acatech IMPULSE

Cybersecurity

Current Situation and Future Challenges

Claudia Eckert, Reinhard Ploss (Eds.)

acatech
NATIONAL ACADEMY OF
SCIENCE AND ENGINEERING

acatech IMPULSE

Cybersecurity

Current Situation and Future Challenges

Claudia Eckert, Reinhard Ploss (Eds.)

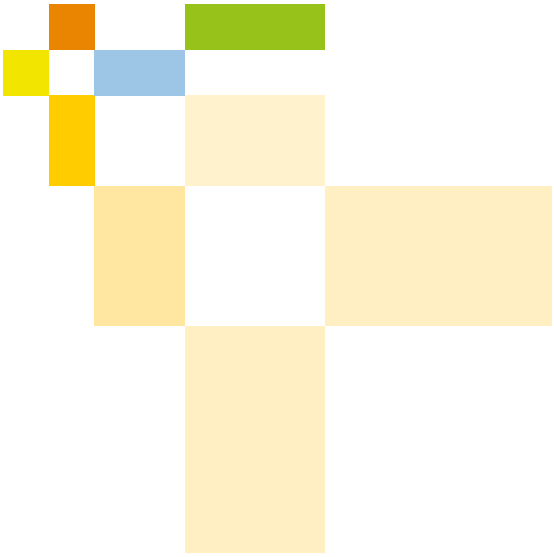
acatech
NATIONAL ACADEMY OF
SCIENCE AND ENGINEERING

The acatech IMPULSE series

This series comprises contributions to debates and thought-provoking papers on strategic engineering and technology policy issues. IMPULSE publications discuss policy options and are aimed at decision-makers in government, science and industry, as well as interested members of the general public. Responsibility for the contents of IMPULSE publications lies with their authors.

All previous acatech publications are available for download from www.acatech.de/publikationen.

Contents



Project

Editors

- Prof. Dr. Claudia Eckert, Fraunhofer Institute for Applied and Integrated Security (AISEC)/Technical University of Munich/acatech Executive Board member
- Dr.-Ing. Reinhard Ploss, acatech President

Project management

- Prof. Dr. Claudia Eckert, Fraunhofer Institute for Applied and Integrated Security (AISEC)/Technical University of Munich/acatech Executive Board member

Project group

- Carlos Arglebe, Siemens Healthineers AG
- Prof. Dr. Johannes Alfred Buchmann, TU Darmstadt/acatech
- Prof. Dr. Claudia Eckert, Fraunhofer Institute for Applied and Integrated Security (AISEC)/Technical University of Munich/acatech Executive Board member
- Alexander von Gernler, genua GmbH
- Prof. Dr. Jörn Müller-Quade, Karlsruhe Institute of Technology (KIT)/acatech
- Raphael Otto, Infineon Technologies AG
- Dr.-Ing. Reinhard Ploss, acatech President
- Prof. Dr. Michael Waidner, Fraunhofer Institute for Secure Information Technology (SIT)/TU Darmstadt/acatech

Further experts

- Prof. Dr. Christian Reuter, TU Darmstadt
- Prof. Dr. Haya Shulman, Fraunhofer Institute for Secure Information Technology (SIT)/Goethe University Frankfurt am Main
- Dr. Sven Herpig, Stiftung Neue Verantwortung e.V.
- Thomas Schauf, Deutsche Telekom AG
- Dr. Dirk Häger, Federal Office for Information Security (BSI)

Authors

- Prof. Dr. Claudia Eckert, Fraunhofer Institute for Applied and Integrated Security (AISEC)/Technical University of Munich/acatech Executive Board member
- Dr.-Ing. Reinhard Ploss, acatech President
- Simon Litsche, acatech Office
- Paul Grünke, acatech Office

Project duration

12/2021–11/2022

1 Introduction and rationale

Digitalisation is making steady progress in Germany. More and more tasks, whether in the private, professional or public sphere, are being performed digitally – a development that has been greatly accelerated by the Covid 19 pandemic. In principle, this should be considered as very positive, as digitalisation holds huge potential for society and the economy. At the same time, however, recent years have seen a significant increase in the levels of threat in cyberspace. Very different kinds of threat scenarios apply to companies, public and government institutions and to private individuals. Companies are increasingly becoming the focus for cybercriminals. The current geopolitical situation has also made it clear that politically motivated cyberattacks can also pose an increased potential threat. Disinformation is a central challenge as digitalisation proceeds and is an issue that cannot be fully addressed by cybersecurity measures. Instead, citizens must ask themselves whether they have the necessary skills to live in a digital world.

Disinformation in the context of new, changed forms of communication is a challenge all of its own which must be addressed separately.

Cybersecurity (see information box) is a necessary prerequisite for successful digitalisation. Cybersecurity also means building trust: systems which enable citizens, industry and policy makers to move around securely on the internet and securely digitalise their business and production processes have the potential to generate considerable added value for the future. An ambitious cybersecurity strategy must therefore be a cornerstone of Germany's digitalisation strategy. The need to strengthen digital sovereignty is closely intertwined with cybersecurity and together they are the foundation for self-determined and trusted activity in cyberspace. If systems and organisations are to be protected from unwanted influence by way, for instance, of data manipulation, extortion attacks (ransomware), information theft or lock-in effects due to monopolisation, it must be ensured that the digital technologies used in Germany are manageable and designed to have sufficient resilience. Ensuring manageability entails assessment capabilities for the risks associated with using technologies in relation to the intended use. In addition, alternatives must be available if it is to be possible to minimise risk autonomously. It is essential for a cybersecurity strategy to include measures to increase resilience and assessment capabilities as well as ways to actively respond to cyberattacks. A cybersecurity strategy cannot specifically address individual needs, but should set out concrete guidelines and also technological requirements without being tied to individual products.

Digital sovereignty (see information box) means having choices.[1] However, this must not be confused with an inward-looking, protectionist approach. In order to reduce technological dependencies and make them more manageable, core skills must likewise be systematically developed and fostered and the development of innovative, trustworthy key technologies driven forward. This includes capabilities along the entire value chain from research through product development to assessment, secure integration and reliable day-to-day operation of IT infrastructure. Further significant core skills include not only risk assessment and modern cryptography such as post-quantum cryptography or homomorphic encryption, but also digital identities, 6G network security, threat intelligence, trusted hardware and securely embedded operating software. Although Germany is already well positioned in some of these areas, it is essential to step up the pace of systematic further development. There is an urgent need for action with regard to software and IT services; in particular when it comes to cloud services, there are no significant European alternatives to the leading international hyperscalers such as Google, Amazon or Microsoft. Germany must press ahead to develop its digital sovereignty with partners who share the same democratic values. Joint European initiatives including the European Chips Act[2], sovereign data spaces[3] or also the revision of the eIDAS Regulation[4] and the new Cyber Resilience Act[5] are major milestones on the way to strengthening digital sovereignty.

A comprehensive cybersecurity strategy must provide answers to all these challenges if digitalisation is to be successfully driven forwards. In this regard, this IMPULSE provides food for thought which can be fleshed out into measures and strategies. This publication also highlights the need for a holistic approach to cybersecurity because it has an impact on every economic, political and societal entity and is deeply intertwined with related issues such as digital sovereignty. An additional intention is to show that successful implementation depends not only on political

1 | See acatech 2021.
2 | See European Commission 2022a.
3 | See European Commission 2020.
4 | See European Commission 2022b.
5 | See European Commission 2022c.

decision makers and companies treating it as a high priority, but also on societal change taking place. This IMPULSE provides an overview of these various issues while forthcoming publications will provide a more in-depth investigation of individual aspects which are only touched on here.

Section 2, Background, provides an overview of significant actors and various methods of attack and a definition of the term cybersecurity. The following section discusses the key challenges associated with increasing cybersecurity, including inadequate implementation of already known concepts. Furthermore, individual fields of relevant research are addressed – German cybersecurity research is already very well positioned – and barriers to research are identified. The significance of societal awareness of cybersecurity and hurdles to behavioural adjustments across society are also highlighted. This is followed by a consideration of the challenges facing policymakers. An analysis is then provided of how cybersecurity is limited by a lack of digital sovereignty. The concluding section 4, Areas of activity, indicates ways in which the tasks in hand can be addressed by the various actors. Experts from a variety of disciplines were interviewed in order to take a holistic approach to the issue with the interdisciplinary team consolidating the content in regular rounds of coordination.

Definition of cybersecurity

Cybersecurity means enabling the use of IT in a secure manner and thus forms the basis for a digitalised society. Cybersecurity has a technical core which meets the protection goals of information security. Fundamental protection goals are confidentiality, integrity and availability.[6] Authenticity is also becoming an increasingly significant goal because communication and interaction are increasingly taking place via digital channels. The true identity of a person with whom one comes into contact, for example via emails, logins or the authorship of updates, is thus becoming increasingly important. Cybersecurity also includes political, sociocultural, legal and economic aspects which are directly related to this technical core. The goal of cybersecurity is thus on the one hand to protect data and information and on the other hand also to protect all communication and information systems used to process and transmit these data and information and the physical systems surrounding them. Since complete protection or fully achieving the protection goals cannot be guaranteed, it is always necessary to weigh up how the goals can be achieved to a reasonable extent at reasonable cost. Society must debate what is meant by "reasonable" in a particular context.

6 | Confidentiality: maintaining authorised restrictions on access and publication of information, including appropriate means for protecting privacy and proprietary information. Integrity: providing protection from improper modification or destruction of information. Availability: ensuring timely and reliable access to and use of information. Further information security protection goals are, for example, data security, authenticity, non-repudiation, legitimacy and reliability.

2 Background

Despite efforts to enhance cybersecurity, there has been a significant increase in cyberattacks in recent years. In 2021, 86 per cent of German companies surveyed in a poll by industry association Bitkom[7] stated that cyberattacks had caused losses. In 2019, the figure was just 70 per cent. Total losses have doubled within these two years. According to a report from BKA[8], there were almost 150,000 cybercrime offences in Germany in 2021, an increase of more than 12 per cent over the previous year. The resultant losses came to around 223.5 billion euro. Cyberattacks are a growing problem internationally as well. Worldwide losses caused by cybercrime have been estimated at around six trillion US dollars in 2021, an amount exceeding the turnover of the global drugs trade, for example.

Cyberattackers can be roughly classified into four different categories, including in terms of motivation: cybercriminals, state-sponsored actors, "access as a service" (AaaS) companies and hacktivists. While the motivation of cybercriminals is usually financial, attacks by state-sponsored actors are usually based on the interests of the states for which they act. Possible objectives include obtaining information by espionage, preparing and carrying out sabotage operations, and manipulating election results or public opinion and perception. Legitimate AaaS companies offer offensive cyber services in a market that is only partially regulated and act in the interests of their clients.[9] Hacktivists, who carry out cyberattacks for ideological or political motives, as yet play only a minor role.[10] Attribution, that is the assignment of an attack operation to a dedicated attacker, is a problematic factor in this classification. This is because the boundaries between the individual actors cannot be drawn sharply and motives can

Figure 1: ENISA threat landscape 2021 – Prime threats (source: ENISA 2021)

7 | See Bitkom 2021.
8 | See BKA 2022.
9 | See Atlantic Council 2021a.
10 | See Security Intelligence 2019.

overlap. It is evident that cybercriminals, for example, regularly collaborate with state-sponsored actors, and state-sponsored groups sometimes act for financial motives.[11,12] Moreover, it is often not clear whether the attacks are for personal gain, to obtain foreign currency, or to disguise other motives.[13] In addition, there is the possibility of attackers making use of other groups' existing infrastructure to cover their tracks. AaaS companies further complicate attribution because their clients typically cannot be identified.[14]

Possible targets for cyberattacks are private individuals, governmental and public bodies as well as institutions and companies, with companies involved with critical infrastructure (CRITIS) being particular targets[15]. Attacks on them can have particularly serious consequences. For example, if hospitals are attacked, human life is put at direct risk.[16] But a shortage of supply of essential goods also has serious consequences, as the attack on the pipeline operator "Colonial Pipeline" showed. As a result of that attack, petrol supplies became scarce in parts of the USA, leading to panic buying and significant price rises.[17] Attribution of the attack is difficult because, although monetary interests were obviously being pursued, there was also the suspicion that it was in reality a state-sponsored smokescreen operation.[18]

Cybercriminals are becoming increasingly professional, as evidenced by the fact that their focus is shifting more and more to targets that promise high returns.[19] Their attacks are therefore currently being directed less against private individuals or small and medium-sized companies, and instead increasingly against larger companies and government bodies.[20,21] For example, Anhalt-Bitterfeld district authority in Germany was attacked and paralysed. The files on the district's IT infrastructure were stolen and encrypted in order to extort money. One of the results of the attack was that welfare benefits could no longer be paid. The district's losses came to some two million euro.[22]

The possibilities for carrying out cyberattacks are many and varied. Figure 1 provides an overview of the main threats identified by the European Union Agency for Cybersecurity (ENISA). Of the nine categories shown, ENISA currently views "ransomware" as the greatest threat.[23]

The methods by which cyberattacks are carried out and the threat scenarios change over time, so it is important for Germany to become resilient if it is to enjoy lasting protection. IT system infrastructure and architecture must consequently be set in such a way that it is capable of countering even new types of cyber attacks. All societal entities – companies, government bodies, private individuals and academia – must play their part. Recent geopolitical developments have made it clear that there are no national borders in cyberspace. For example, the beginning of the war in Ukraine saw a cyberattack on the KA-SAT satellite network, which led to the breakdown of the country's communication services. Remote servicing of wind turbines throughout Central Europe was also disrupted as collateral damage.[24] Germany must therefore take an international stance on the issue of cybersecurity and foster cross-border cooperation. In particular, this also includes becoming more involved in the process of international standardisation and driving forward the development of internationally applicable standards.

11 | See Intel471 2020.
12 | See Mandiant 2019.
13 | See Accenture 2020.
14 | See PwC 2020.
15 | See BBK for an overview of sectors which count as CRITIS.
16 | See Handelsblatt 2020.
17 | See Washington Post 2021.
18 | See Atlantic Council 2021b.
19 | See CrowdStrike 2021a.
20 | See Flashpoint 2021.
21 | See Europol 2019.
22 | See Süddeutsche Zeitung 2022.
23 | See ENISA 2021.
24 | See Tagesspiegel Background Cybersecurity 2022.

3 Challenges

3.1 Inadequate implementation of known concepts

Cybercriminals very often limit themselves to attacking simple targets. Insecurely configured IT systems (hardware and software), systems with weak controls or systems with unaddressed security vulnerabilities are therefore often the victims of a successful cyberattack. It is therefore important for comparatively simple "cyberhygiene" measures to be applied consistently, including, for example, keeping software updated. It is essential to understand and embed all security measures as a process. Since cybersecurity is not static, all security measures have to be continuously reviewed and implemented.

In the long term, cybersecurity will have to be more consistently taken into account right from the system design stage. Concepts such as "security by design" already exist but have rarely been implemented to date. A new concept for securely designing multi-user systems is known as "zero trust architecture" (see information box and Figure 2). However, small and medium-sized companies and local authorities in particular often lack the resources and knowledge to implement this concept by themselves. But even federal government agencies and many relatively large companies rarely implement "zero trust architecture" and as a result the concept has to date barely been used in Germany.

To avoid being targeted by cybercriminals, it is usually sufficient if the effort involved exceeds the potential benefit of an attack. However, regardless of the measures taken, it is impossible to completely secure against cyberattacks. The goal should therefore be to balance the cost and level of protection against the potential loss and to design the package of measures accordingly. In addition, measures to increase resilience should also be taken. Therefore, in addition to appropriate protective measures, there is also a need for incident response plans and expertise so that attacks can be withstood and normal operation efficiently resumed after an attack. Such emergency plans are of particular relevance to institutions and companies involved with critical infrastructure (CRITIS) since in such cases failure has enormous potential for damage to society as a whole. The plans should, however, not be limited to CRITIS since many institutions and companies which are currently below the CRITIS threshold are essential to subsystems and significant losses would occur, especially in the event of prolonged downtime.

"Zero trust architecture"

"Zero trust" describes a concept for building a cybersecurity strategy that differs significantly from the approach commonly used to date. Until now, it has been conventional practice to define a company context within which all participants are implicitly trusted ("trusted network") and to protect this context, this domain, externally.

"Zero trust" abandons the idea of an implicitly trusted domain and instead takes a data-centric approach. Instead of trusting every user active in the domain (for example because access is made via an employee's terminal), all users wishing to access corporate data must authenticate themselves ("never trust, always verify"). A second step involves validating the security of the terminal used. Authentication and validation requirements can here be configured dynamically and depending on the sensitivity of the data to be accessed. The principle of "least-privileged access", which grants each user only as many rights and access options as are necessary for them to carry out their tasks, additionally applies here. In this context, trust in the tools and systems enabling this process is crucial to the success of "zero trust architecture".[25] See Figure 2 for a graphical representation of zero trust architecture.

3.2 Research needs and research funding

There is constant, dynamic competition between cyber attackers and defenders. The task of research is not only to further develop methods to assess the need for protection, but also to develop new architectures, security solutions, as well as tools and methods to make existing systems more resilient to attacks. At the same time, ways must be found to simplify complex procedures so that as many users as possible can benefit from and use them with confidence. Although Germany is a leader in many research fields in cybersecurity, research must continue to be consistently funded if this leading position is to be maintained.

Central themes of research in this area currently include not only encryption methods and methods for quantifying risks, methods for automated and continuous assessment of system resilience against attacks, and concepts for implementing the zero trust

25 | See CrowdStrike 2021b.

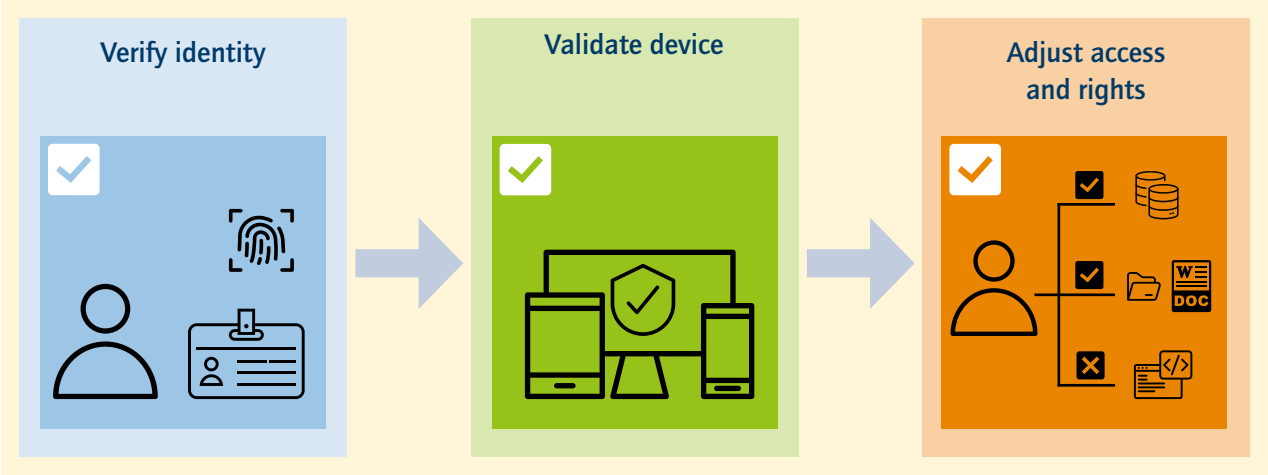


Figure 2: Zero trust architecture (source: own presentation using Noun icons)

principle and automatically verifying and updating it, but also new methods and tools for assessing the trustworthiness of AI processes and machine learning algorithms. The use of quantum computers could result in existing encryption methods becoming insecure. This necessitates a shift to new methods and requires new procedures, such as post-quantum cryptography, and their seamless integration into existing system landscapes. Further important fields of research include the further development of methods for designing but in particular for securely operating systems over their entire lifetimes. Also crucial is the further development of practically applicable test procedures capable of carrying out automated testing and verification of complex software and hardware artefacts – including for correctness as well as the absence of known vulnerabilities. Germany's research landscape is well positioned in these areas, but there is a lack of efficient transfer of results into practical applications.

A central stumbling block for applied IT security research remains the still uncertain legal situation. Testing systems for vulnerabilities requires IT security researchers to use the same methods commonly used in cyberattacks. Since current IT criminal law makes no distinction according to an attacker's intention, researchers are therefore at risk of criminal liability. This circumstance means that it tends to be cybercriminals rather than researchers who uncover vulnerabilities, as a result of which they are often exploited rather than remediated. Policy makers are called upon to create a clear framework for research and to adapt relevant legislation in such a way that research into IT security is possible in Germany without the risk of legal consequences.

Another barrier to research is inadequate availability of data. On the one hand, not all attacks are registered, as those responsible usually try to cover their tracks. On the other hand, attacks are often not reported or made accessible to security researchers, for example out of fear of reputational damage to the affected company or for data protection reasons. There is thus a need to develop ways and procedures for the relevant data to be investigated by suitable individuals or authorities for analysis purposes while respecting data protection guidelines.

3.3 Digital skills in society

Raising society's overall level of cybersecurity means firmly embedding the issue across society. This will be founded on behavioural adjustments which will only be achievable if simple migration paths, appropriate alternative offerings, and uncomplicated and convenient cybersecurity solutions are available. It is crucial for the technologies to be understandable and easy to use for users, especially private individuals. There must be an emphasis on usability because security measures that are too complex are rarely used, which means that systems often remain insecure and vulnerable. Security should therefore ideally be implemented by default, that is without further intervention, in products and services for private users. Companies and researchers, supported by government funding and incentives, are here called upon to develop solutions which meet these requirements.

The central tasks for citizens is to secure their own terminals and private infrastructure, for example in smart home scenarios. Since they cannot directly influence the security of the installed applications, the security of the cloud platforms which are usually integrated, or the security of the apps and web services, government is called upon to define an appropriate regulatory framework. This includes, for example, secure internet infrastructure which wards off as many cyberthreats as possible. An easy-

to-use, reliable method for securing identities in digital space is also important. Balancing the security and risk of individual components and different technologies is something else which is largely impossible for private individuals to do. End users must be able to obtain information about device security and the duration of support by software updates simply and transparently. Security assessments of individual software and hardware products and of digital services (such as software-as-a-service), for example through official certification schemes or through voluntary or mandatory manufacturer's declarations, can be of assistance here. However, if they are to have the desired effect, such official certificates must be issued by a suitable and appropriately equipped independent institution. Manufacturer's declarations must likewise be verified, at least on a random basis, by an independent institution and should be backed up by policy guidelines ensuring that making fraudulent declarations does not pay off. In this way, aspects of cybersecurity can have a greater influence on purchasing decisions for software and hardware products and for digital services and become a differentiating factor among competing providers. As a result, security will come to have financial value for manufacturers too. A step in this direction has already been taken through the certification and labelling of technologies with the German Federal Office for Information Security (BSI) security mark, although this has so far been limited to a few product groups.[26]

Not only ease of application but also widespread public awareness of the relevant knowledge are essential for bringing about behavioural changes. While awareness of the issue of cybersecurity has increased significantly in recent times, in-depth IT skills are often still lacking. It is critical to enable the public to become more cybersecure, for instance by increasing educational/training provision which should as far as possible reach every level of society starting with schoolchildren and students and extending to working people at every skill level. The goal should be for safe handling of digital technologies and their risks to become as natural as dealing with dangers in road traffic. A central plank is consistent implementation of "cyberhygiene" measures which should be familiar to all citizens. Greater digital literacy helps people to recognise increasing, anti-democratic disinformation campaigns and to be able to evaluate them appropriately. In addition, educational/training provision must also be geared toward training more cybersecurity specialists.

3.4 Challenges for policy makers

Policy makers have a crucial role to play in increasing cybersecurity in Germany. It is the responsibility of policymakers not only to create an appropriate legislative framework but also to provide education/training. The cybersecurity strategy in its third version[27] and the cybersecurity agenda[28] presented in preparation for the fourth version of the strategy show that policymakers are intensively addressing the issue of cybersecurity in Germany. Nevertheless, there are many aspects of cybersecurity which have not yet been appropriately considered or implemented. For example, Germany has a very diverse range of agencies with responsibilities in cybersecurity.[29] While this is in principle a positive thing, there is a need for fundamental consolidation so that responsibilities are assigned more clearly and communication between the individual agencies is improved. Despite the numerous institutions at federal and state level, there are, for example, currently no regulations governing how to implement active cyber defence. Such regulations are not to be confused with counterattacks or "hackbacks" in the wake of a cyberattack. Since government institutions are also users of technology, they should endeavour to play a pioneering role in increasing cybersecurity and adopt innovative approaches and technologies to serve as a good example for other users. Government should to this end promote secure open-source solutions for administration and find ways to run them institutionally, for example through foundations. These solutions can then in turn be provided to business and community users as inexpensive and secure alternatives. Other countries are much further along in this respect.

Singapore's strategy, for example, is based on the government consistently advancing its sovereign responsibilities while engaging society by identifying opportunities for citizens to see how each and every individual can add value to Singapore's cybersecurity.[30] The USA has set out very specific and ambitious measures for how cybersecurity is to be implemented by all government agencies and has also backed them up with clear responsibilities, processes and deadlines. For example, all US federal agencies must implement a "zero trust architecture" by 2024.[31]

This kind of approach would also make sense for Germany, as it would significantly raise the general level of security. It is important here for the specified architectures and measures to be not

26 | See BSI.
27 | See BMI 2021.
28 | See BMI 2022.
29 | See Stiftung Neue Verantwortung 2022.
30 | See Cyber Security Agency of Singapore 2021.
31 | See The White House 2021.

only as specific and ambitious as possible, but also implementable using current technology. Regular reviews and adjustments of these specifications should therefore be scheduled. In addition to government bodies, these specifications should also apply to the mainly private-sector operators of critical infrastructure. Support for companies in implementing the guidelines is also conceivable, since a high level of security in critical infrastructure should be a fundamental goal of government action. Public institutions at municipal level could potentially also be included. Consistent implementation would entail requiring that only those suppliers who can meet these specifications are considered for public calls for proposals. This would increase the supply of appropriate products and services which would in turn lead to falling costs and open up more inexpensive access to products and services with these high security standards for an increasing number of users. While the cybersecurity agenda calls for untrusted manufacturers to be excluded from infrastructure expansion, this will only be possible if appropriate alternative offerings are available.

3.5 The challenge of digital sovereignty

Digital sovereignty (see information box) must not be equated with inward-looking self-sufficiency. When it comes to digital sovereignty, the requirement must be to have at least one good alternative so that the tools and systems used to ensure cybersecurity and enable this process can be trusted. This requires strengthening the country's own innovation ecosystem together with partners and shaping international norms and standards in line with European ideas. Digital sovereignty also includes consciously entering into and diversifying dependency relationships on those issues in which a separate European innovation ecosystem is not (yet) possible.

In the context of the Ukraine conflict, the Federal Office for Information Security (BSI) considers Kaspersky antivirus software, which originates from Russia, untrustworthy.[32] This underlines the importance of having various alternative offerings because it cannot be assumed that partner countries will remain permanently political stable at all times. Since there are sufficient alternatives available in this antivirus software market segment, the BSI's assessment has not had any far-reaching consequences. In other areas, however, especially in that of IT services, software and chip production, hardly any alternatives are available, which is why the creation of alternative offerings should be a key objective. If, once all factors have been weighed up, it is concluded that the level of security is not sufficient and a more secure alternative should be selected, alternatives must first be available at all levels (see Figure 3). At the very least, the underlying know-how must be available. The focus should be on central key technologies or fundamental basic components.[34] This opens up the possibility, for example, of having hardware manufactured according to your own particular specifications in order to increase the level of security, for example by preventing the installation of hardware backdoors. In addition, this can enhance assessment capabilities, that is the understanding of the system effects of individual building blocks. This is because increasingly larger and more complex systems and the resulting cascading effects make it more difficult to assess the security of the systems under consideration. Moreover, software in particular is often not developed by a single manufacturer but, as with physical products, entire supply chains or networks are involved in its creation. A security evaluation therefore always implicitly refers to the intermediate products it contains. However, security aspects are often not the main focus during development. Furthermore, proprietary software is often opaque, which further complicates assessment. There is also a lack of control options for preventing possible manipulation of the software. But even open-source software with visible source code is not automatically secure. This is because due to the high

Definition of digital sovereignty

Digital sovereignty means that people, companies and policy makers are capable of independently deciding how and with what objectives digital transformation should be shaped. This is a matter of both competitiveness and political self-determination. European-style digital sovereignty aims to give all entities freedom of choice in digitalisation and must follow European concepts of law and values, be open to the world, and foster fair competition. acatech has developed a layered model with eight levels which build on one another in order to map the complexity of digital sovereignty.[33]

32 | See BSI 2022.
33 | See acatech 2021.
34 | Basic components mean in this connection all the fundamental elements required for IT systems and cyber-physical systems to function, such as chip and semiconductor technology as well as manufacturing processes, operating systems and firmware for internet-of-things (IoT) devices, and the associated management software.

complexity of the source code of current software products, a well-founded security assessment can no longer be made manually, even by experts, but only through comprehensive analyses using appropriate tools. Another problem in this context is that open-source solutions are currently often developed by individuals or small groups. Sovereignty should be fostered by setting up (international) institutional organisations to ensure greater transparency, trustworthiness and independence.

In the absence of alternative offerings, the easiest and most cost-effective option for many users is to rely on the services of hyperscalers such as Microsoft, Amazon or Google. Their offerings are generally well secured against cyberattacks and simple to use. However, compliance with the protection goal of confidentiality can be problematic here, as there is no way to check how secure one's own data is with a hosting provider. Customers simply have to trust the supplier. This in particular involves risks because all hyperscalers are currently located outside Europe and thus also subject to their respective local legislation. The PATRIOT Act and the CLOUD Act, for example, grant US authorities far-reaching powers to access data hosted by cloud providers.

There are various approaches to creating European alternatives, the key factor being to lay the foundations for a thriving and innovative ecosystem. In central, already occupied technology fields, at least enough know-how should be developed to enable sufficient assessment capabilities. However, it is still more important to develop sufficient innovative capacity to be able to identify and play a part in shaping future trends at an early stage. The goal must always be to develop products and services that are competitive with leading international offerings. Alternative offerings could be developed, for example, by fostering innovation, start-ups or open-source technologies. However, this can only be achieved through joint action by partners from business and politics at the European level.

A further possibility for exerting influence is through international bodies which set norms and standards. One critical factor to note is that Chinese companies have recently become more involved here, while European engagement has stagnated or even declined. The cause for this would appear to be a lack of incentives for researchers and companies to engage in time-consuming and labour-intensive standardisation processes. However, even if Europe succeeds in making a stronger mark on international standards again, technologies from countries that do not conform to European values will still have to be used. Solutions must therefore be found as to how such technologies can be successfully used without a critical impact on system security.

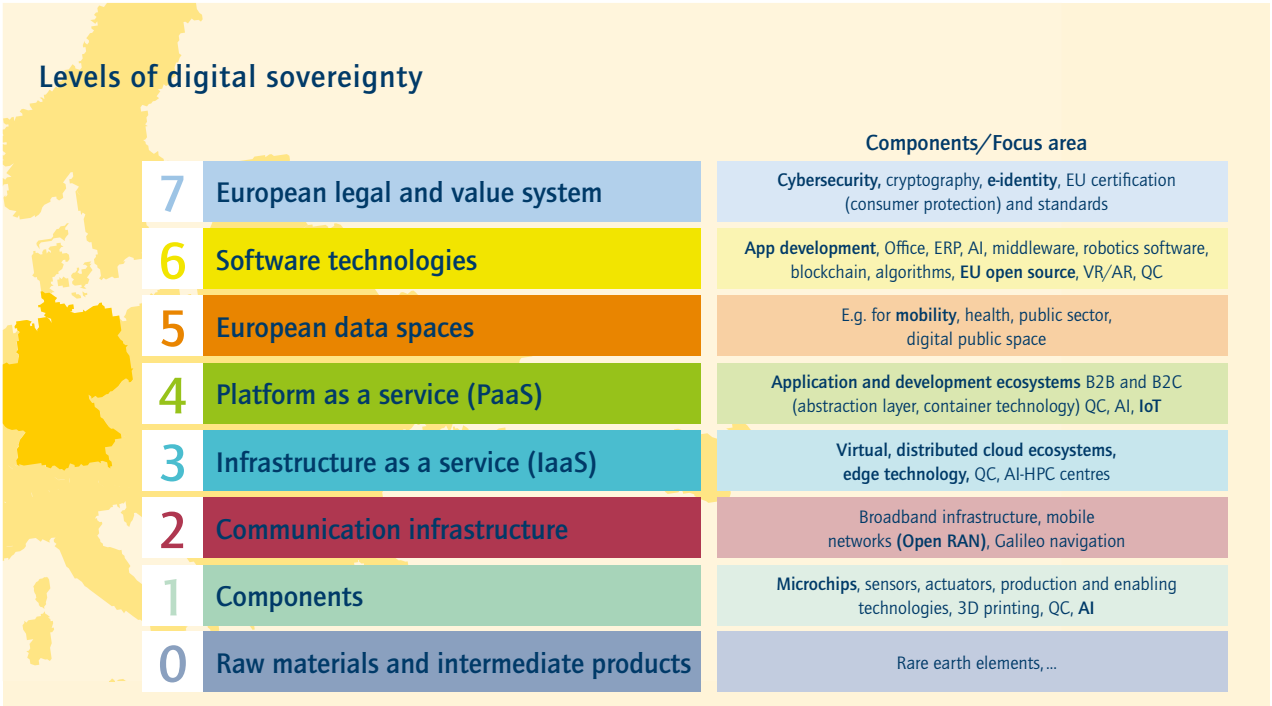


Figure 3: Levels of digital sovereignty according to acatech's layer model (source: own presentation)

4 Areas of activity

Constant and consistent further development of cybersecurity is necessary to provide Germany with lasting protection from attacks from virtual space. This is closely linked to the strategic goal of extending digital sovereignty. The two goals are interdependent: in the absence of adequate cybersecurity, digital sovereignty cannot be ensured and the more digital sovereignty prevails, the greater is the achievable level of cybersecurity. The cybersecurity agenda published by the Federal Ministry of the Interior and Community (BMI) in July 2022 shows that policymakers have recognised the urgency of the issue.[35] It can be viewed as a further development of 2021's cybersecurity strategy and already indicates the path the amendment to the cybersecurity strategy planned for 2023 will take. Many measures and approaches of the cybersecurity agenda are going in the right direction, but have not yet been sufficiently fleshed out. The new cybersecurity strategy should be guided by the concrete and ambitious set of measures recently published in the United States.[36] One critical factor is the obvious conflict of interest in the cybersecurity agenda between increasing cybersecurity and enhancing criminal prosecution capabilities. For instance, there is talk of "vulnerability management" which might suggest that not all known vulnerabilities are to be remediated. There is additionally talk for example of "expanding" and "modernising investigative capabilities and tools" and tighter control of content on social media. While these measures are useful in their own right, they do not serve to enhance cybersecurity and so should not be part of the cybersecurity debate.

Various areas of activity for increasing cybersecurity are addressed below and set against the appropriate points in the cybersecurity agenda. The stated areas of activity do not amount to a concrete set of measures but are intended to encourage more detailed examination in greater depth.

Areas of activity for political decision makers

It is the responsibility of policy makers to create a legislative framework to drive Germany's cybersecurity forward. At the same time, government bodies such as ministries are also users of technology. These governmental bodies should endeavour to play a pioneering role with the goal of encouraging offerings in this area through government demand for more secure technologies, such that the market for them grows over time and they become more readily available.

- **Ambitious cybersecurity strategy:** Germany needs a comprehensive and ambitious cybersecurity strategy. This must not stand alone, but must be embedded in a comprehensive and coherent digitalisation strategy. Cybersecurity is not an end in itself but instead forms the basis for secure and trustworthy digitalisation. While the cybersecurity strategy cannot specifically address individual needs, it should set out concrete guidelines and also technological requirements without being tied to individual products.
- **Implementation of zero trust:** The cybersecurity agenda identifies key principles, such as for instance security "by design" and "by default" in federal government. Even more important, however, is consistent and ambitious implementation of the zero trust principle, as is also being driven forward by the US government. The cybersecurity strategy scheduled for early 2023 must therefore include a concrete, ambitious timeline and action plan for public sector institutions.
- **Secure infrastructure:** It is the responsibility of policy makers to drive forward the development of properly functioning, maximally secure infrastructure. For example, the government can work with internet service providers to enhance national internet infrastructure security by implementing the DNSSEC protocol (Domain Name System Security Extension) in all local internet domains, which will mean that many attacks are warded off before they even reach end users.
- **Consolidation of agency architecture:** Currently, there are 75 different agencies, committees and initiatives with cybersecurity responsibilities at the federal level alone.[37] The cybersecurity agenda's approach of upgrading individual institutions is therefore a step in the right direction. A comprehensive consolidation of these structures is essential in order to allocate responsibilities more clearly and improve coordination between the individual institutions. Individual agencies should be assigned a clear mission and definite responsibilities. In particular, the experts surveyed are in favour of upgrading the Federal Office for Information Security (BSI) and detaching it from the Federal Ministry of the Interior and Community (BMI) to avoid conflicts of interest.
- **Modernisation and standardisation of official infrastructure:** Modernisation of official infrastructure should also be part of the above-mentioned timeline and action plan. In this connection, efforts should be made to standardise the soft-

35 | BMI 2022.
36 | The White House 2021.
37 | See Stiftung Neue Verantwortung 2022.

ware and hardware solutions used. Among other things, this facilitates data exchange between the various state bodies. In addition, the use of standardised technologies increases security by allowing resources to be pooled for more comprehensive security reviews. Proposals from the cybersecurity agenda, such as for instance the introduction of a central videoconferencing system or investment in post-quantum cryptography and the further development of information security management, are supported by the experts surveyed.

- **Guideline function for official IT infrastructure:** In the course of modernising and standardising official infrastructure, the aim should be to set up a system that can be used as a guideline for users in other settings. The emphasis must be on a high level of usability so that companies and private individuals are able to follow such guidelines. One example is the introduction of a uniform, secure and easy-to-use procedure for verifying digital identities while maintaining existing data protection guidelines.
- **Certification of critical technologies:** Again in the course of modernising and standardising official infrastructure, relevant technologies (in particular critical components) should be comprehensively tested and certified in terms of their safety, integrity and the possibility of political influence. The same also applies to intermediate products and supply chains. Technologies which meet the stringent requirements can be included in a permit list which must be updated regularly and revised as necessary. On this basis, approval and recommendation can be provided for all administrative establishments. This approach helps increase overall cybersecurity because companies and private individuals can also follow the permit list, so in turn creating an incentive for manufacturers and developers to meet the permit list criteria. This approach extends the proposal in the cybersecurity agenda of developing the BSI's auditing capabilities with regard to the trustworthiness of manufacturers, because in the proposal the focus is limited to operators of critical infrastructure.
- **Open source for government:** The federal government should drive ahead with the development of secure, verified open-source solutions for government bodies because this will create demand for these open-source solutions and so foster their development. Since the contributors to open-source technologies are not usually identified, it must be ensured that no hidden malicious code is included (see Area of activity – digital sovereignty). After appropriate in-depth testing, these solutions can also be included in the permit list, so making them available as an inexpensive option for every area of Germany's administration. The preliminary work at the federal level makes it easier for state, local, and municipal governments to implement complex cybersecurity procedures without driving up their costs. The cybersecurity agenda does not take a position on this significant issue, so some catching up will have to be done during the formulation of the cybersecurity strategy.
- **Active defence:** Active defence is vitally significant in the event of massive cyberattacks. It is important to distinguish this approach from hackbacks. In the upcoming cybersecurity strategy, attention should be paid to clear communication and consistent and clear use of terminology. In order to be able to respond quickly in an emergency, the still numerous existing hurdles on the way to implementing active cyberdefence must be overcome in the near future. As yet unresolved are issues around responsibilities, how to ensure an appropriately short response time while appropriately balancing costs and benefits, and how to deal with any collateral damage.

Areas of activity – companies

On the one hand, companies are users of digital technologies, but on the other they also develop (intermediate) products and services of many different kinds. It is important for companies to understand the significance of cybersecurity and act accordingly. Numerous companies have already recognised this and implemented appropriate measures. Companies that are part of critical infrastructure occupy a special position due to their importance for the functioning of society. Accordingly, the level of security to be achieved must be (even) higher here.

- **Usability:** For all digital (intermediate) products and services, the goal must be to focus on user-friendly cybersecurity from the outset and to understand it as part of the concept. This is because only easy-to-use cybersecurity solutions will be consistently used and only if security is taken into account from the outset can complex measures (such as security by design) be thoroughly implemented. Growing user awareness and minimum government standards will also give rise to a competitive economic advantage.
- **Supply chain security for software products:** Software manufacturers must ensure that the intermediate products contained in their software are secure. This also includes an analysis of the political setting in which an intermediate product has been developed.
- **Boosting resilience:** The Covid-19-pandemic has shown how vulnerable our complex economic system is. It is thus important to focus more strongly on resilience[38], in particular for companies which are part of critical infrastructure. In a cyber-

38 | See acatech 2022.

security context, this specifically means not only investing in measures to increase security, but also preparing plans and measures in the event of a successful attack. These include for instance capabilities to maintain emergency operation and rapidly restore normal operation ("graceful degradation"). Where possible and appropriate, analogue protection mechanisms should be implemented. For instance, a mechanical pressure relief valve can prevent a gas pipeline from exploding, even if the supplier's entire IT system has been taken over by hackers.

Areas of activity – research

The dynamic evolution of cybersecurity is leading to a contest between attackers and defenders with the defenders always trying to remain one step ahead. Research has the central task in this contest of continually developing new methods and tools which help to increase security and ease of use of secure solutions.

- **Research funding:** The research funding proposed in the cybersecurity agenda is a central pillar for enhancing both cybersecurity and digital sovereignty. In addition to monetary investment in research projects, it is important to establish the right regulatory framework. Funding should primarily be focused on research in key technologies, such as for instance risk evaluation, assessment capabilities, cryptography, digital identities, network security, threat intelligence, trusted hardware, quantification and engineering of secure software. The Federal government's cybersecurity strategy must specifically identify these and other relevant fields of research and drive them forward.
- **Transfer and requirement engineering:** If research results are to help increase cybersecurity, transfer to application is central. Therefore, migration paths should be considered right from the beginning of research projects. Applied research should also be geared to the needs of future users and ensure that development does not ignore existing needs.
- **(Automated) testing and verification procedures:** A fundamental building block for increasing cybersecurity is to further develop methods and practically applicable testing and verification procedures for automated testing of complex software and hardware artefacts for correctness as well as the absence of known vulnerabilities. Such methods will assist with creating permit lists of tested hardware and software and verifying the security of open-source solutions.
- **Data availability:** Researchers must have access to data from structured cyberattacks on companies to learn from. While such data are already available to the Federal Office for Information Security (BSI), they cannot currently be used because this would require a new interpretation of the General Data Protection Regulation (GDPR). One way of enabling the use of the available data would be to create a secure data space for verified researchers. A confidentiality agreement, for example, could protect the identity of the companies involved. The cybersecurity strategy must find an appropriate solution to this problem.
- **Clear definition of scope for activity:** Legal certainty for research must be created. For example, researchers seeking out vulnerabilities must be protected by legislation. At present, such activities can still be classed as hacking and are therefore punishable under criminal law. The cybersecurity agenda unfortunately takes no account of this point.

Areas of activity – society

Achieving long-term sustainable change will require a lasting change in society's awareness of cybersecurity. Education is key here. Education is primarily provided by the state, but social institutions can also play a part. However, it is just as important for society to be assisted by the provision of easy-to-use tools. The focus of the cybersecurity agenda, however, is on combating criminal content rather than empowering society, so the following points should receive attention in the next version of the cybersecurity strategy:

- **Usability and interoperability:** One important factor in assisting private users to increase their cybersecurity is the availability of easy-to-use security solutions. Many methods for increasing cybersecurity are still too complex for private users to implement and this is where researchers and companies are called upon to develop simpler options. Ideally, cybersecurity should be present by default and not have to be configured after the fact. Messaging services for example, unlike emails, offer such security but their business models are based on user lock-in. To remedy this situation, the government or the European Union must require interoperability.
- **Digital skills:** In addition to media skills, digitally skilled citizens need a basic understanding of digital technologies, processes and procedures. The curriculum for school pupils of all ages should focus much more on digital skills in order to develop and extend this understanding. There is also a need for appropriate, low-threshold continuing education programmes for working people. The goal must be for sovereign action in the digital world to become a matter of course.
- **Targeted disinformation:** Targeted disinformation is a major problem for democratic states. The workings of social media algorithms contribute to the formation of information bubbles. Freely available technologies for creating realistic deep

fakes further exacerbate the problem. A uniform, secure and easy-to-use procedure for verifying digital identities is important for countering targeted disinformation campaigns and deep fakes. This will make it easier for citizens to determine the authenticity of the author while at the same time authorities will be able to identify the creators of criminal content and take appropriate action. Citizens will additionally need to put their digital skills into practice. At the European level, social media platforms must be required to delete fake news while not censoring.

- **Certification schemes:** Official certification schemes or manufacturer labels, either voluntary or mandatory, will help private individuals to assess the security of products, applications or services more quickly and easily. In this way, security can become a competitive advantage for companies while simultaneously boosting confidence in technology. BSI has already taken the first steps in this direction with the introduction of the IT security label, but it is currently limited to too few product groups to have a major impact.

Areas of activity – digital sovereignty

Without digital sovereignty there can be no cybersecurity. At the same time, a high level of cybersecurity also leads to greater digital sovereignty. The following measures will help to advance both objectives in parallel. This can only be achieved through joint action by partners from business and politics at the European level.

- **Alternative offerings:** Both hardware and software solutions are often offered for sale within oligopolistic market structures. As a result, it is rarely possible for users to choose an alternative if, for example, there are security concerns about one particular solution, and this explains the importance of creating secure alternative offerings. The cybersecurity agenda also seeks to ensure that untrusted manufacturers are excluded from developing the infrastructure needed for advancing digitalisation. Crucially, however, appropriate alternative offerings must be available. Enabling the emergence of such alternatives requires a combination of various approaches, such as for example greater support for open-source projects, better funding for start-ups and European chip production. This will also ensure better hardware availability. In addition, public procurement law should be adapted in such a way that young European companies and open-source approaches are given preference in tenders. Government demand, which exists in any event, can in this way be put to efficient use. At the same time, (applied) research projects must be initiated and driven forward. Joint European initiatives such as for instance the Chip Act,[39] the establishment of sovereign data spaces,[40] the revision of the eIDAS Regulation[41] or indeed the new Cyber Resilience Act[42] are good approaches to strengthening digital sovereignty.
- **Skills in key technologies:** Closely linked with the creation of alternative offerings is the development of skills in key technologies,[43] because, in the absence of the relevant know-how, it will not be possible to develop alternative offerings. In addition, assessment capabilities are the foundation for evaluating the security of technologies. Appropriate know-how can in turn be fed into international standardisation committees in order to influence the future direction in which technologies will develop.
- **Trusted open-source software:** Open-source solutions can help create secure alternatives thanks to their great innovation potential. However, if this is to happen, open-source software must be extensively tested, kept updated and maintained, and its security (including supply chains) verified. Concepts for systematic and largely automated integrity checks could be helpful here. Planning certainty is crucial for both operation of and demand for open-source software. It is important to involve the international open-source community and to keep the community alive so that source code can be permanently updated and security vulnerabilities can be remediated as soon as they are identified. Open source must be trustworthy in the long term in order to be efficient and usable in all areas. It is accordingly important for development not only to be in the hands of individuals or small groups but wherever possible for institutions (such as foundations) to take over further development. These bodies can then make a preselection from the profusion of open-source offerings and provide this selection with an increased level of security through extensive testing and by offering to maintain the software. Verified curators, for example paid by public-private partnerships or foundations, can provide testing and maintenance. Such bodies should also take over operation of the open-source solutions.

39 | See European Commission 2022a.
40 | See European Commission 2020.
41 | See European Commission 2022b.
42 | See European Commission 2022c.
43 | These include risk evaluation, cryptography, digital identities, network security, threat intelligence, and trusted hardware.

References

acatech 2022
acatech (Ed.): *Security, Resilience and Sustainability* (acatech IMPULSE), Munich 2022.

acatech 2021
acatech (Ed.): *Digital Sovereignty. Status Quo and Perspectives* (acatech IMPULSE), Munich 2021.

Accenture 2020
Accenture (Ed.): *2020 Cyber Threatscape Report*, 2020. URL: www.accenture.com/_acnmedia/PDF-136/Accenture-2020-Cyber-Threatscape-Full-Report.pdf [Retrieved: 27.09.2022].

Atlantic Council 2021a
Atlantic Council (Ed.): *Countering Cyber Proliferation – Zeroing in on Access-as-a-Service*, 2021. URL: www.atlanticcouncil.org/wp-content/uploads/2021/03/Offensive-Cyber-Capabilities-Proliferation-Report-1.pdf [Retrieved: 27.09.2022].

Atlantic Council 2021b
Atlantic Council (Ed.): *Assessing Russia's Role and Responsibility in the Colonial Pipeline Attack*, 2021. URL: www.atlanticcouncil.org/blogs/new-atlanticist/assessing-russias-role-and-responsibility-in-the-colonial-pipeline-attack/ [Retrieved: 27.09.2022].

BBK
Federal Office of Civil Protection and Disaster Assistance: *Sektoren und Branchen KRITIS*. URL: www.bbk.bund.de/DE/Themen/Kritische-Infrastrukturen/Sektoren-Branchen/sektoren-branchen_node.htm [Retrieved: 27.09.2022].

Bitkom 2021
Bitkom (Ed.): *Wirtschaftsschutz 2021*, 2021. URL: www.bitkom.org/sites/default/files/2021-08/bitkom-slides-wirtschaftsschutz-cybercrime-05-08-2021.pdf [Retrieved: 27.09.2022].

BKA 2022
Federal Criminal Police Office: *Cybercrime. Bundeslagebild 2021*, Wiesbaden 2022.

BMI 2022
Federal Ministry of the Interior and Community: *Cybersicherheitsagenda des Bundesministeriums des Innern und für Heimat. Ziele und Maßnahmen für die 20. Legislaturperiode*, Berlin 2022. URL: www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/themen/sicherheit/cybersicherheitsagenda-20-legislatur.pdf?__blob=publicationFile&v=4 [Retrieved: 27.09.2022].

BMI 2021
Federal Ministry of the Interior, Building and Community: *Cybersicherheitsstrategie für Deutschland 2021*, Berlin 2021. URL: www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/2021/09/cybersicherheitsstrategie-2021.pdf;jsessionid=9AA3AE7DC92A8FF6770FDE6EC5DCEB35.2_cid332?__blob=publicationFile&v=2 [Retrieved: 27.09.2022].

BSI 2022
Federal Office for Information Security: "BSI warnt vor dem Einsatz von Kaspersky-Virenschutzprodukten", (press release of 15.03.2022). URL: www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2022/220315_Kaspersky-Warnung.html [Retrieved: 27.09.2022].

BSI
Federal Office for Information Security: *IT-Sicherheitskennzeichen,* 2022. URL: www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/IT-Sicherheitskennzeichen/it-sicherheitskennzeichen_node.html [Retrieved: 27.09.2022].

CrowdStrike 2021a
CrowdStrike (Ed.): 2021. *Global Threat Report*, 2021. URL: go.crowdstrike.com/rs/281-OBQ-266/images/Report2021GTR.pdf [Retrieved: 27.09.2022].

CrowdStrike 2021b
CrowdStrike (Ed.): *Zero Trust Security Explained: Principles of the Zero Trust Model*, 2021. URL: www.crowdstrike.com/cybersecurity-101/zero-trust-security/ [Retrieved: 27.09.2022].

Cyber Security Agency of Singapore 2021
Cyber Security Agency of Singapore: *The Singapore Cybersecurity Strategy 2021*, 2021. URL: www.csa.gov.sg/News/Publications/singapore-cybersecurity-strategy-2021 [Retrieved: 27.09.2022].

ENISA 2021
European Union Agency for Cybersecurity (ENISA): *ENISA Threat Landscape 2021*, 2021. URL: www.enisa.europa.eu/publications/etl-2021/enisa-threat-landscape-2021-2022-final_de.pdf [Retrieved: 27.09.2022].

European Commission 2022a
European Commission: *European Chips Act*, 2022. URL: ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-chips-act_en [Retrieved: 27.09.2022].

European Commission 2022b
European Commission: *eIDAS Regulation*, 2022. URL: digital-strategy.ec.europa.eu/en/policies/eidas-regulation [Retrieved: 27.09.2022].

European Commission 2022c
European Commission: *Cyber Resilience Act*, 2022. URL: digital-strategy.ec.europa.eu/en/library/cyber-resilience-act [Retrieved: 27.09.2022].

European Commission 2020
European Commission: *European data strategy*, 2020. URL: ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_en [Retrieved: 27.09.2022].

Europol 2019
European Union Agency for Law Enforcement Cooperation Europol: *IOCTA. Internet Organised Crime Threat Assessment*, 2019. URL: www.europol.europa.eu/sites/default/files/documents/iocta_2019.pdf [Retrieved: 27.09.2022].

Flashpoint 2021
Flashpoint (Ed.): *Facing Five Types of Ransomware and Cyber Extortion*, 2021. URL: www.flashpoint-intel.com/blog/facing-five-types-of-ransomware-and-cyber-extortion/ [Retrieved: 27.09.2022].

Handelsblatt 2020
Handelsblatt (Ed.): *Todesfall nach Hackerangriff auf Uni-Klinik Düsseldorf*, 2020. URL: www.handelsblatt.com/technik/sicherheit-im-netz/cyberkriminalitaet-todesfall-nach-hackerangriff-auf-uni-klinik-duesseldorf/26198688.html [Retrieved: 27.09.2022].

Security Intelligence 2019
Security Intelligence (Ed.): *The Decline of Hacktivism: Attacks Drop 95 Percent Since 2015*, 2019. URL: securityintelligence.com/posts/the-decline-of-hacktivism-attacks-drop-95-percent-since-2015/ [Retrieved: 27.09.2022].

Intel471 2020
Intel471 (Ed.): *Partners in Crime: North Koreans and Elite Russian-speaking Cybercriminals*, 2020. URL: intel471.com/blog/partners-in-crime-north-koreans-and-elite-russian-speaking-cybercriminals [Retrieved: 27.09.2022].

Mandiant 2019
Mandiant (Ed.): APT41: *A Dual Espionage and Cyber Crime Operation*, 2019. URL: www.mandiant.com/resources/blog/apt41-dual-espionage-and-cyber-crime-operation [Retrieved: 27.09.2022].

Noun
Noun Projekt. URL: https://thenounproject.com [Retrieved: 17.12.2021].

PwC 2020
PwC (Ed.): *Cyber Threats 2020: A Year in Retrospect*, 2020. URL: www.pwc.co.uk/cyber-security/pdf/pwc-cyber-threats-2020-a-year-in-retrospect.pdf [Retrieved: 27.09.2022].

Süddeutsche Zeitung 2022
Süddeutsche Zeitung (Ed.): *Ein Jahr nach Cyberangriff: Anhalt-Bitterfeld spürt Folgen*, 2022. URL: www.sueddeutsche.de/wirtschaft/internet-koethen-anhalt-ein-jahr-nach-cyberangriff-anhalt-bitterfeld-spuert-folgen-dpa.urn-newsml-dpa-com-20090101-220705-99-910444 [Retrieved: 27.09.2022].

Stiftung Neue Verantwortung 2022
Stiftung Neue Verantwortung (Ed.): *Deutschlands staatliche Cybersicherheitsarchitektur*, 8. Auflage, 2022. URL: www.stiftung-nv.de/sites/default/files/cybersicherheitsarchitektur_achteauflage0422.pdf [Retrieved: 27.09.2022].

Tagesspiegel Background Cybersecurity 2022
Tagesspiegel Background Cybersecurity (Ed.): *Attacke auf Viasat – eine gezielte Cyberaktion*, 2022. URL: background.tagesspiegel.de/cybersecurity/attacke-auf-viasat-eine-gezielte-cyberaktion [Retrieved: 27.09.2022].

The White House 2021
The White House (Ed.): *Executive Order 14028: Improving the Nation's Cybersecurity*, 2021. URL: www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/ [Retrieved: 27.09.2022].

Washington Post 2021
Washington Post (Ed.): *Panic Buying Strikes Southeastern United States as Shuttered Pipeline Resumes Operations*, 2021. URL: www.washingtonpost.com/business/2021/05/12/gas-shortage-colonial-pipeline-live-updates/ [Retrieved: 27.09.2022].

About acatech – National Academy of Science and Engineering

acatech advises policymakers and the general public, supports policy measures to drive innovation, and represents the interests of the technological sciences internationally. In accordance with its mandate from Germany's federal government and states, the Academy provides independent, science-based advice that is in the public interest. acatech explains the opportunities and risks of technological developments and helps to ensure that ideas become innovations – innovations that lead to greater prosperity, welfare, and quality of life. acatech brings science and industry together. The Academy's Members are prominent scientists from the fields of engineering, the natural sciences and medicine, as well as the humanities and social sciences. The Senate is made up of leading figures from major science organisations and from technology companies and associations. In addition to its headquarters at the acatech FORUM in Munich, the Academy also has offices in Berlin and Brussels.

Editors:

Claudia Eckert
Fraunhofer Institute for Applied and Integrated Security
Lichtenbergstraße 11
85748 Garching near Munich | Germany

Reinhard Ploss
acatech – National Academy of Science and Engineering
Karolinenplatz 4
80333 Munich | Germany

Series editor:
acatech – National Academy of Science and Engineering, 2022

Munich Office
Karolinenplatz 4
80333 Munich | Germany
T +49 (0)89/52 03 09-0
F +49 (0)89/52 03 09-900

Berlin Office
Pariser Platz 4a
10117 Berlin | Germany
T +49 (0)30/2 06 30 96-0
F +49 (0)30/2 06 30 96-11

Brussels Office
Rue d'Egmont/Egmontstraat 13
1000 Brussels | Belgium
T +32 (0)2/2 13 81-80
F +32 (0)2/2 13 81-89

info@acatech.de
www.acatech.de

Recommended citation:
Eckert, C./Ploss, R. (Eds.): *Cybersecurity. Current Situation and Future Challenges* (acatech IMPULSE), Munich 2022.

Bibliographical information published by the Deutsche Nationalbibliothek
The Deutsche Nationalbibliothek lists this publication in the Deutsche Nationalbibliografie; detailed bibliographical data is available online at http://dnb.d-nb.de.

Coordination: Dr. Anna Frey, Paul Grünke, Simon Litsche
Edited by: Alrun Straudi
Translation: Paul Clarke and Charlotte Couchman, Lodestar Translations
Layout-concept, conversion and typesetting: Groothuis, Hamburg
Cover photo: © shutterstock/Khakimullin Aleksandr

The original version of this publication is available at www.acatech.de.

Professional cyberattacks by organised criminals and politically motivated actors pose an increasingly serious threat to Germany and the whole European region. Cybersecurity, that is the ability to counter such attacks, is a central plank of successful digitalisation. It creates trust in the digital systems which are in daily use. Digital sovereignty is closely intertwined with cybersecurity. Together they form the foundation for self-determined and trusted activity in cyberspace.

Cybersecurity should be considered a task for society as a whole: policy makers, business, academia as well as citizens are all affected. This IMPULSE provides an overview of the issues together with suggestions as to how all involved stakeholders can help to increasing cybersecurity. The cornerstone must be an ambitious cybersecurity strategy designed by policymakers.