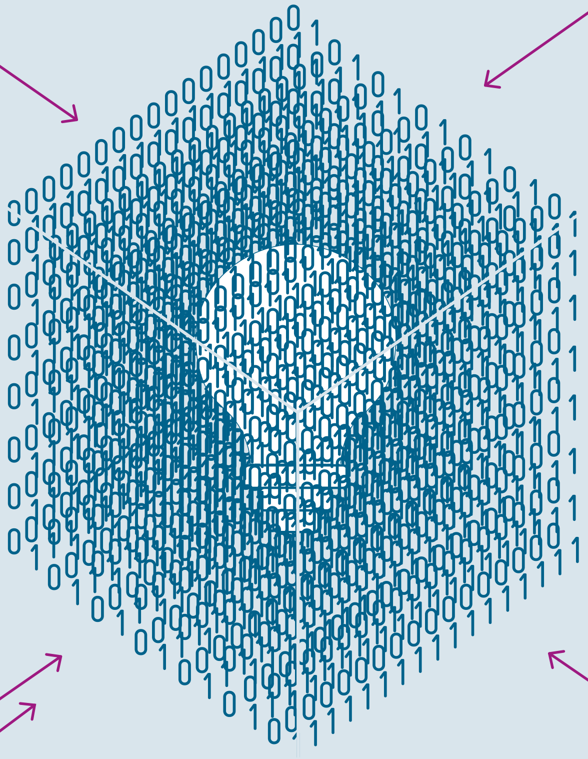
B 2 Cybersecurity

Download data

Ongoing digitalization and connectivity make companies more vulnerable to cyberattacks. Corporate innovation activities are directly affected by this threat.

Malware performs unwanted or harmful functions on a computer system.

Ransomware is used by attackers to encrypt the data in an IT system to prevail upon users to pay a ransom.



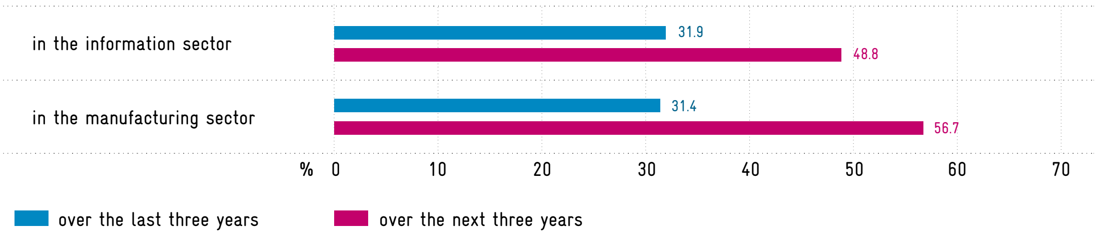
Advanced persistent threats have a high threat potential because the attackers find weaknesses in a targeted and persistent manner in order to exploit them.

Social engineering manipulates people to persuade them to disclose confidential information, open files or links with stored malware, or transfer money to unauthorized recipients.

DDoS attacks cause network services to fail after they have been overloaded and thus blocked by a huge number of requests.

Assessments by companies on the development of the threat from cyberattacks[1]

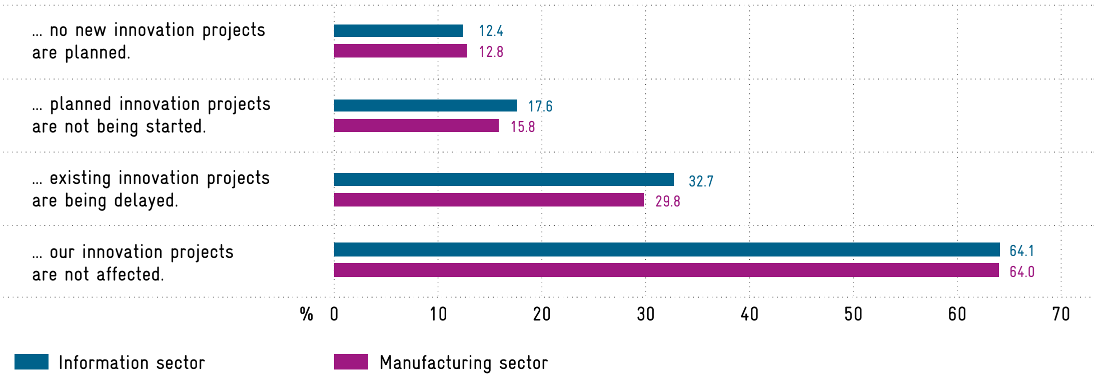
Increase or sharp increase in the threat from cyberattacks …



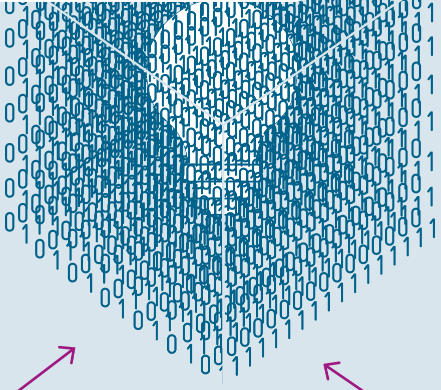
Sector-specific extrapolation of results to the question: "How do you assess the change in cyberattack exposure for your company?" Legend: 56.7 percent of manufacturing companies expect the threat of cyberattacks to increase or rise sharply over the next three years.

Impact of cyber threats on innovation activities[2]

Because of the threat of a cyberattack …



Sector-specific extrapolation of results to the question: "What impact is the threat of a cyberattack having on your company's innovation activities?". Multiple answers possible. Legend: 12.8 percent of manufacturing companies are not planning any new innovation projects because of the threat of a cyberattack.



See chapter D 7 for a list of sources of infocharts.

B 2 Cybersecurity

Ongoing digitalization and connectivity make innovative companies more vulnerable to cyberattacks. The majority of innovative German companies in the information and manufacturing sectors are therefore quite aware of the need to protect the information technology (IT) they need for innovation activities.[148] In addition, more than half of these innovative companies expect the threat posed to their business by cyberattacks to grow further in the coming years.[149] Corporate innovation activities are directly affected by this risk (cf. figure B 2-2).[150] As a result, cyberattacks have an indirect negative impact on Germany's economic growth. This applies in particular to the contribution to growth made by future digital technologies such as artificial intelligence or the Internet of Things, because the success of these technologies partly depends on their security.

Cybersecurity in turn is itself the subject of innovation, and its products and services contribute directly to economic growth and prosperity in Germany. The gross value added of the German IT security industry amounted to €15.5 billion in 2017, accounting for 14.3 percent of the total IT industry with its gross value added of €108.6 billion – compared to 12.9 percent in 2010. Gross value added in the IT security industry grew nominally by an average of 5.6 percent per year from 2010 to 2017. By contrast, the average nominal growth of the overall IT sector and the economy as a whole was lower, amounting to 4.3 percent and 3.4 percent per annum respectively in the same period.[151]

In addition, cybersecurity has an important role to play in maintaining critical infrastructures (CIs). CIs are found in the sectors of energy, information technology and telecommunications, water, food, health, finance and insurance, transport and traffic.[152]

However, an increase in cybersecurity – and thus an increase in German corporate innovation activities – faces a number of obstacles stemming, among other things, from the characteristics of cybersecurity. Typically, cybersecurity has the characteristics of a public good with the associated external effects. Individual actors invest too little in cybersecurity because they do not take into account the positive effects for other actors. In addition, users of IT products such as hardware or software have only limited insight into the level of security made available by providers. Furthermore, it is often difficult for companies to quantify the risk of a cyberattack and assess the resulting damage.

At present, both the private and the public sectors are keen to recruit cybersecurity experts. Yet corresponding positions remain vacant for quite long periods of time. Smaller companies in particular, which are less likely to have cybersecurity experts in their workforce, are therefore finding it difficult to utilize external offers of information on cyber threats and their prevention, and to implement protective measures.

Cybersecurity and innovations B 2–1

Different kinds of cyber threat

According to the Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnologie, BSI, cf. box B 2-1), cybersecurity involves all aspects of security in information and communication technology (ICT).[153] The term cybersecurity has a broader definition than the term IT security. "The field of action of classic IT security is extended to include the whole of cyberspace. This covers all information technology that is connected to the internet and comparable networks and includes communications, applications, processes and processed information based on it."[154] A cyberattack is a case of unauthorized access to IT systems with the aim of provoking a data leak or malfunction. Such an attack on IT systems uses resources of information technology itself.[155]

Because of the abundance of different hardware and software products, there is also a multitude of methods for gaining unauthorized access to IT systems. In its latest status report, the BSI analyses the attack methods it has observed. These include identity theft, malware, ransomware, distributed denial of service (DDoS), botnets, spam, advanced persistent threat attacks (APT attacks) and attacks exploiting modern processor architecture (cf. box B 2-2).

Malware attacks are the most common type of attack with a share of 53 percent, followed by DDoS attacks (18 percent) and APT attacks (12 percent).[156]

Box B 2-1

Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik, BSI)[157]

The BSI is part of the Federal Ministry of the Interior, Building and Community (BMI). It deals with all aspects relating to IT security with the aim of enabling and promoting the secure use of information and communication technology.

In addition to the BSI's official seat in Bonn, there are so-called contact persons in six other cities. These are central contact points for Länder and local authorities, Federal and EU authorities in the respective regions, companies, think tanks and decision-makers in society. Furthermore, the National Cyber Defence Centre (Nationales Cyber-Abwehrzentrum, Cyber-AZ) is located at the BSI. Its remit is to optimize operational cooperation between different government bodies and to co-ordinate their activities. Members of the Cyber-AZ include, for example, the Federal Police and the secret services.

The 'Act to Strengthen the Security of Federal Information Technology' (BSI Act) defines the tasks of the BSI. Its purpose is to draw attention to the topic of IT security in administration, business and society and to support these institutions in implementing IT security on their own authority. This takes the form of formulating minimum standards for Federal IT and recommendations for action for companies and citizens. The BSI is also responsible for protecting the computers and networks of the federal administration. The BSI reports once a year to the Committee on Internal Affairs of the German Bundestag on these issues.

The tasks of the BSI also include (i) the testing, certification and accreditation of IT products and services, (ii) warning against malware or security gaps in IT products and services, (iii) providing IT security advice to the federal administration and other target groups, (iv) informing and sensitizing citizens to the topic of IT and internet security, (v) the development of uniform and binding IT security standards, and (vi) the development of cryptosystems for the Federal Government's IT.

The act implementing the 'EU Directive concerning measures for a high common level of security of network and information systems' (NIS Directive)[158] also created new powers for the BSI in 2017. On the one hand, the BSI's supervisory and enforcement powers vis-à-vis operators of CI were extended, and new powers were created vis-à-vis providers of digital services. On the other hand, cooperation between the Länder and the BSI was strengthened, enabling the BSI to provide the Länder with even more comprehensive support and technical expertise.[159]

Box B 2-2

Current attack methods according to BSI status report[160]

The following description illustrates relevant methods of attack. Some of them overlap and can be combined, e.g. in a multi-stage attack.

Identity theft is a phenomenon that is highly relevant for online business. A specific login is often required to use online services such as social networks, streaming portals, online shops or booking sites. The user is identified to the provider via individual login data. If these login data are stolen, unauthorized persons can gain extensive insight into the user's private sphere and misuse this information. In 2013, for example, an attack succeeded in stealing the names, email addresses and passwords of three billion Yahoo customers.[161] Over a period of five years, the Marriott hotel chain was exposed to unauthorized access to customer data, resulting in the theft of the names, passport numbers and credit card data of about 500 million customers.[162] Identity theft data can be used to gain information for other types of attacks such as social engineering or credit card fraud. Stolen data sets are often sold on online marketplaces. It is possible to check online whether one's login data have been stolen and published.[163]

Malware comprises all types of computer programs that can perform unwanted or harmful functions on a computer system.[164] As reported by the BSI, the IT-security company AV-TEST recorded about 114 million malware variants in the last BSI reporting period between 1 June 2018 and 31 May 2019. This corresponds to approximately 312,000 malware activities daily.[165] According to the BSI cybersecurity survey, 53 percent of the reported attacks used malware.[166] In addition, attacks with malware are among the ten biggest threats to systems for manufacturing and process automation (industrial control systems).[167]

Ransomware is used by an attacker to encrypt the data in an IT system to prevail upon users to pay a ransom. However, the payment of ransoms in the past has not always resulted in the perpetrators decrypting the data again. There are no aggregated figures on damage levels. Nevertheless, individual cases of damage illustrate the damage potential of ransomware attacks. For example, a Norwegian aluminium company reported a ransomware attack in March 2019 and after only a week it had already recorded losses of about €40 million. As recommended by the BSI, the company did not pay a ransom, but restored its data from backups.

IT systems can also be disrupted by so-called **DDoS** (Distributed Denial of Service) **attacks**. These attacks cause network services to fail after they have been overloaded by a large number of requests and thus blocked. Such services include, for example, email

Cyber risks as a threat to innovation activities

Cyberattacks can serve various purposes that impact on companies both in general and in relation to their innovation activities. A distinction is made between attacks on confidentiality, integrity and availability.[170]

In attacks on confidentiality, perpetrators try to spy on confidential information, for example by wiretapping a radio network or recovering deleted information. Attacks on integrity can be manipulations of e.g. information, software or interfaces. In attacks on availability, perpetrators aim to sabotage information or IT services, for example by launching DDoS attacks.

Cyberattacks reduce the potential revenues and increase the potential costs of innovation activities. This in turn reduces the returns from these activities and the incentives for R&D. While the cyber-protection of innovation activities entails costs, it increases the incentives for R&D to the extent that the additional revenues from the protected innovation activities cover the additional costs of cybersecurity.

A representative survey[171] conducted on behalf of the Commission of Experts shows how the threat of cyberattacks can affect corporate innovation activities. 64 percent of both companies in the information sector[172] and companies in the manufacturing sector[173] do not believe that the danger services or corporate websites. DDoS attacks are the second most common type of attack, accounting for 18 percent of all reported attacks, according to the BSI cybersecurity survey.[168] For an estimate of the damage, the BSI refers to the company Netscout, which has calculated total DDoS losses for German companies in 2018 of around four billion euros. Cloud servers are increasingly being rented for DDoS attacks. In the winter of 2018, 59 percent of DDoS attacks were carried out via cloud servers, compared to two percent two years earlier.

Botnets consist of a large number of networked devices such as computers, smartphones or IoT (Internet of Things) devices over which an attacker has gained control. This allows the attacker to misuse the devices for their own aims. When the motives are financial, devices can be misused for cryptocurrency mining, for example.[169] However, botnets can also be used for sabotage when implemented in DDoS attacks.

Spam is defined as unsolicited emails, sometimes containing advertising, which aim to defraud, contain malware, or seek to induce the recipient to disclose login data. The BSI has registered a 40 percent decline in spam compared to the previous reporting period. Spam containing malware has decreased by as much as 96 percent. However, the effectiveness of spam has increased considerably, so it cannot be assumed to involve less potential to cause damage. For example, there are malware programs that analyse the email traffic in an infected system and send new spam messages to contacts of the infected system by referring to the previous email traffic. Such e-mails can deceive even sensitized persons.

APT (Advanced Persistent Threat) attacks pose a particular threat. They are characterized by a high threat potential because the attackers find out weaknesses in a targeted and persistent manner in order to exploit them. The threat scenario is aggravated by the fact that gaining access to powerful tools for APT attacks has become increasingly easy.

In addition to exploiting weaknesses in software, weaknesses in hardware can also be exploited for attacks. Examples of this are attacks using modern processor architecture such as the Spectre variants, Meltdown or Foreshadow. It is unlikely that these weaknesses can be fully overcome. However, the BSI has not yet seen any indication that this method of attack has been actively exploited.

of a cyberattack influences their innovation projects (cf. figure B 2-3). Existing innovation projects are being delayed by the risk of a cyberattack in 32.7 percent of information sector companies and 29.8 percent of manufacturing companies. The figures are significantly higher among companies that expect the threat of cyberattacks to increase or sharply increase over the next three years than among companies that do not expect such an increase.[174] In 17.6 percent of companies in the information sector and 15.8 percent of manufacturing companies, planned innovation projects are not being started because of the danger of a cyberattack. In 12.4 percent of IT companies and 12.8 percent of manufacturing companies, no new innovation projects are planned because of the risk of a cyberattack.

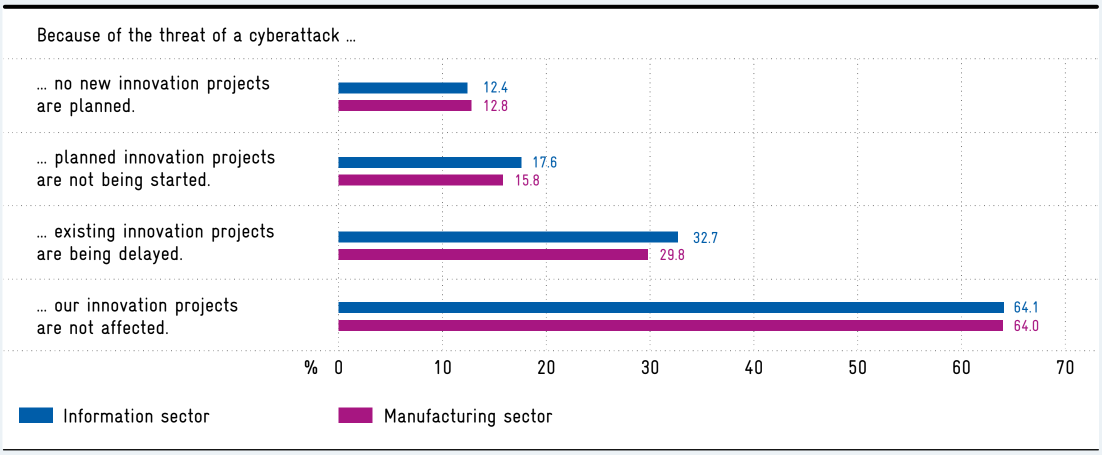
Furthermore, the survey shows that even in companies with no ongoing innovation projects, the risk of a cyberattack plays a role in the decision not to plan any new innovation projects. For example, 14.5 percent of IT companies and 16.2 percent of manufacturing companies with no ongoing innovation projects are not planning new innovation projects.

In order to minimize cyber risks, companies in the information and manufacturing sectors are focusing primarily on investing in IT security, giving the workforce further training in IT, and recruiting qualified IT staff (cf. figure B 2-4). In some cases, the degree of digitalization of innovation processes is also being reduced; in others, innovation projects are being relocated from abroad to Germany. To

Fig. B 2-3

Download data

Impact of cyber threats on innovation activities

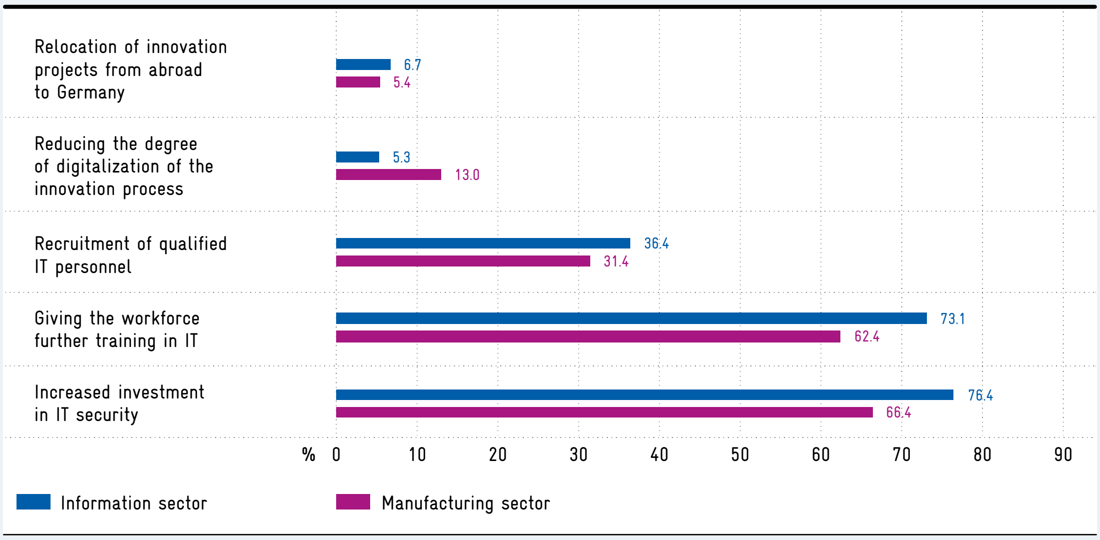


Sector-specific extrapolation of results to the question: "What impact is the threat of a cyberattack having on your company's innovation activities?". Multiple answers possible. Legend: 12.8 percent of manufacturing companies are not planning any new innovation projects because of the threat of a cyberattack.
Source: ZEW Business Survey in the Information Economy, 3rd quarter 2019. Calculations in ZEW (2020).
© EFI–Commission of Experts for Research and Innovation 2020.

Fig. B 2-4

Download data

Measures taken by companies to minimize cyber risks

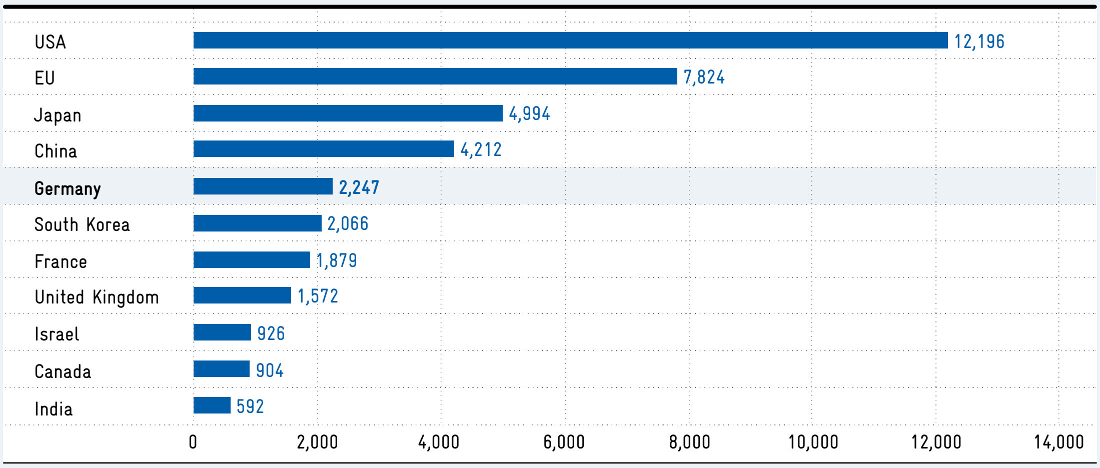


Sector-specific extrapolation of results to the question: "Are the following measures being taken in your company to minimize cyber risks?". Multiple answers possible. Legend: 13.0 percent of manufacturing companies are reducing the degree of digitalization of the innovation process in order to minimize cyber risks.
Source: ZEW Business Survey in the Information Economy, 3rd quarter 2019. Calculations in ZEW (2020).
© EFI–Commission of Experts for Research and Innovation 2020.

Fig. B 2-5

Download data

Number of transnational patents in the field of cybersecurity (top 10 countries and EU) 2000–2017



Source: own diagram based on calculations by the Max Planck Institute for Innovation and Competition.
© EFI–Commission of Experts for Research and Innovation 2020.

minimize cyber risks, 19.2 percent of manufacturing companies with 5 to 19 employees are reducing the degree of digitalization of their innovation process. This applies to only 4.7 percent of manufacturing companies with 20 to 99 employees and to 3.6 percent of companies with a staff of over 100. Reducing the degree of digitalization in response to cyber threats appears particularly critical if there is a risk of losing productivity potential.

Patent activities in cybersecurity

In view of increasing and ever-changing cyber risks,[175] there is a great need to counter these risks with innovative cybersecurity solutions. Innovations in cybersecurity make it possible to both increase the level of protection and expand potential for value creation.[176] Patent applications can provide an indication of innovation activities.[177] For the following analysis, the Commission of Experts refers to international patenting activities that can be illustrated by transnational patent applications. The assignment of the patents to countries is based on the nationality of the first applicant. Figure B 2-5 shows the distribution of transnational patent families in the field of cybersecurity for the years 2000 to 2017 for the ten countries with the most patents plus the EU.[178] With 6.2 percent of patents, German inventors are a long way behind inventors from the USA (33.5 percent), Japan (13.7 percent) and China (11.6 percent). Inventors from EU countries together account for 21.5 percent. The USA and China became increasingly important over the period under consideration and show an above-average increase in patent applications, especially at the end of the period considered.[179]

A comparison between a country's patent activities in the field of cybersecurity with the country's patent activities as a whole reveals that Germany, unlike the USA and Israel, is not specialized in the field of cybersecurity.[180] This specialization by the USA and Israel is also reflected in evaluations made by the American industry analyst Cybersecurity Ventures, according to which 112 of the world's 150 most innovative cybersecurity companies come from the USA, 18 from Israel and only one from Germany.[181]

Challenges at the company level B 2-2

A number of obstacles can contribute to companies failing to achieve the level of protection they need against cyber risks. These include, in particular, the problem of recruiting cybersecurity experts who can improve protection and detect and ward off attacks. In addition there is lack of information on current threat situations, on the extent of damage, and on the quality of IT security products.

Need for experts and competencies

The lack of qualified IT security experts poses a threat to IT security in many companies.[182]

The European Commission has carried out a study in the EU Member States to determine how long it takes to fill vacancies requiring digital skills.[183] This analysis shows that a relatively high proportion of job vacancies in the field of cybersecurity are still unfilled after 90 days. In fields like machine learning and the Internet of Things, a much larger proportion of these positions are filled after 90 days than in cybersecurity.[184]

The high demand for cybersecurity experts is matched by only a few courses of study for cybersecurity experts in Germany.[185] No student statistics are available for the relatively young subject of cybersecurity. Up to now, cybersecurity topics have mostly been taught in computer science courses. The number of students studying computer science rose from 69,559 in the 2010/2011 academic year to 115,005 in 2017/2018, i.e. by almost two thirds.

Because cyberspace touches on many areas of life, it is important to understand cybersecurity not only as a purely technical discipline. For example, there are interfaces with the social sciences, economics and law. When planning study programmes, these should be taken into account accordingly.

Not only academically trained specialists are needed to improve the level of cybersecurity across the board; cybersecurity should also be increasingly integrated into vocational education and training. This could take account of the fact that the level of cybersecurity is not only determined by technical innovations but also by the way people handle hardware and software. There is currently no specific training programme for IT security experts. Training programmes are currently being modernized for IT professions such as computer science expert, IT management assistant, electronics technician for IT systems, and management assistant for IT systems.[186] Since August 2018, IT security has been increasingly included into content of apprenticeship training.

A total of 16,869 new training contracts were concluded in these four IT occupations in 2017. Furthermore, a new recognized occupational profile, 'digitalization of labour, data privacy and information security', has been added to apprenticeship programmes in industrial metal and electrical occupations and for mechatronics technicians teaching content on information security in an integrative way.

In order to develop cybersecurity skills and adapt them to changing requirements, it is in companies' own interests to provide advanced training for their cybersecurity experts and to make use of existing personnel resources. In addition to classic further training courses, innovative approaches can also make a contribution. For example, there are courses offered using methods such as gamification that train staff to ward off attacks (cf. box B 2-6).

In addition to cybersecurity experts, all other employees also have an impact on the level of cybersecurity in a company. For example, emails, which are an important part of everyday working life for most company employees, are often used as a gateway for cyberattacks.[187] In a survey of companies conducted by KPMG,[188] 90 percent of companies counted carelessness and 83 percent of companies counted insufficiently trained personnel among the factors that favour e-crime.[189] It is therefore important to raise awareness and offer further training to the entire workforce on cybersecurity. Many companies already have appropriate measures in place. However, surveys show that smaller companies are less active here.[190]

Reducing the lack of information

A lack of information makes it more difficult for companies to deal with cyber threats.[191] For one thing, companies cannot reliably assess the risk of cyberattacks and any resulting damage. For another, as buyers they often have difficulty in assessing the quality of cybersecurity products and services due to the high and increasing complexity of IT systems and rapidly changing security requirements.

Various measures can be taken to reduce the lack of information on the risks of cyberattacks and the resulting damage. Operators of critical infrastructures, providers of online services and telemedia providers are legally obliged to report cyberattacks to the BSI. For its part, the BSI issues warnings and information via the Federal Government's Computer Emergency Response Team (CERT-Bund).[192] In addition, there are initiatives in which companies exchange information on cyberattacks with each other or with government agencies.[193] However, small and medium-sized enterprises (SMEs) in particular

Box B 2-6

Example: Further training through gamification

The skills required to ward off cyberattacks must be regularly trained and updated. Providers of so-called cyber ranges offer such training. However, cyber ranges are often located on providers' premises, so cybersecurity professionals may be absent from the company for some time for training, thus increasing the training costs.

The Israeli company Cympire has developed a software-based cyberattack defence training environment that can replicate the customers' IT infrastructure. This means that training courses can be held regardless of location, and the time required can be reduced. In addition, the services offered by Cympire include innovative elements such as gamification, which are suitable for increasing experts' motivation to train.

often do not have the necessary resources to become involved in such initiatives.

Further measures for reducing information asymmetries in the market for cybersecurity products and services include certification, quality seals and minimum standards. Liability rules that make manufacturers responsible for security breaches in the event of damage are another possible way of dealing with information asymmetries. This creates incentives to already pay more attention to security during product development (security-by-design) in order to avoid compensation payments or expensive insurance policies.[194]

Germany has a national certification body for IT security, the BSI, where companies can apply for certification as an IT security service provider or for security or staff certification for certain products or services.[195] European-level implementation of both certifications and minimum standards of IT security started only recently and represents a very complex challenge. The EU Cybersecurity Act,[196] which came into force in June 2019, forms the foundation for certification. As a legal framework for market and product surveillance, the New Legislative Framework[197] serves as a basis for minimum standards of cybersecurity in products.

Insurance against cyber risks

Apart from investing in cybersecurity, companies can take out cyber-insurance policies to limit their costs from cyberattacks. Cyber insurances are often a combination of liability, business-interruption and data insurance covering both a company's own and third-party losses.[198] The benefits of cyber insurance can include:[199] compensation for business interruptions, reimbursement of data-recovery costs, assumption of third-party losses, payment of IT forensics, offer of legal advice for data breaches, payment for crisis communication, and call-centre costs.

The first cybersecurity policies in Germany came onto the market in 2011.[200] Accordingly, this is a relatively young insurance market. According to a survey conducted by Bitkom, 14 percent of industrial companies have taken out cyber insurance.[201] This share varies between small, medium-sized and large companies. Ten percent of companies with 10 to 99 employees have cyber-insurance. The share for companies with 100 to 499 employees is 23 percent and for companies with more than 500 employees 32 percent.

Reasons given for not taking out cyber insurance include the assessment of a low risk of exposure to cyberattacks, an unfavourable cost-benefit ratio, or excessive costs of risk assessment.[202]

Cybersecurity and the role of the state B 2-3

The state has various roles to play in maintaining cybersecurity. By funding R&D in cybersecurity, it helps create the necessary expertise for protection against cyberattacks. At the same time, it supports the role of cybersecurity as a driver of innovation, which can lead to new products and services. The state also provides reliable information on the threat situation and possible protective measures. Based on this information, companies can better manage their cybersecurity activities and protect their innovation activities. In addition, it is the responsibility of the state to ensure security in cyberspace through legal and regulatory measures and law enforcement.[203]

R&I funding for cybersecurity

With its research framework programme 'Self-Determined and Secure in the Digital World 2015–2020', the Federal Ministry of Education and

Research (BMBF) is funding research in IT security with about €180 million.[204] The main priorities of this research framework programme are high-tech technologies for IT security, secure and trustworthy ICT systems, application areas of IT security, and privacy and data protection. As part of the research framework programme, the three competence centres CISPA[205] (Saarbrücken), KASTEL[206] (Karlsruhe) and CRISP[207] (Darmstadt) have been funded by the BMBF since 2011. In December 2019, the CRISP competence centre led to the National Research Centre for Applied Cybersecurity ATHENE, which combines the work of more than 500 researchers from the Fraunhofer Institutes SIT and IGD, Darmstadt Technical University (TU) and Darmstadt University of Applied Sciences.[208]

The BMBF has also been funding the start-up incubator StartUpSecure with €2 million a year from 2017 to 2020. Partners are CISPA, CRISP, KASTEL and the Horst Görtz Institute for IT Security at the Ruhr University Bochum.[209] According to the BMBF, StartUpSecure has initiated ten start-ups so far.

The Central Office for Information Technology in the Security Sector (Zentrale Stelle für Informationstechnik im Sicherheitsbereich, ZITiS) conducts research and development in the fields of digital forensics, telecommunications surveillance, and crypto- and Big-Data analysis. The budget of ZITiS in 2019 was approximately €36 million. With the establishment of the Agency for Innovation in Cybersecurity (Agentur für Innovation in der Cybersicherheit, Cyber Agency), the Federal Government is also investing up to €402.5 million in new cybersecurity technologies up to 2023.[210] The Cyber Agency is to be founded as a limited liability company and will begin business operations this year.[211] The Cyber Agency aims to initiate and promote R&I projects in the field of cybersecurity and to accelerate procurement procedures.[212, 213] However, the Cyber Agency will be more closely linked to politics than the civil SprinD (cf. chapter A 1). This stronger connection with politics includes a transparency obligation vis-à-vis the German Bundestag, whose budget committee also decides on new lines of business or spin-offs, for example. Furthermore, in the selection of its projects the Cyber Agency is guided essentially by the needs of the two supervising ministries, the Federal Ministry of Defence (BMVg) and the Federal Ministry of the Interior, Building and Community (BMI).

Education and raising awareness

Since 2011, with the initiative 'IT Security in Commerce', the Federal Ministry of Economics and Energy (BMWi) has supported measures to sustainably improve awareness of IT security, especially among SMEs.[214] Among other things, the initiative offers IT security checks[215] and an IT security navigator[216] to help companies improve their data protection and provide an overview of the assistance on offer. Campaigns such as 'SME aware – Awareness in SMEs'[217] or the poster campaign 'IT security is NOT a game'[218] aim to raise companies' awareness of cybersecurity. Other programmes such as the BMBF's 'SME innovative: ICT'[219], the BMWi's 'go-digital' or 'SME 4.0 Competence Centres', and the KfW's 'ERP Digitalization and Innovation Loan' also contain elements aimed at promoting IT security.

The BSI performs a central task in the field of cybersecurity (cf. box B 2-1); its primary tasks include providing information and advice on all important IT security issues and supporting the implementation of appropriate measures.[220] As well as citizens[221] and companies,[222] the BSI also provides the federal and Länder administrations[223] with information and advice. It uses different formats such as annual situation reports, reports from the CERT-Bund[224] or Citizen CERT, and cooperation platforms such as the Alliance for Cybersecurity.[225]

In addition, the 'Germany Safe on the Net' (Deutschland sicher im Netz) initiative, an association under the auspices of the Federal Ministry of the Interior, provides a wide range of services for consumers and small businesses on how best to deal safely and confidently with the digital world.[226]

Measures for secure digital infrastructures

It is the task of the Federal Government – and its European partners – to ensure the security of digital infrastructures. The development of the new 5G standard in the mobile network has made policy makers and the public much more aware of digital infrastructure security. A recommendation by the European Commission aims to develop a toolbox defining both technical and non-technical criteria for assessing cyber risks for 5G networks and includes measures for making 5G networks secure.[227] Non-technical criteria for cyber risks can, for example, include the trustworthiness of producers or sources of supply and take into account their regulatory environment. Promoting diversity among producers and suppliers in the European internal market can help make networks more resilient.[228] Furthermore, multilateral projects such as the GAIA-X data cloud (cf. chapter A 1) aim to encourage the creation of secure digital infrastructures at the national and EU level.

B 2-4 Recommendations

The Federal Government recognized the importance of cybersecurity at an early stage and, among other things, launched R&D programmes and information measures to boost cybersecurity. In addition, the BSI was developed into the central institution for ensuring cybersecurity. However, the threat landscape for businesses is subject to constant change, so that implemented programmes for promoting cybersecurity need to be reviewed and, if necessary, adapted. From an innovation-policy perspective, it is particularly critical that companies delay innovation projects – or do not even begin projects in the first place – due to the danger of cyberattacks. Against this background, the Commission of Experts recommends the following:

Meet the demand for skilled workers and skills

- Teaching cybersecurity skills in vocational training and higher education should be further promoted to meet the growing demand for cybersecurity experts. Such moves should cover not only technical dimensions, but also deal with legal issues (cyber law) and ethical aspects (cyber ethics).

Ensure the security of digital infrastructures

- The approval of digital infrastructure components should be based on criteria that apply throughout the European single market. These criteria should take into account technical and non-technical aspects and apply equally to EU and non-EU suppliers. Corresponding initiatives by the European Commission, e.g. on the roll-out of 5G networks, should be supported.
- The Federal Government should push ahead with multilateral initiatives such as the GAIA-X data cloud in order to provide impetus for the establishment of secure digital infrastructures at the national and EU level.

Launch Cyber Agency quickly

- The Cyber Agency should begin operations quickly and practise demand-driven procurement to promote innovative projects that help protect Germany's technological sovereignty in cybersecurity. It is important here to constantly and openly follow new technological developments to be able to react flexibly to changing needs. An evaluation of the Cyber Agency should examine what stimuli it generates for R&I activities in cybersecurity.

Improve information on cyber threats

- It is particularly important to provide easily accessible information and advisory services for SMEs. The effectiveness of implemented programmes to promote cybersecurity in SMEs should be reviewed and adapted to the constantly changing threat situation.
- In order to improve the information available on the quality of cybersecurity products and services, initiatives should be supported which are aimed at developing minimum standards and certification systems, particularly at the European level.
- There is a need to consider whether the existing reporting obligations need to be extended in order to improve the information available on cyber risks and to deal more effectively with cyber threats.