Recommendation of the
40th General Assembly of the
German Rectors' Conference
on 13 May 2025
in Magdeburg

Pressure on universities, federal states and the federal government to act – HRK recommendations on cybersecurity

Table of Contents

Summary
The security authorities rate the general threat situation for universities as extremely high regarding cybersecurity. In particular, the following potential scenarios can currently be identified: ransomware attacks, espionage and spying on dissident networks and social movements. Artificial intelligence (AI) is also increasingly being used in these threat scenarios.

Balancing resilience, openness and digital sovereignty is a particular challenge for universities in the face of the threat of cyberattacks. But there are also solutions and strategies here. In order to develop and implement these, the HRK makes the following recommendations to universities, federal states and federal government:

The HRK recommends that *universities* fulfil the tasks of maintaining university IT operations and safeguarding particularly sensitive data through multi-level security system concepts. These concepts must include prevention, emergency plans and exercises, which can also be implemented through cooperation and consultations. Universities have a special responsibility when it comes to teaching cybersecurity practices.

The HRK recommendations to the *federal states* involve the establishment of cross-university structures. Reporting channels and contact persons must be named and there must be increased awareness of the issue and more further training provided. This will require considerable additional funding, which will also require support from the federal government.

The *federal government* is recommended to take action in line with its overarching role in risk prevention. This implies giving warning signals and identifying possible responses, promoting cross-border communication and ramping up research. As part of the new possible ways to increase cybersecurity, innovative financing models must also be implemented quickly in cooperation with the federal states.

I. Current security situation

In light of its recommendation entitled „Information security[1] as a strategic task for leaders of universities“[2] published in 2018, the German Rectors' Conference states that its guidelines for universities are still essentially valid. However, the recommendation must be re-contextualised in light of the new security situation following the so-called „turning point in history“.[3]

Security authorities rate the threat level for universities as extremely high in terms of cybersecurity. This rating was also based on the Russian war of aggression against Ukraine, the armed conflicts in the Middle East and the tensions in East Asia.

Universities are of particular interest for potential attacks. The reasons for this include the personal data of (highly) qualified employees, the results of excellent research, the incentives for innovation through transfer, international cooperations and the educational mandate in the interests of a democratic society. As a result, the question is not whether, but when, an incident will occur at the individual universities.

In particular, the following threat scenarios can currently be identified:

- Ransomware attacks[4]
- Espionage[5]
- Spying on dissident networks.[6]

Artificial intelligence (AI) is increasingly being used in these threat scenarios. This also applies to the production of disinformation, which is being perfected through AI: spam is becoming more „intelligent", deep fakes[7] falsify media content (images, videos, voices) in a realistic manner and robocalls[8] are computerised answering machines that make telephone calls with pre-recorded messages as if done by a robot.

II. Universities caught between resilience, openness and digital sovereignty

The current cybersecurity situation has led to universities finding themselves in a particularly tense relationship between the requirements of resilience, openness and digital sovereignty. Resilience[9] is the central concept of cybersecurity. Openness[10] is a constitutive characteristic of German universities. The digital sovereignty[11] of universities must have an appropriate bearing on reality, both in terms of the different initial parameters (including size, expertise) and the threat scenarios. Digital sovereignty in the broader sense therefore means that universities have control over selecting their own technologies based on functionality, speed of implementation, controllability, security and cost-effectiveness. It is important to ensure no university becomes unilaterally dependent on cybersecurity products that may be prohibited through regulatory provisions, e.g. with regard to data protection. In terms of preparing for cyberattacks and in the interests of digital sovereignty, it is fundamentally important to pool internal expertise and management skills, assign clear responsibilities and establish rules for the cooperation of all university members.

Balancing resilience, openness and digital sovereignty is a particular challenge in the face of the threat of cyberattacks. A university can only implement the necessary balancing processes by taking into account its orientation, its legal framework and, last but not least, its available resources. There is therefore no externally prescribed master plan for increasing cybersecurity that is „valid for all universities".

III. HRK recommendations on cybersecurity

In light of the introductory remarks, the HRK makes the following recommendations to universities, federal states and federal government.

1. Recommendations addressed to universities

Define basic and core safeguards

There are two main tasks for university leadership:

- the maintenance of university IT operations and
- the safeguarding of particularly sensitive data.

The HRK therefore recommends that universities adopt multi-level security system concepts[12]: in terms of basic safeguards, particular attention should be paid to the set-up of individual business continuity management (BCM)[13], the university-wide introduction of two-factor authentication[14] and the use of functional e-mail accounts. In order to determine core safeguards, the respective data, information and systems requiring special protection must be identified in advance.[15] In terms of the multi-level security system concept, there must be an examination of how decentralised units are handled: i.e. whether the aim is to achieve integrated unity or decentralised self-sufficiency.

Precautions

Prevention is cost-effective because repairing damage that has occurred is far more expensive than the cost of prevention. One effective tool is vulnerability scanning. Outdated hardware and software, e.g. in laboratories (measuring devices or control computers with old operating systems), for which updates can no longer be installed, must first be (partially) isolated and then replaced through sustainable replacement planning. The risk posed by specialised (in-house) software must also be examined. It is also important to have backups and disaster recovery plans in place for all centralised data and systems. To prevent cyberattacks, security operation centres (SOC)[16] can conduct regular, proactive security scans.

Plan for an emergency

As part of business continuity management (BCM), emergency plans are prioritised as core university processes,[17] which also include installing an emergency hotline or having a first call system in place.[18] Checklists or emergency cards are also helpful in this context.[19] Universities can also sign framework agreements with companies as APT response services[20]. These services provide support in handling the wide range of tasks involved in emergency management and contribute specialised expertise for these tasks, which is not usually available in this form at universities.

Practise drills

Cybersecurity drills[21] should be made mandatory in the same way as fire drills. With regard to the preparation, effort and setting of these exercises, there are various training scenarios that are also offered for external services: easy-access formats include simulation games, which have also proven to be very helpful, particularly at management level. In addition to easy-access formats, coordination exercises with different locations can also be considered for operational university staff.

Reduce the attack surface
Not all data must necessarily be publicly visible and retrievable via the Internet. Universities should therefore examine whether and, if so, how less data can be produced, stored and made publicly accessible.[22] Information worth protecting, e.g. about IT security structures or measures, should not be made public and/or make its way onto social media (e.g. LinkedIn) because it is very easy to spy on people there using special filters.

Utilise cooperations
The HRK renews its recommendation for cooperation on cybersecurity. IT security is a team game. Cooperation can extend to nationwide and network concepts, communication concepts for incidents, training and awareness measures, exchange of experience and purchasing cooperations, security operation centres (SOC)[23], peer audits, peer penetration tests and personnel for computer emergency response teams.[24] However, the prerequisite for cooperation is that the funding bodies both enable the universities to cooperate and stimulate cooperation.[25]

Have consultations
Closely related to cooperation are consultations, which can also be organised as cooperation with non-profit organisations (e.g. the Higher Education Information System (HIS), German National Research and Education Network (DFN), Centres for Communication and Information Processing (ZKI)). Framework agreements can be very useful here. Consultations can also extend to mental health support following cyberattacks and incidents of blackmail.

Safeguard communication skills
The HRK recommends prior planning on how to structure communication during a cyberattack by having a crisis and communication plan in place.[26] Among other things, this should include alternative communication channels in the event that e-mail communication or a telephone system suddenly goes down due to a system failure. Communication with students is a particular challenge during an attack. In the event of this, it is important to set up a „shadow system" that enables fast and secure communication (e.g. website) as a preventive measure.[27]

Teach cybersecurity practices

Universities also need to teach awareness and build skills in relation to cybersecurity. These measures apply to all university members and are important for everyone.[28] As far as students are concerned, it makes sense to integrate the teaching of cybersecurity skills into the curriculum. On this basis and depending on the university profile, the technical competence and excellence in research in relevant subjects can play a role in increasing the cybersecurity of the entire university.

Embed cybersecurity in the university culture
We must succeed in viewing cybersecurity as a comprehensive creative and cultural asset.[29] This also includes practising a culture of error. Mistakes in relation to cybersecurity should not be seen as a failure, but as an impetus for joint learning to further develop cybersecurity. Rather than misunderstood shame, open communication about any mistakes must be perceived as a positive experience and an expression of a resilient university culture.

2. Recommendations addressed to the federal states

Establish cross-university structures
The federal states must work with their universities to develop overarching concepts and strategies for cybersecurity. Overarching concepts should build on existing collaborations, the expansion of which must be promoted through appropriate empowerment and incentives.[30] Existing state initiatives can be set up or expanded as part of the centres for communication and information processing (computer centres, ZKI[31]) or based on state institutions for digital university teaching[32]. This can achieve a critical size for action units and promote the development of core IT facilities.

Safeguard data across universities
The federal states are recommended to set up a cross-university data safeguarding system. They can do this by setting up a basic service to provide a cooperative operating model. Individual selected universities or institutions can use state funds to provide other universities with a storage infrastructure. This enables universities to safeguard their data outside their own infrastructure and restore it quickly in the event of an incident. A separate „data safe“ can also be established with regard to business-critical data, particularly in administration.[33]

Define reporting channels and contact persons
The HRK recommends the improvement of reporting channels and the clear designation of contact persons. After the initial experiences with cyberattacks, it was often not clear which people in the ministries and authorities needed to be informed. This must be remedied. So far, support from state authorities (e.g. the State Criminal Police Office (LKA), the Federal Office for the Protection of the Constitution) has been very helpful. The information from the State Offices for the Protection of the

Constitution was particularly useful, but came late. On the other hand, the deletion period is so short due to data protection requirements that fast and direct communication and exchange channels are necessary.

Enable and provide further training
The HRK would like to point out that cyberattacks are developing extremely dynamically and therefore recommends that the federal states promote appropriate further training for university members. Funding should be provided for on-site training and further training with external providers, but also for the conceptual development of academic continuing education through the universities. Digital self-study modules[34] that accommodate university members' usual flexible and remote working methods offer a special way to impart cybersecurity knowledge and skills.

Practise a political culture of error
Analogous to the aforementioned further development of the internal culture of error at universities, the HRK also recommends practising a political culture of error at state level. The field of cybersecurity is so dynamic and complex that errors cannot be ruled out, even in the interaction between universities, authorities and ministries. In critical situations, a political culture of error plays a decisive role in ensuring that errors can be identified and quickly rectified.

Improve basic equipment
The HRK calls on the federal states to provide adequate basic equipment, also with regard to cybersecurity. Investment funds are required to increase the resilience of the IT infrastructure and material resources are needed for additional hardware and software. Additional personnel are essential for increasing cybersecurity. Cybersecurity specialists are needed at all levels right up to the Chief Information Officer (CIO). As maintaining expertise in resilience is an ongoing challenge, permanent positions are required. In addition, due to the particular shortage of skilled labour in the IT sector, jobs need to be re-evaluated or a higher pay scale authorised. Currently, only a single-digit percentage of total IT expenditure is used for cybersecurity.[35] It will take considerable effort to achieve the target formulated by the Federal Office for Information Security (BSI), according to which 20 per cent of IT budgets are to be earmarked for cybersecurity[36]. This can only be achieved with the support of the federal government through innovative financing models. (See below)

Expand research funding
The HRK recommends that the federal states fund research on cybersecurity, either together or in coordination with the federal government. (See below)

3. Recommendations addressed to the federal government

Avert dangers

In view of the threat situation, the HRK recommends that the federal government take even more action in line with its overarching role in risk prevention.

This role arises from the international dimension of cybersecurity. There is an area of tension here, as organisations in industry and society also engage in international cooperation with countries that do not share the values of liberal democracies. This also applies to global academic cooperation. Universities are also gateways for attacks, especially for obtaining data on cooperation partnerships, transfer organisations and the entire innovation system. Cyberattacks on universities therefore also jeopardise the competitiveness of the German economy.

On the national level, the federal states in Germany generally have decentralised responsibility for security issues. In view of the threat situation, however, the federal government is also called upon here, as there are cross-state threat situations and the entirety of the German higher education landscape certainly deserves standards that apply in the case of a national critical infrastructure. In addition, it must be the task of the federal government to contribute to the cross-state networking of the relevant universities and university alliances and to provide impetus for this. This applies in particular to the consolidation of concepts and initiatives of the federal states.

Give warning signals and demonstrate possible responses

The federal government must help to improve early warning systems and provide more information for response options. For example, the Federal Office for Information Security (BSI) should offer more university-specific information for emergency planning and services. A nationwide service for detecting security vulnerabilities also appears necessary. Nationwide simulation games, prevention measures and awareness-raising programmes could also be considered.

The HRK considers it necessary to improve the flow of information between and with the intelligence services and sees a special role for the federal government in this. For example, in the event of an attack, the Federal Office for the Protection of the Constitution must be able to inform the equivalent offices in the federal states and the universities concerned in parallel, which is currently only possible in one state. A structured interplay between incident reporting by universities on the one hand and the provision of information by the services on the other is desirable. However, it should be noted that the intelligence services may not interfere with university autonomy.

Ramp up research

The federal government is already funding a wide range of IT security projects.[37] The HRK acknowledges the federal government's research funding on cybersecurity to date and recommends expanding the corresponding programmes. In addition, the federal government should support research projects for new protection and defence technologies, among other things. In addition, the development of new security standards in the EU context must be promoted and programmes for the further development of digital sovereignty must be established.

Reorganise financial responsibility

The role of the federal government in averting danger, the international dimension of cybersecurity, the need for cross-state cooperation and the coordination of specialised service centres mean that the federal government is responsible. The HRK calls for funding with which the federal government combines, completes and consolidates the cybersecurity efforts of the universities and the federal states and also forms an overarching framework for cross-state cooperation. Agile and unbureaucratic funding is needed to increase cybersecurity as quickly and significantly as possible. As measures to increase cybersecurity must also be embedded in the strategies of the universities, funding must also include the relevant efforts and concepts. In view of the threats to education, research and internal security, the HRK is open to innovative solutions and appropriate funding modalities.

Appendix 1: Glossary

Spying on dissident networks: This spying can target, for example, political dissidents, religious minorities and the LGBTQ or women's movement from foreign regimes. In most cases, the aim is not only to spy on existing networks in Germany, but also to identify their contacts or „mirror networks" in the countries of origin in order to prosecute them politically and under criminal law. This represents a new quality of threat to the life and limb of those affected.

Business continuity management (BCM): Emergency management that comprehensively governs all activities aimed at ensuring orderly operations following incidents.[38] The BSI's business continuity management concept is part of information security management (ISM).[39]

Core IT facilities: Facilities at universities where equipment, expertise and methods are available. Expensive devices that can only be operated with specialised knowledge are bundled centrally here and made accessible to researchers and external parties. With core facilities, universities can not only save money, but also be specific in closing gaps in their equipment pool. In addition to the efficient use of devices, costs for maintenance and repairs are shared.[40]

Cybersecurity and information security: The term „cybersecurity" has become more relevant than the concept of „information security": the concept of cybersecurity focuses on the risk of an attack via communication networks and networked systems and the need to minimise damage.

Digital sovereignty: At the institutional level in the narrower sense, it is primarily aimed at in-house IT services, the avoidance of irreversible dependencies and the influence of universities on the software used.[41]

Deep fake: A portmanteau of „deep learning" and „fake". Deep fake refers to AI-generated or AI-manipulated image, sound or video content that resembles real people, objects, places, facilities or events and would falsely appear to a person to be real or truthful.[42]

Openness: A constitutive characteristic of German universities. Universities can and want to fulfil their mission of education, research, transfer and democratic dialogue. But they can only do this if they are open to society and to national and international cooperation of all kinds.[43] Quantitative indicators of this openness are the high fluctuation in the 2.9 million students and almost 800,000 university employees as well as the quantity of just under 37,000 international collaborations. This illustrates the major

challenge for universities in creating the greatest possible resilience.

Ransomware attacks: University computers are infected and blocked using encryption for the purpose of extorting money. Such attacks have increased significantly in recent years. The boundaries between private and state attacks are becoming increasingly blurred.

Resilience: Central concept of cybersecurity. Above all, resilience works towards the goal of returning „to a functional system status as quickly as possible after an attack"[44]. This is based on the realisation that „absolute security cannot be created in any information security system"[45]. Prevention and subsequent adjustment of the system to at least the same level as before the attack also serve this main objective of returning to a workable state.

Robocalls: A portmanteau of „robot" and „calls". In robocalls, computerised answering machines make telephone calls with pre-recorded messages as if done by a robot.

Security operation centre (SOC): Regularly checks the IT systems of participating universities for possible security vulnerabilities, provides information on current threats and searches the darknet for university data, such as leaked access data. If hackers should penetrate a system, the SOC can also support the universities with forensic analyses and damage repair.[46]

Espionage: This continues to be a method used by state agencies, whereby nationals, who may initially be uninvolved in espionage (e.g. students and visiting academics), are roped in to spy. Recently, the focus of espionage targets has been on the further development of high technology, cooperation with the defence sector, political analyses and geographical data and maps.

Appendix 2: About the creation of the recommendations

These recommendations were prepared by the HRK Standing Committee on Digitalisation. The Committee is headed by the HRK Vice-President for Digitalisation and Academic Continuing Education, Professor Dr Ulrike Tippe. The permanent members of the Committee are Professor Dr Philipp Ahner, Mr Malte Dreyer, Professor Dr Hannes Hartenstein, Professor Dr Wolfram Horstmann, Professor Dr Michael Jäckel, Professor Constanze Langer, Professor Dr Gerhard Lauer, Mr Jens Andreas Meinen, Professor Dr Jörg Müller-Lietzkow, Ms Paula Paschke, Professor Dr Hans Pongratz, Professor Dr Arnd Steinmetz and Professor Dr Jens Weiss. The Committee is supported by Dr Elmar Schultz at the HRK Office.

The starting point for the creation of the recommendations was a Committee hearing on 4 November 2024 on the topic of „Cybersecurity at universities: Balance between resilience, digital sovereignty and openness". Dr Christian Grimm, Professor Dr May-Britt Kallenrode, Mr Oliver Kaczmarek, Professor Dr Maria Leitner, Dr Florian Rautenberg and Professor Dr Fabian Schmieder were consulted. The results of the consultation were supplemented by a focus round on 18 November 2024, the day before the HRK General Assembly, and by a discussion with Professor Dr Haya Schulmann, Professor Dr Michael Backes and Mr Thomas Franke at the Committee meeting on 28 January 2025.

The HRK would like to thank everyone involved for their contributions.

---

[1] See glossary for the definition of information security and cybersecurity.
[2] HRK (2018), Information security as a strategic task for leaders of universities, 6 November, https://www.hrk.de/resolutions-publications/resolutions/beschluss/detail/information-security-as-a-strategic-task-for-leaders-of-universities/, last accessed: 28/03/2025.
[3] It should also be noted that the legal framework has evolved. On 18 October 2024, the NIS2 Directive on the level of cybersecurity in the EU (Network and Information Systems (NIS)) repealed the previous NIS Directive of 23 June 2017. The Cyber Resilience Act (CRA) of 10 December 2024 also places security requirements on hardware and software products. It is also possible that DORA (the Digital Operational Resilience Act) of 17 January 2023 – a regulatory framework aimed at strengthening the digital resilience of all companies in the EU financial sector – may also have an impact on other sectors.
[4] See glossary.
[5] Ibid.
[6] Ibid.
[7] Ibid.
[8] Ibid. A portmanteau of „robot" and „calls".
[9] Ibid.
[10] Ibid.
[11] Ibid.
[12] Cf. HRK (2018), Information security, p. 12f, 16.
[13] See glossary.

[14] Hardware tokens or YubiKeys, for example, are possible solutions if company mobile phones are not an option.
[15] A differentiation between basic and core safeguards is in line with the BSI's IT-Grundschutz Methodology. BSI, https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/Zertifizierte-Informationssicherheit/IT-Grundschutzschulung/Online-Kurs-IT-Grundschutz/Lektion_2_Sicherheitsmanagement/Lektion_2_09/Lektion_2_09_node.html (available only in German), last accessed: 28/03/2025. The question of defining what is and what is not „critical data, information and systems" does not appear to be trivial. Indicators could be a particular risk to assets, irreparable damage or a threat to the organisation's existence.
[16] See glossary.
[17] The following provide guidance: ZKI (ed., 2023) Guidelines on preparing for information security incidents, https://zenodo.org/records/10130339 (available only in German), last accessed: 28/03/2025 and HIS-HE (2023), Crisis management after cyber-attacks - Recommended Actions, https://medien.his-he.de/publikationen/detail/krisenmanagement-nach-cyber-angriffen-handlungsempfehlungen (available only in German), last accessed: 28/03/2025.
[18] The DFN is therefore pursuing the idea of a „112 number" in the style of the European fire service number 112.
[19] BSI, Set of measures for emergency management, https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/Notfallkarte/Massnahmenkatalog_Notfallmanagement.pdf?__blob=publicationFile&v=3 (available only in German), last updated: May 2021, last accessed: 28/3/2025 and BSI, IT emergency card „What to do in IT emergencies", https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Unternehmen-allgemein/IT-Notfallkarte/IT-Notfallkarte/it-notfallkarte.html, last accessed: 28/03/2025.
[20] Services for defence against ongoing or completed attacks in the event of targeted attacks by strong adversaries (Advanced Persistent Threat, APT), see BSI (2025), List of qualified APT response services, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Dienstleister_APT-Response-Liste.html (available only in German), last updated: 23/01/2025, last accessed: 28/03/2025.
[21] The aims and learning objectives of such exercises are to experience certain situations, make certain decisions, communicate within the team and with external parties, test emergency plans and to complete documentation and technical analyses in a short space of time. Quoted from Leitner, HRK hearing 04/11/24.
[22] The concept of „digital sobriety" also includes the idea of saving energy and reducing the digital carbon footprint.
[23] See glossary.
[24] HRK (2018), Information security, https://www.hrk.de/fileadmin/redaktion/hrk/02-Dokumente/02-01-Beschluesse/HRK_MV_Empfehlung_Informationssicherheit_06112018_EN.pdf, 06/11/2018, p. 15, last accessed: 28/03/2025; HRK (2021), Utilising the momentum of digitalisation, https://www.hrk.de/fileadmin/redaktion/hrk/02-Dokumente/02-01-Beschluesse/2021-06-08_HRK-S-Entschliessung_zu_digitalen_Lehrinfrastrukturen_EN.pdf, 8 June 2021, p. 5, last accessed: 28/03/2025; HRK (2023), „Digital University", https://www.hrk.de/fileadmin/redaktion/hrk/02-Dokumente/02-01-Beschluesse/2023-11-14_HRK-MV_Entschliessung_Digitale-Hochschule-Kooperationen.pdf (available only in German), 14/11/2023, p. 12, last accessed: 28/03/2025.
[25] Ibid., p. 6f.
[26] HRK (2018), Information security, p. 5, 14f.
[27] Experience has shown that completely shifting communication to individual messenger services is not a viable solution.
[28] Cf. HRK (2018), Information security, p. 9.
[29] HRK (2018), Information security, pp. 4, 5, 9.
[30] HRK (2023), „Digital University", p. 6f.
[31] ZKI, https://www.zki.de/ueber-den-zki/mitglieder/ (available only in German), last accessed: 28/03/2025.

[32] Network of the German federal state institutions for digital university teaching, https://netzwerk-landeseinrichtungen.de/ (available only in German), last accessed: 28/03/2025.
[33] Ministry of Culture and Science of the State of North Rhine-Westphalia (2025), Cybersecurity, https://www.mkw.nrw/themen/wissenschaft/wissenschaftspolitik/cybersicherheit (available only in German), last accessed: 28/03/2025.
[34] A good example of this is SecAware.nrw, an online self-learning programme on cybersecurity and IT security for universities in North Rhine-Westphalia. Ibid.
[35] Data for this status quo cannot be found in the literature. However, discussions with many organisations in Germany and the EU have shown that currently two to five per cent of the total IT staff expenditure is used for cybersecurity. This corresponds to a share of one to four per cent of total IT expenditure.
[36] This BSI guideline refers to states and companies that should spend twenty per cent of their IT expenditure on cybersecurity, 07/04/2024, https://www.ad-hoc-news.de/sonstige/die-praesidentin-des-bundesamtes-fuer-sicherheit-in-der/65115311 (available only in German), last accessed: 02/05/2025. Universities are comparable to companies and the state when it comes to sensitive innovation and personal data.
[37] BMBF (2025), Funding projects in the field of networking and the security of digital systems, https://www.forschung-it-sicherheit-kommunikationssysteme.de/projekte (available only in German), last accessed: 31/03/2025.
[38] BSI (2022), Glossary and list of abbreviations, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Hilfsmittel/Standard200_4_BCM/Standard_200-4_BCM_Glossar.pdf?__blob=publicationFile&v=4 (available only in German), p. 4, last accessed: 31/03/2025.
[39] BSI (2023), https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Hilfsmittel/Standard200_4_BCM/Standard_200-4_BCM_Flyer.pdf?__blob=publicationFile&v=2, (available only in German), last updated: September 2023, last accessed: 31/03/2025.
[40] Jedicke, Philipp (2024), Core Facilities: Shared research infrastructure - a model for the future? https://www.forschung-und-lehre.de/forschung/geteilte-forschungsinfrastruktur-ein-zukunftsmodell-6429 (available only in German), Forschung und Lehre online magazine from 23/05/2024, last accessed: 31/03/2025.
[41] Cf. HRK (2023), „Digital University", p. 11f. Further information from the German Council of Science and Humanities (2023), https://www.wissenschaftsrat.de/download/2023/1580-23.pdf?__blob=publicationFile&v=11 (available only in German), October 2023, last accessed: 31/3/2025 and Krupka, D. (2020), Dimensions of digital sovereignty - an overview. In: German Informatics Society (ed.) Key aspects of digital sovereignty, working paper, https://gi.de/fileadmin/GI/Allgemein/PDF/Arbeitspapier_Digitale_Souveraenitaet.pdf (available only in German), pp. 4-7, last accessed: 31/03/2025.
[42] EU Artificial Intelligence Act, Chapter I, Art. 3, No. 60, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202401689 of 13 June 2024, last accessed: 31/03/2025.
[43] Standard expressions for this characteristic include concepts such as „Open universities for advancement through education", https://offene-hochschulen.de/ (available only in German), last accessed: 31/03/2025; HRK (2015), „German Universities Open to the World", 11/11/2015, https://www.hrk.de/home/universities-against-xenophobia/, last accessed: 31/03/2025 and the insistence on the „openness of participation" in social debates, cf. HRK (2024), Protecting universities as a free space for discourse, (https://www.hrk.de/fileadmin/redaktion/hrk/02-Dokumente/02-01-Beschluesse/02-01-01-Englische_Beschluesse/2024-05-14_HRK-MV_Entschliessung_Hochschulen-als-freien-Diskursraum-sichern_EN.pdf 14/05/2024, last accessed: 31/03/2025.
[44] HRK (2018), Information security, p. 14.
[45] Ibid.
[46] North Rhine-Westphalia (2024), For more cybersecurity! Universities launch joint security operation centre, https://www.mkw.nrw/fuer-mehr-

cybersicherheit-hochschulen-starten-gemeinsames-security-operation-center (available only in German), 27/06/2024, last accessed: 31/03/2025.