_leben_in_der_digitalen_welt

The forum "Privacy and self-determined living in the digital world" is an interdisciplinary group of experts who—as a project—analyse from various academic perspectives the socially relevant issues regarding the protection of privacy and formulate proposals for holistic solutions.

To this end the forum identifies the relevant interfaces between the disciplines and enters into intensive academic and open debate from which new research topics are developed.

www.forum-privatheit.de (in German only)

Promoting of small and medium-sized enterprises (SMEs)

The IT security segment in Germany makes up just below 10 % of the entire IT sector. For small and medium-sized businesses in particular, IT security is an important business area. For more than half of SMEs in Germany IT security is the prevailing technology trend in information technology.

Young, dynamic companies with innovative ideas for new IT security solutions are supported by the Federal Ministry of Education and Research so that they can react flexibly and internationally in the rapidly growing and constantly changing field of IT security. Small and medium-sized IT companies tend to take a relatively long-term view and play an important role in the widespread adoption of new IT security solutions, and the research activities of SMEs receive particular support.

Since 2007, the Federal Ministry of Education and Research has been offering fast and easy access to technology funding programmes in the form of the "KMU-innovativ" research initiative for SMEs in addition to the traditional funding programmes.

www.kmu-innovativ.de (in German only)

4.2 Strengthening European and international cooperation

Research and innovation secure the competitiveness of Germany and Europe within the global market. Current challenges cannot be overcome by a single nation working alone. As part of this programme, bilateral measures and participation in EU measures should bring together national interests and research shared solutions.

Horizon 2020

The European "Horizon 2020" framework programme for research and innovation brings together previously disparate EU programmes for the promotion of research and innovation. Taking an interdisciplinary approach, it considers the entire innovation cycle and so encourages cooperation and the exchange of ideas. The aim of German IT security research is to anchor internationally-relevant research topics on IT security into three programme sections:

- "Excellent Science": Ensuring the competitiveness of the European Union through exceptional research performance
- "Industrial Leadership": Promoting industrial investment and research, particularly in the field of key technologies
- "Societal Challenges": Promoting research and innovations to solve major societal challenges along the entire value creation chain from research to market launch

Examples are the research focuses "Quantum communication" and "Cryptography", which can be found in the sections "Excellent Science" and "Industrial Leadership".

www.horizon2020.de (in German only)
ec.europa.eu/programmes/horizon2020/

Fit for Europe

In order to strengthen the participation of German entities in European IT security research projects and—in particular—in the "Horizon 2020" framework programme for research and innovation, national expertise is being brought together and developed with a view to future topics in the field of European IT security research. Funding measures should be employed to create a successful European network, with German participation, from the European and interdisciplinary cooperation of partners from research institutes together with business and end users.

EUREKA

EUREKA is an initiative for user-driven research in Europe offering industry and science a framework for binational and multinational cooperation projects. The initiative contributes to enabling the technical and financial resources available in Europe to be used more effectively—including in the field of IT security research—so increasing the competitiveness of Europe on the global stage.

The project "Safe and Secure European Routing—SASER" is one example of a successful cooperation project in which partners from five European countries are working together to develop scientific and technical solutions for powerful communication networks, with high security standards and a sustainable cost and energy structure. This successful approach should be continued in order to ensure the existence of competitive European technologies in the future as well.

4.3 Developing dialogue

Innovative IT security solutions must comply with the diverse requirements and needs of public, commercial, and private users. Social dialogue which involves all affected parties—from the world of science to busi-

❞ IT security is European. ❝

ness and private individuals—can contribute to better understanding of the needs of all those involved and to appropriate action. Aligning IT security research to the needs of the market, and quickly and efficiently exploiting scientific knowledge for commercial purposes, requires close intermeshing of science and the economy. At the same time, it is important to ensure the transparent presentation of research results to the public.

In the world of IT security research, legal, economic, and social issues are becoming increasingly important. Comprehensive and realizable solutions for IT security can be achieved only if there is dialogue between the various disciplines and a framework of broad, interdisciplinary cooperation.

The research framework programme follows a systemic approach which takes into account the entire innovation chain, from basic research, via applied research, right through to the value creation delivered by the results. Ongoing exchange of information between universities, extra-university research, and companies allows research focuses to be agreed, projects implemented, and the results of research exploited. Research results consequently get to market, and society, faster in the form of innovations that can be enjoyed by end users.

In the case of socially controversial issues such as privacy and IT security, discussion with citizens that is factually and technically sound can enable a realistic assessment of the opportunities and risks for individuals, and for society as a whole, and can help determine an achievable consensus of opinion.

This dialogue should:

- educate citizens and help them navigate the vast amount of information;
- provide a platform for citizens to discuss the opportunities and challenges of privacy and IT security;
- allow citizens to develop well-founded opinions derived from open exchange of information with experts.

The results of dialogue with citizens are taken into account in the setting of research fields.

4.4 Encouraging a new generation of scientists

To be able to offer cutting-edge secure IT products and services in Germany, we must leverage as far as possible the existing innovation potential we possess. This in turn is driving constantly rising demand for qualified young professionals in IT security.

IT security research addressing the challenges of global competition in science and business must place high priority on supporting the upcoming generation of talent, and corresponding initiatives should be reinforced as part of the programme. This will also encourage the setting-up of young and innovative companies.

European Center for Security and Privacy by Design
EC SPRIDE
EUROPEAN CENTER FOR SECURITY AND PRIVACY BY DESIGN
TECHNISCHE UNIVERSITÄT DARMSTADT
Fraunhofer SIT

Research projects and centres of competence offer young researchers the opportunity to discuss their work with recognized researchers and build communities bringing together new and established researchers.

4.5 General conditions of the research framework programme

IT security is always user-driven. In every area touched by information technology, right from the outset IT security must be considered as well. Linking IT security technology and application fields can open up completely new opportunities and business areas. Considering for example the IT security of Industry 4.0, it is insufficient to simply transfer traditional and established IT security solutions into the new networked IT production world. Industry 4.0 requires new, challenging approaches to architectures and processes. This research framework programme contributes to the ability to exploit these opportunities.

The measures of this research framework programme do not exist in isolation but rather are intermeshed with other research policy activities, in particular those of the civil security research programme, health research (especially personalised medicine), new topics such as "Innovations for the production, services, and workplace of tomorrow", "The information society", and "Electronic systems", and the federal government's research agenda for demographic change.

The research framework programme is designed as an open programme and as such the original programme assumptions, participant structure, and research focus will be reviewed during the programme to assess whether they remain valid, or whether it is necessary to update or extend the programme's content. Task-based budget analysis will also be performed to consider the financial feasibility of measures.

The research framework programme is thus an open platform for application topics in the context of IT security, incorporating all relevant activities in the High-Tech Strategy fields of application comprising digital economy and society, sustainable business and energy, healthy living, intelligent mobility, civil security, and an innovative working world.

The programme is planned to run from 2015 to 2020, the Federal Ministry of Education and Research alone intending to make more than 180 million Euros available to the research framework programme to promote IT security.

Published by
Bundesministerium für Bildung und Forschung/
Federal Ministry of Education and Research (BMBF)
Division Communication Systems; IT Security
53170 Bonn
Germany

Orders
In writing to
Publikationsversand der Bundesregierung
P. O. Box 48 10 09
18132 Rostock
Germany
E-mail: publikationen@bundesregierung.de
Internet: http://www.bmbf.de
or by
Phone: +49 30 18 272 272 1
Fax: +49 30 18 10 272 272 1

March 2015

Printed by
BMBF Hausdruckerei

Layout
VDI/VDE Innovation + Technik GmbH

Photo credits
3dkombinat / fotolia: Page 22/23
bugphai / fotolia: Page 14/15
Eugenio Marongiu / fotolia: Page 10/11
Karelnoppe / fotolia: Page 5
Lulla / fotolia: Page 24/25
Maksim Kabakou / fotolia: Page 6/7
Martin Cassel / EC SPRIDE: Page 26
morganimation / fotolia: Page 2/3
ojoimages / fotolia: Page 16/17
ojoimages4 / fotolia: Page 18/19
Federal Press Office
Steffen Kugler: Preface
Ralf Kalytta / fotolia: Page 8/9
Rawpixel / fotolia: Page 20/21
Robert Kneschke / fotolia: Page 12/13
storm / fotolia: Title

This publication is issued free of charge as part of the public relations work of the Federal Ministry of Education and Research. It is not intended for commercial sale. It is not allowed to be used for canvassing purposes during an election campaign by political parties, candidates, or campaigners. This applies to parliamentary elections, state parliamentary elections, local elections, and European Parliament elections.

In particular, distribution of this publication at election meetings and at party information stands shall constitute misuse, as shall the insertion, attachment, and affixing of party-political information or advertising material. Furthermore, it is prohibited to pass this information on to others for the purpose of canvassing.

Regardless of how and in what quantity this publication has reached the recipient, it cannot be used in any way which might be understood as the taking of sides by the Government in favour of individual political groups even at times when no election is upcoming.

www.bmbf.de