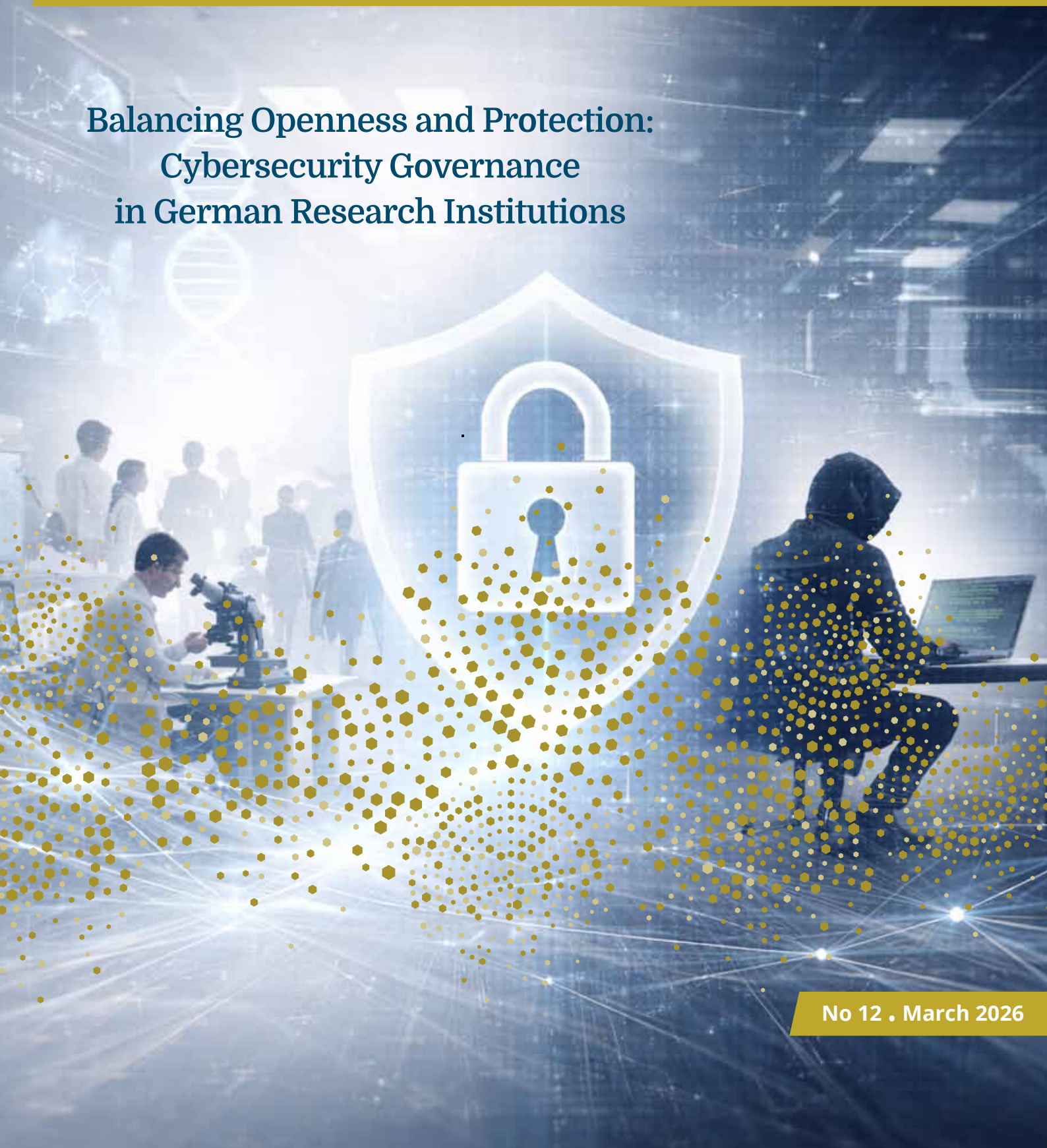
BIGS POLICY PAPER

Brandenburg Institute for **Society** and **Security**

Tim Stuchtey, Esther Kern, Hanna Denecke, Andreas Könen, Nadine Nagel

Balancing Openness and Protection: Cybersecurity Governance in German Research Institutions



No 12 . March 2026

IMPRINT

Located in Potsdam, the Brandenburg Institute for Society and Security is an independent, non-partisan, non-profit organization with an inter- and multidisciplinary approach with a mission to close the gap between academia and practice in civil security. The views expressed in this publication are those of the author(s) alone. They do not necessarily reflect the views of the Brandenburg Institute for Society and Security (BIGS).

BIGS
BRANDENBURGISCHES INSTITUT für GESELLSCHAFT und SICHERHEIT

Brandenburgisches Institut für Gesellschaft und Sicherheit gGmbH

Executive Director:
Prof. Dr. Tim H. Stuchtey

Dianastraße 46
14482 Potsdam

Telefon: +49-331-704406-0

E-Mail: info@bigs-potsdam.org
www.bigs-potsdam.org

Authors:
Prof. Dr. Tim H. Stuchtey, Esther Kern, Hanna Denecke, Andreas Könen, Nadine Nagel

Title:
Balancing Openness and Protection: Cybersecurity Governance in German Research Institutions

Editor:
Brandenburgisches Institut für Gesellschaft und Sicherheit gGmbH
(Brandenburg Institute for Society and Security)

Prof. Dr. Tim H. Stuchtey (V.i.S.d.P.)

ISSN: 2194-2412
BIGS Policy Paper No. 12, March 2026

Frontcover: erstellt mit ChatGPT 5.2

Balancing Openness and Protection: Cybersecurity Governance in German Research Institutions

Tim Stuchtey, Esther Kern, Hanna Denecke,
Andreas Könen, Nadine Nagel

BIGS
BRANDENBURGISCHES INSTITUT
für GESELLSCHAFT und SICHERHEIT

ABSTRACT

Cybersecurity has emerged as a defining challenge for research governance. In Germany, universities and public research institutes operate within a highly open, internationally connected scientific ecosystem that amplifies both innovation and vulnerability. This paper examines cybersecurity governance in German research institutions through a science policy lens, focusing on the interplay between academic openness and institutional protection. Drawing on case studies, policy analysis, and expert interviews, the paper identifies systemic weaknesses in organizational culture, fragmented IT governance, and insufficient policy coordination between federal, state, and institutional levels. The study proposes a policy framework for balancing openness and protection by embedding cybersecurity culture, strengthening institutional accountability, and integrating research security into European and national policy instruments such as the NIS-2 Directive. By conceptualizing research institutions as both producers and subjects of cybersecurity, this paper contributes to current debates on research governance, national resilience, and science diplomacy.

Keywords:
Cybersecurity, Science Policy, Research Governance, Espionage, Academic Freedom, Critical Infrastructure

TABLE OF CONTENT

1. INTRODUCTION

In recent years, cyberattacks on German universities and research institutions have underscored the fragility of digital infrastructures in academia. Incidents such as the 2024 University of Potsdam (Foschung & Lehre 2024) shutdown and the ransomware attack on the University of the Bundeswehr (Specht 2025) in Munich demonstrate that research organizations have become prime targets for cyber operations. These attacks disrupt teaching and research, compromise sensitive data, and erode trust in the academic system's capacity to safeguard intellectual property and public investment.

The vulnerability of the academic sector stems not only from technological exposure but also from the cultural and institutional fabric of science itself. Scientific inquiry thrives on openness, collaboration, and global exchange; principles that often conflict with the restrictive logic of cybersecurity. Researchers commonly share data through unsecured channels, collaborate via foreign cloud systems, or overlook security protocols to avoid administrative friction. While such practices embody academic efficiency, trust, and cooperation, they also render institutions susceptible to espionage and sabotage.

This tension between openness and protection is not merely operational; it reflects a governance dilemma at the heart of modern science policy. German research institutions navigate a multi-level regulatory landscape involving federal ministries, state authorities, EU frameworks, and internal autonomy guaranteed under Article 5(3) of the German Basic Law. The resulting system favors freedom and decentralization but complicates the establishment of coherent cybersecurity governance.

The objective of this paper is to analyze how cybersecurity challenges reshape research governance in Germany. Specifically, it investigates how policy frameworks, institutional cultures, and legal constraints interact to produce – or inhibit – effective protection mechanisms. The analysis builds on the argument that research institutions must evolve from reactive crisis management to proactive resilience governance.

The structure of the paper proceeds as follows: Section 2 introduces the conceptual framework linking cybersecurity and science policy. Section 3 outlines the methodological approach based on document analysis and expert interviews. Section 4 presents findings on the threat landscape, institutional vulnerabilities, and cultural barriers. Section 5 discusses implications for research governance and policy coordination. Section 6 concludes with recommendations for balancing openness and protection in the academic sphere.

2. CONCEPTUAL FRAMEWORK AND LITERATURE BACKGROUND

2.1 Cybersecurity as a Governance Challenge in Science Policy

Cybersecurity in research institutions sits at the intersection of digital governance, national security, and academic freedom. Unlike corporate or governmental cybersecurity, where hierarchies and compliance regimes are more rigid, academia operates through a culture of autonomy and trust. This creates a unique governance dilemma: how can research institutions protect sensitive data, infrastructure, and intellectual property without undermining the principles of open science?

Theoretical approaches from science policy and organizational governance provide a foundation for addressing this tension. According to Jasanoff's concept of co-production (2004), science and governance mutually shape each other; security measures embedded in research governance not only protect knowledge but also redefine the very norms of scientific practice. Similarly, Bijker et al. (1987) emphasize that sociotechnical systems, like university IT infrastructures, are socially constructed and must be managed through both technical design and institutional culture.

From a policy perspective, cybersecurity in science represents a form of knowledge governance (Nowotny, 2008), in which the state, academia, and industry co-regulate flows of information. Yet, the governance of these flows remains fragmented. German universities operate under federalism, with higher education largely managed at the *Länder* level, while cybersecurity policy and national security remain federal competencies. This dualism complicates policy coherence and institutional accountability.

2.2 Openness, Dual-Use, and the Political Economy of Research

The principle of openness, e.g. sharing data, methods, and results, is central to scientific progress. However, as the study of dual-use research shows (Rappert & Gould, 2009), the dissemination of knowledge can also pose security risks when technologies have both civilian and military applications. Dual-use research in biotechnology, artificial intelligence, and materials science demonstrates how open science can inadvertently enable adversarial states or non-state actors to gain access to sensitive innovations.

China's strategy of "military-civil fusion," which systematically integrates civilian research into military applications, illustrates this dynamic vividly. Partnerships with Western universities, joint research programs, and scholarship schemes have occasionally served as vectors for strategic technology transfer. In Germany, several universities have reported cases where visiting scholars or research partnerships were later linked to Chinese defense institutions (Felden et al., 2022). These findings align with the Australian Strategic Policy Institute's (2019) documentation of at least 15 Chinese universities directly associated with military entities.

This interconnection between science and geopolitics demands a reframing of cybersecurity as not just an IT matter, but as part of research integrity and sovereignty. When academic data and findings become instruments of state competition, science policy must move from passive openness to managed openness; balancing collaboration with vigilance.

2.3 The Cultural Dimension of Cybersecurity

Organizational research underscores that cybersecurity effectiveness depends as much on cultural as on technical factors. Schein's (2010) model of organizational culture identifies shared assumptions and values as the core drivers of behavior. In academic institutions, values like autonomy, transparency, and collegiality dominate, thereby creating resistance to hierarchical control or restrictive IT policies.

The European Union Agency for Cybersecurity (ENISA) (2023) proposes cultivating a "cybersecurity culture" that normalizes responsible digital behavior across all organizational levels. In science, this requires redefining what responsible research conduct entails: not only ethical and reproducible, but also secure. Studies such as Kello (2017) and Rid (2020) emphasize that cyber risks are not purely technical but strategic, shaped by institutional norms, geopolitical context, and human factors.

Thus, the challenge for German research policy lies in embedding cybersecurity into the fabric of scientific culture – through awareness, leadership, and incentives – rather than imposing it as an external bureaucratic requirement.

2.4 Theoretical Model Guiding the Analysis

Drawing from the above strands, this paper adopts a multi-level governance model to analyze cybersecurity in research institutions. The model distinguishes three interdependent layers:

1. Macro (Policy Level):
National and EU frameworks, such as NIS-2, research security initiatives, and geopolitical dynamics.

2. Meso (Institutional Level):
University governance structures, IT management, and research collaboration policies.

3. Micro (Cultural Level):
Daily practices of researchers, attitudes toward cybersecurity, and informal norms of data sharing.

The analytical assumption is that failures in cybersecurity arise not only from insufficient technical safeguards but also from misalignments between these three levels. Policies remain ineffective when institutional incentives and cultural values do not support them. Conversely, a harmonized approach linking governance, culture, and technology enhances resilience without undermining scientific openness.

Quelle: Fotolia

3. METHODOLOGY AND DATA

3.1 Research Design

This study employs a qualitative research design grounded in comparative policy analysis. The purpose is to understand how governance structures, institutional cultures, and regulatory environments shape cybersecurity resilience in German research institutions. The design integrates document analysis, semi-structured expert interviews, and secondary data from cyber incident reports between 2019 and 2024.

Given the exploratory nature of the topic at the intersection of science governance and cybersecurity, the approach prioritizes contextual depth over statistical generalizability. It seeks to identify structural patterns, governance logics, and recurring vulnerabilities within the German research landscape.

3.2 Data Collection

Three complementary data sources underpin the analysis:

1. Expert Interviews:

Fifteen semi-structured interviews were conducted between October 2024 and February 2025 with cybersecurity officers, university administrators, policy advisers, and representatives of security agencies. The interviews explored institutional cybersecurity measures, experiences with cyber incidents, and perceived policy gaps. Interviewees were anonymized to ensure confidentiality and openness.

2. Document and Policy Analysis:

Relevant policy documents, including the German federal and state cybersecurity strategies, EU's NIS-2 Directive, and institutional security guidelines, were systematically reviewed. The analysis also covered official responses from the Federal Ministry of Education and Research (BMBF) and the Federal Office for Information Security (BSI).

3. Empirical Case Studies:

Recent cyber incidents involving German universities and research institutes were analyzed through media reports, parliamentary inquiries, and institutional statements. These include cases from the University of Potsdam (2024), University of Duisburg-Essen (2022), and Fraunhofer Institute for Microstructure of Materials and Systems (IMWS) (2022).

3.3 Analytical Framework

Data were analyzed using a **thematic coding strategy** (Braun & Clarke, 2006), aligning interview material and documents with the multi-level governance framework introduced in Chapter 2. Codes were clustered around three dimensions:

- **Institutional vulnerabilities and incident management,**
- **Cultural perceptions and behavioral patterns,**
- **Policy and regulatory coherence.**

A cross-case synthesis (Yin, 2018) enabled comparison of institutional responses and policy interactions. The analysis aimed to uncover how governance fragmentation and cultural inertia constrain effective cybersecurity integration in the research sector.

3.4 Limitations

Several limitations should be noted. First, cybersecurity incidents are often underreported, creating an incomplete empirical picture. Second, interviews relied on self-assessment, which may lead to social desirability bias. Third, the dynamic policy environment –particularly ongoing NIS-2 implementation – means that institutional practices evolve rapidly. These limitations are mitigated by triangulating multiple data sources and focusing on structural rather than event-specific insights.

4. FINDINGS

4.1 The Expanding Threat Landscape

The findings reveal that German research institutions have become increasingly attractive targets for cyber espionage and ransomware attacks. Since 2019, over forty universities and research organizations have suffered significant disruptions due to attacks. Although many incidents remained localized, their cumulative effect indicates systemic weaknesses in institutional cybersecurity governance. Attack vectors included phishing, ransomware, and exploitation of outdated software systems. The overall IT infrastructure of research organizations is vulnerable towards cyberattacks. IT security researchers (Shulmann/Waidner 2023) found in all 85 member universities possible attack vectors. This included known vulnerabilities of central services such as email or single sign-on. Additionally, password regulations proved insufficient or were shared. Another analysis of the state of cybersecurity within research organization concluded that the protection of the systems is not good enough. In some cases, it was even possible to access data of root users (Wolfangel/Rehme 2023).

In several international cases (Fortify 2023), threat actors were linked to state-sponsored groups, such as Russia's APT28 and China's Mustang Panda, whose goals ranged from data theft to disruption of academic operations. While there are no known cyberattacks by state-sponsored groups in Germany, the German domestic intelligence service (Bundesamt für Verfassungsschutz, BfV) warned in March 2025 selected civil society organizations including scientific institutions about potential state-controlled cyberattacks (Bewarder/Flade 2025). If successful, attacks on universities affect a large number of people due to the high number of users. Often, digital systems such as communication platforms, digital learning platforms, and certificate issuance systems are unavailable. Additionally, research data may be lost or stolen.

4.2 Organizational Fragmentation

A recurring pattern is the **decentralization of IT governance**. German universities maintain distributed IT systems managed at faculty or departmental levels. While this autonomy aligns with academic self-governance, it undermines unified security protocols. In interviews, IT officers described limited authority over research group systems and little compliance enforcement capacity outside the administrative branches of the organization This fragmentation and decentralization was noted as a significant challenge in our interviews. One person summarized it as "freedom of research and teaching. Precisely that professors do what they want and insist on this special status. [...] There is no easy way to implement measures due to this situation."

The German Rector's Conference (Hochschulrektorenkonferenz, HRK) has issued guidelines, but these are voluntary (Hochschulrektorenkonferenz 2018 & 2025). Therefore, the extent to which cybersecurity measures are implemented depends on management and department heads. A survey of universities shows that only a small number of them implement active measures to prevent cyberattacks (Stifterverband für Deutsche Wissenschaft 2024).

This fragmentation also extends to reporting lines. Cyber incidents are not consistently documented or reported to the BSI. The absence of a mandatory reporting regime, unlike in critical infrastructure sectors, contributes to weak situational awareness and risk understanding at the national level. This also complicates learning across organizations.

4.3 Cultural Resistance

The study identifies **cultural resistance** to cybersecurity measures among academic staff. Many researchers perceive security protocols as bureaucratic hindrances to scientific freedom. For example, two-factor authentication and institutional data storage policies are frequently bypassed in favor of convenience. This behavioral pattern reflects what one interviewee termed a "false sense of immunity"; the belief that academic work is too specialized to attract external threats.

This cultural dimension complicates policy enforcement. As stated before, the tension between freedom of research as well as teaching and security is seen by interviewees as an obstacle to the introduction of security measures. One person noted that the "transformation is now beginning in people's minds, because it is quite difficult, especially in the university environment," to implement more strict security measures. Another stated that there is a need for some top-down approaches since "the level of knowledge is poor. [...] Professors are [...] specialists. So they deal with their own very narrow field of expertise, and if it doesn't happen to concern cybersecurity, then they don't know much about it, they don't get much information on the side, but only what is given to them, and I think they are given very little."

Additionally, one person mentioned that "information security was simply ignored for many years in the university environment. And now the management levels also have to learn to become aware of their responsibility." This reflects the requirement of willingness to learn about the respective risks in a research environment. And consequently, the willingness on the management level to implement security measures.

4.4 Policy Gaps and Legal Ambiguity

At the policy level, the integration of cybersecurity into research governance remains incomplete. The German Constitution guarantees academic freedom under Article 5(3), limiting direct state intervention in university operations. This autonomy has historically shielded universities from rigid regulation, but now hinders coherent cybersecurity governance.

The introduction of the **EU's NIS-2 Directive** (2022) represents a potential turning point by classifying "research" as a critical sector. However, Germany's implementation restricts applicability to research institutions with commercial purposes—thereby excluding most universities and publicly funded institutes. As a result, the vast majority of the research ecosystem remains outside formal cybersecurity regulation.

Interviewees mentioned this as a possible lever for aiming towards a better security level and to hold them more accountable. As one person stated, "that's the dilemma, because you also mentioned regulators. A data protection officer must be appointed. I have clearly defined the tasks, and although we all know that we need secure information, not all universities have yet understood that they really need to create a position for this and not wait until someone is sent to them. [However,] there is no law that requires me to do this."

4.5 International Comparison

Comparative analysis shows that other EU countries and allies have begun integrating research security into national cybersecurity frameworks. For instance:

- **Estonia** enforces a comprehensive Cybersecurity Act (2023), integrating universities and higher school education into the act. This involves mandating audits and reporting duties for universities.
- **The United Kingdom** has introduced a "Trusted Research" framework that integrates cybersecurity, export control, and ethics in a unified framework, guided by the National Cyber Security Centre (NCSC). This combines awareness training with national guidance.
- **The United States** relies on grant-based cybersecurity compliance (e.g., National Institute of Health (NIH) and National Science Foundation (NSF) requirements) but faces underfunding and uneven implementation.

Germany's approach, by contrast, remains fragmented between state-level higher education laws and federal cybersecurity policies, thereby creating governance blind spots.

4.6 Case Studies Overview

1. University of Potsdam (2024):

The university's email system was taken offline for several weeks following an attack from outside the organization. Although a separate phishing attempt occurred in close temporal proximity, there is no clear indication that it was connected to the external attack.*

2. University of Duisburg-Essen (2022):

A ransomware attack by the group *Vice Society* encrypted servers and student data. The attack led to a shutdown of the complete IT infrastructure. The restoration process lasted over six months and cost approximately €1.7 million.

3. Fraunhofer Institute for Microstructure of Materials and Systems (2022):

A ransomware incident led to data leaks on the dark web, underscoring risks in applied research institutions closely collaborating with industry. Encrypted data could not be restored fully.

Across these cases, delayed detection, fragmented response coordination, and limited backup capabilities were recurring problems. In severe cases, IT infrastructure was not available to students and staff for months. This led to problems with communication, collaborative working, enrollment, and the issuance of certificates and transcripts. The Technical University Berlin (Team Datenschutz der TU Berlin 2022) for example, needed more than a year to return to a normal state of their IT systems. Institutions with preexisting cybersecurity frameworks recovered faster and minimized data loss.

* In an earlier version, the text indicated that the external and the phishing attack were related. In hindsight, this does not seem to be the case.

5. DISCUSSION AND POLICY IMPLICATIONS

5.1 Interpreting the Findings through a Governance Lens

The empirical findings reveal a persistent misalignment between the governance of research institutions and the demands of cybersecurity resilience. German universities and public research organizations operate within a federated, decentralized framework emphasizing academic autonomy and institutional self-governance. This design promotes diversity and innovation but weakens the coherence of cybersecurity strategy. The absence of binding standards across the sector fosters fragmentation, leaving institutions vulnerable to asymmetric threats from both cybercriminals and state actors.

From a governance perspective, this fragmentation reflects what Pierre and Peters (2000) describe as "hollowed-out governance", where responsibilities are distributed among multiple semi-autonomous entities, yet coordination mechanisms remain weak. Cybersecurity thus becomes an "everybody's problem and nobody's responsibility." This is exemplified by the differences within the individual *Länder* dealing with the issue. Some of them provide services, resources, and guidance to their universities to implement better cybersecurity measures, while others do not. In those *Länder*, universities are on their own when it comes to cybersecurity.

Integrating cybersecurity into science governance requires not only compliance mechanisms but also cognitive and normative change. Academic institutions must recognize security as an enabler of research integrity rather than as an external constraint.

5.2 Academic Freedom and Legal Constraints

Germany's constitutional guarantee of academic freedom (Art. 5(3) Basic Law) presents both a foundation and a constraint for cybersecurity policy. While it protects scientific inquiry from state interference, it also limits the imposition of centralized IT security mandates. The policy discussion around research security is probably best described with the metaphor of a "protected openness" *(geschützte Offenheit)*; a framework that preserves collaboration while embedding risk awareness and data governance.

However, the current legal ambiguity allows universities to interpret cybersecurity obligations unevenly. Unlike data protection, which is governed by the GDPR and institutional Data Protection Officers, cybersecurity lacks a comparable legal anchor in academia. The implementation of the NIS-2 Directive could have partially closed this gap, yet its narrow definition of "research institutions" leaves much of the publicly funded research landscape outside formal coverage.

This legal asymmetry undermines consistency: while some institutions (e.g., Fraunhofer Institutes) fall under regulatory scrutiny due to their industrial engagement, others (e.g., Max Planck or university research units) remain unregulated despite comparable risk exposure. Some of the *Länder* have addressed the issue in their cybersecurity strategies such as North Rhine-Westphalia, Baden-Württemberg and Baveria. North Rine-Westphalia also dedicated additional funding to universities to strengthen their security posture. Baveria set requirements and measures for the period 2023-2027 for the group of public universities. Aligning cybersecurity governance with academic autonomy thus demands a differentiated approach. One that distinguishes between institutional missions while maintaining common baselines.

5.3 Cultural Transformation and Institutional Learning

Technical defenses alone are insufficient. The empirical evidence highlights the importance of fostering a **cybersecurity culture** that permeates all organizational levels. Cultural change requires leadership commitment, continuous training, and clear accountability. Initiatives such as ENISA's *Cybersecurity Culture Framework* provide guidance but must be localized for academic contexts.

Three cultural levers emerge from the data:

1. Leadership Signaling:
Senior management must communicate cybersecurity as a strategic priority rather than an IT concern.

2. Incentive Structures:
Security compliance should be integrated into performance indicators, funding conditions, and audit criteria.

3. Peer Norms:
Researchers should view secure practices like encryption or controlled data sharing as integral to "good scientific practice."

Embedding these elements requires what Argyris and Schön (1978) call *double-loop learning*; questioning underlying assumptions rather than merely adjusting procedures. Only through iterative learning processes can institutions transition from reactive defense to proactive resilience.

Available empirical data shows that German universities are lacking in this regard. Security measures to foster a cybersecurity culture within the ecosystem are not being implemented good enough. While the importance of the issue is increasingly recognized, the risk is often seen as being in other organizations rather than one's own. Furthermore, the level of security measures is often considered to be higher within one's own organization than within others. This creates a false sense of security (Stifterverband für die Deutsche Wissenschaft (2024). Interviews showed that often measures and processes have be initiated. However, the level of implementation is not where it should be. This is often due to unclear responsibilities, a lack of binding requirements, and insufficient resources.

5.4 The European Dimension: Harmonization and Research Security

At the EU level, the intersection of research policy and cybersecurity is gaining salience. The Council's 2024 *Recommendations on Research Security* explicitly acknowledge hybrid threats – including espionage and digital interference – as risks to academic integrity. The EU's *Horizon Europe* program now includes clauses on cybersecurity and data governance in funding agreements.

Nevertheless, implementation remains fragmented across member states. While the EU provides coordination and regulatory templates (e.g. NIS-2, Cyber Resilience Act), actual enforcement lies with national authorities. Germany's delayed transposition of NIS-2 and lack of clear mandates for universities illustrate this tension between European aspiration and national execution. A coherent science policy response would require harmonizing legal definitions of "research entities" and integrating cybersecurity into existing instruments such as the German *Wissenschaftsrat* recommendations or the *HRK* guidelines.

There is also a need to streamline legislation on the *Länder* level. While some of the Higher Education Acts on the regional level address the necessity to handle sensitive research responsibly, taking into account potential consequences or unintended use, others do not.

5.5 Policy Recommendations

Based on the analysis, five policy priorities emerge:

1. Institutional Governance Reform:

Mandate each university and public research institution to establish a Chief Information Security Officer (CISO) reporting directly to leadership. Encourage the adoption of standardized Information Security Management Systems (ISMS) aligned with ISO 27001 or equivalent.

2. Funding-Linked Compliance:

Integrate cybersecurity criteria into federal and EU research funding requirements. Institutions should demonstrate compliance with security protocols as part of grant eligibility.

3. Capacity Building and Training:

Develop national training programs for researchers and IT personnel. Introduce "cyber hygiene" modules in graduate education, akin to existing ethics and data protection courses.

4. Legal Clarification and Integration:

Define the boundaries between academic freedom and cybersecurity obligations through amendments or interpretative guidance under German higher education law.

5. Cross-Sector Collaboration:

Establish a standing "Research Security Council" bringing together ministries, research associations, and intelligence agencies to facilitate knowledge exchange and threat assessment.

5.6 Toward a Resilience-Based Science Policy

Cybersecurity in research should be reframed as an element of **scientific resilience**; the ability of institutions to maintain core functions and trust even under attack. This concept aligns with broader shifts in EU and German policy toward resilience as a governance paradigm (Boin & Lodge, 2020). Rather than emphasizing compliance alone, resilience underscores adaptability, learning, and recovery.

For science policy, this means:

- Embedding cybersecurity in risk management and crisis governance frameworks.
- Viewing research infrastructures as components of national critical infrastructure.
- Strengthening inter-institutional solidarity—sharing best practices, incident data, and recovery protocols.

By positioning cybersecurity within resilience policy, Germany can transform vulnerability into institutional learning and policy innovation.

Cybersecurity in research is not a technical add-on but a governance imperative. The German science system's openness, while foundational to its success, must evolve toward structured protection. Policy reforms should aim to integrate cybersecurity into the ethics, governance, and funding architecture of academia without eroding freedom of inquiry.

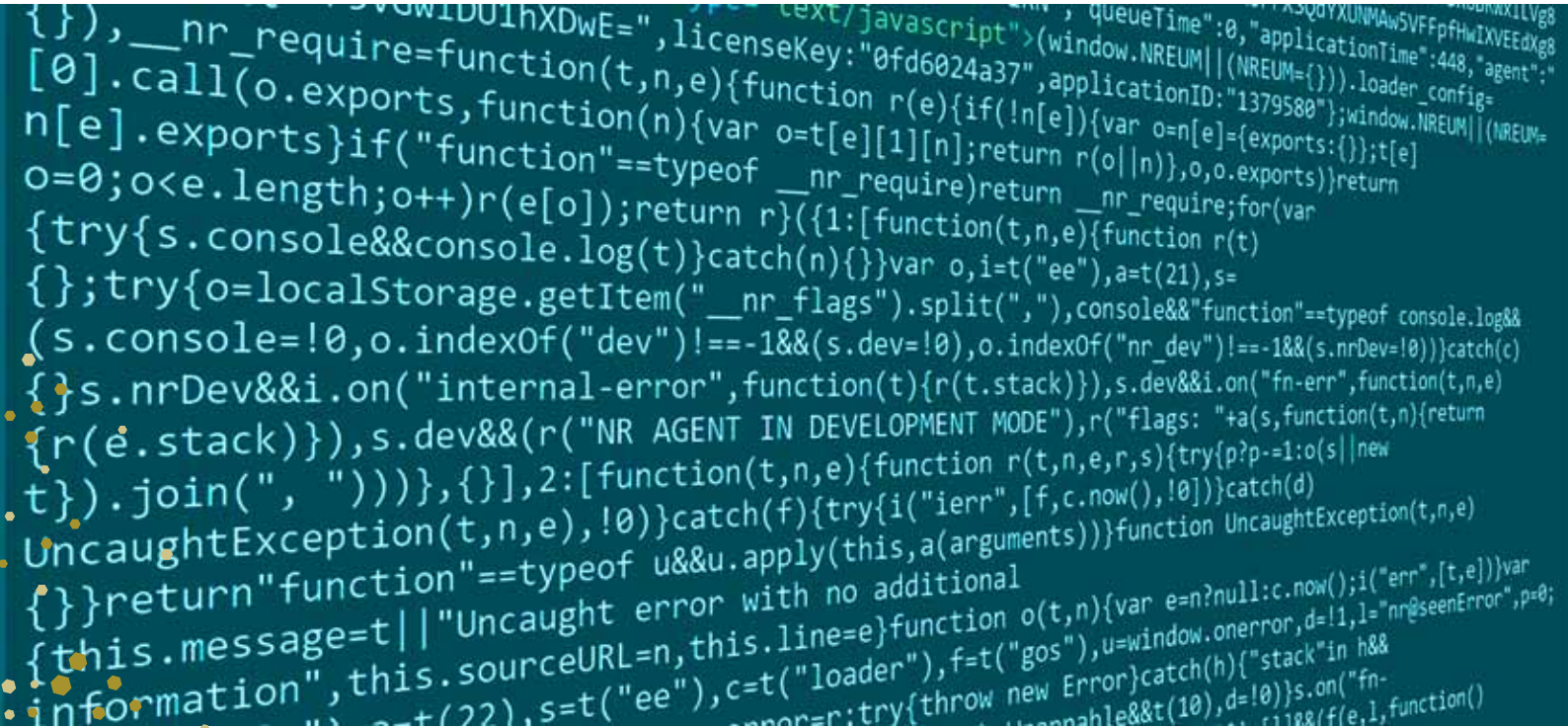
Achieving this balance demands a cultural and institutional shift: recognizing that secure science is not less open, but more sustainable. A future-proof science policy will ensure that Germany's research institutions remain globally connected yet resilient against the strategic exploitation of openness.

6. CONCLUSION

This paper examined cybersecurity governance in German universities and research institutions through the lens of science policy. The findings illustrate that the open, decentralized structure of German academia – while essential for scientific creativity – produces vulnerabilities when confronted with increasingly sophisticated cyber threats. Empirical evidence shows that universities and research institutes face recurring cyberattacks, yet their responses remain fragmented due to legal ambiguity, cultural resistance, and limited coordination between governance levels.

The analysis demonstrates that cybersecurity in science is not merely an IT issue but a matter of institutional governance, organizational culture, and national policy coherence. Strengthening resilience requires embedding cybersecurity principles within the values and practices of academia. This implies developing clear accountability structures, aligning funding incentives with security compliance, and integrating cybersecurity into research ethics and integrity frameworks.

Ultimately, achieving balance between openness and protection calls for a paradigm shift in science policy from reactive defense to proactive resilience. German and European policymakers must treat research infrastructures as components of critical societal systems, safeguarding not only data but also the credibility and autonomy of scientific knowledge. In an era of geopolitical uncertainty and hybrid threats, resilient science governance is essential for preserving both academic freedom and societal trust in research.



Quelle: Shutterstock

ACKNOWLEDGEMENT

We want to thank Kai Pascal Beerlink and Liv Rodefeld for their research support for this paper. We also want to thank all the people who were open to talk about cybersecurity within the German research context and everyone who gave us an international perspective.

REFERENCES

Argyris, C., & Schön, D. (1978) Organizational learning: A theory of action perspective. Reading, MA: Addison-Wesley.

Bewarder, M., & Flade, F. (2025) 'Verfassungsschutz warnt deutsche NGOs vor Ausspähung', Tagesschau: https://www.tagesschau.de/investigativ/ndr-wdr/cyberspionage-russland-ngo-100.html.

Bijker, W. E., Hughes, T. P., & Pinch, T. J. (Eds.) (1987) The social construction of technological systems: New directions in the sociology and history of technology. MIT Press.

Boin, A., & Lodge, M. (2020) 'Designing resilient institutions for transboundary crisis management: A time for public administration', Public Administration, 98(2): 492–505.

Braun, V., & Clarke, V. (2006) 'Using thematic analysis in psychology', Qualitative Research in Psychology, 3(2): 77–101.

Council of the European Union (2024) Council Recommendation of 23 May 2024 on enhancing research security.

Der Spiegel (2022). ‚Hacker erpressen die Universität Duisburg-Essen': https://www.spiegel.de/netzwelt/web/universitaet-duisburg-essen-hacker-erpressen-die-hochschule-a-ec8b93b2-8111-417c-bf14-e7e933d47732.

European Union Agency for Cybersecurity (ENISA). (2023) Cybersecurity culture in organizations: Implementation guide. Athens: ENISA.

European Parliament, Council of the European Union (2022). Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive).

Fortify (2023) Threat Groups Actively Targeting Higher Education Institutions: https://fortifydata.com/threat-advisory/threat-groups-targeting-higher-ed/.

Forschung & Lehre (2024) ‚Folgen der Cyber-Attacke auf die Uni Potsdam': https://www.forschung-und-lehre.de/management/folgen-der-cyber-attacke-auf-die-uni-potsdam-6802.

Felden, E., Petersmann, S. & Conrad, N. (2022) 'Are European Academics Helping China's Military?', Deutsche Welle: https://www.dw.com/en/are-european-academics-helping-chinas-military/a-61834716.

Jasanoff, S. (2004) States of knowledge: The co-production of science and the social order. Routledge.

Hochschulrektorenkonferenz (2018) Empfehlung der 25. Mitgliederversammlung der HRK am 06. November 2018 in Lüneburg - Informationssicherheit als strategische Aufgabe der Hochschulleitung.

Hochschulrektorenkonferenz (2025) Empfehlung der 40. Mitgliederversammlung der HRK am 13. Mai 2025 in Magdeburg - Handlungsdruck für Hochschulen, Länder und Bund – HRK-Empfehlungen zur Cybersicherheit.

Joske, A. (2019) The China Defence Universities Tracker: Exploring the military and security links of China's universities. Australian Strategic Policy Institute.

Kello, L. (2017) The virtual weapon and international order. Yale University Press.

Nowotny, H. (2008) Insatiable curiosity: Innovation in a fragile future. MIT Press.

Pierre, J., & Peters, B. G. (2000) Governance, politics and the state. Macmillan.

Rappert, B., & Gould, C. (Eds.). (2009) Biosecurity: Origins, transformations, and practices. Palgrave Macmillan.

Rid, T. (2020) Active measures: The secret history of disinformation and political warfare. Farrar, Straus and Giroux.

Roth, M. (2022) ‚Wie es nach dem Hackerangriff am Fraunhofer-Institut in Halle weitergeht', MDR: https://www.mdr.de/nachrichten/sachsen-anhalt/halle/halle/hackerangriff-fraunhofer-institut-daten-darknet-lka-update-100.html.

Shulmann, H., & Waidner, M. (2023) ‚Forschung muss besser geschützt werden', Forschung & Lehre: https://www.forschung-und-lehre.de/detailview/forschung-muss-besser-geschuetzt-werden-5449.

Specht, F. (2025) ‚Hackerangriff auf die Universität der Bundeswehr', Handelsblatt: https://www.handelsblatt.com/politik/deutschland/cyberkriminalitaet-hackerangriff-auf-die-universitaet-der-bundeswehr/100107638.html.

Stifterverband für die Deutsche Wissenschaft (2024) Hochschul-Barometer 2024. Lage und Entwicklung der Hochschulen aus Sicht ihrer Hochschulen aus Sicht ihrer Leitungen. Ausgabe 2024.

Team Datenschutz der TU Berlin (2022) ‚TU Berlin: Nach einem Jahr sind die Auswirkungen des IT-Sicherheitsvorfalls weitgehend überwunden', TU Berlin: https://blogs.tu-berlin.de/datenschutz_notizen/2022/05/31/tu-berlin-nach-einem-jahr-sind-die-auswirkungen-des-it-sicherheitsvorfalls-weitgehend-ueberwunden/.

Wolfnagel, E., & Rehme, R. (2023) ‚Noten und Atteste frei zugänglich: Wir haben die IT-Sicherheit von Unis und Hochschulen getestet', RiffReporter: https://www.riffreporter.de/de/technik/hacking-datenschutz-ransomware-hochschulen-universitaeten-daten-im-netz-it-sicherheit.

Yin, R. K. (2018) Case study research and applications: Design and methods (6th ed.). Sage Publications.

BIGS

BRANDENBURGISCHES INSTITUT
für GESELLSCHAFT und SICHERHEIT

Hanna Denecke *is a political scientist and Research Fellow at BIGS.*

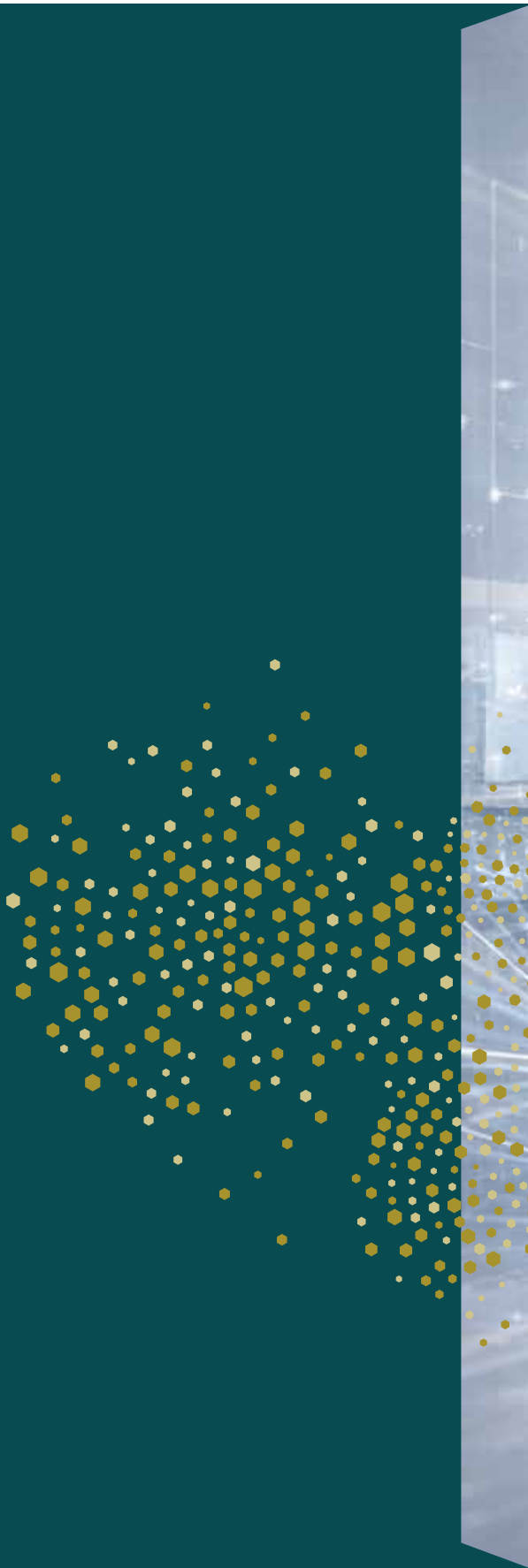
Esther Kern *is a political scientist and Fesearch Fellow at BIGS.*

Andreas Könen *is a mathematician and Non-Resident Senior Fellow at BIGS.*

Nadine Nagel *is an industrial engineer and Visiting Fellow at BIGS.*

Prof. Dr. Tim Stuchtey *is an economist and the Executive Director of BIGS. Additionally, he is Professor of the Economics of Cybersecurity at the German University of Digital Science.*

Located in Potsdam, the ***Brandenburg Institute for Society and Security*** *is an independent, non-partisan, non-profit organization with an inter- and multidisciplinary approach with a mission to close the gap between academia and practice in civil security.*



www.bigs-potsdam.org