CIVITAS EUROPE

A VEKTOR GROUP COMPANY

ATTACK ON CRITICAL INFRASTRUCTURE

Command capability is essential for a resilient response

Hagen Peukert

WHITE PAPER · NOVEMBER 2026

3 November 2026

Publisher: CIVITAS Europe

A Vektor Group company · civitas-europe.de

1. Critical infrastructure: Vulnerable cogs in an open society

The number of recorded incidents worldwide aimed at disrupting, paralysing or destroying existing installations and facilities is rising. Cyberattacks against public institutions, government agencies or companies, carried out by criminals and/or state actors, the physical destruction of power grids, the disruption and temporary paralysis of transport networks and hubs, as well as externally directed sabotage[1], disinformation and manipulation all add to the everyday dangers and risks arising from accidents, incidents that cause damage and natural disasters in a highly industrialised and globally interconnected society. Bitkom's *Wirtschaftsschutz 2025* study puts total losses from theft, espionage and sabotage at €289.2 billion, with cyberattacks accounting for 70 per cent.[2] The consequences of extensive urban sprawl, regulated natural areas and climate change are occurring in ever quicker succession, posing significant challenges for resilience and crisis response.

In addition to the sometimes severe disruption caused by the suspension of day-to-day operations or restrictions on mobility, the financial damage is enormous.

Russia's war against Ukraine shows how the destruction of critical infrastructure is used in an attempt to defeat a society and a sovereign state militarily or destabilise them from within. The strategy is to deprive them of critical infrastructure, their lifeline and the foundation of public and individual life.

Whether in war and hybrid scenarios or in the aftermath of disasters and major incidents, protecting critical infrastructure affects everyone and is a responsibility for society as a whole.

The Critical Infrastructure Umbrella Act (*KRITIS-Dachgesetz*), adopted in 2026, established a legal framework for strengthening the physical resilience of critical facilities.[3] Which facilities are covered and when individual obligations apply are determined by the Act and the regulation that sets out its details.[4] Operators of critical facilities are required to take measures to strengthen their resilience. These include preparing and implementing resilience plans that set out, on the basis of the operators' risk analyses and assessments, the appropriate and proportionate technical, security and organisational measures taken to strengthen resilience.[5]

Authorities and public and private operators face compliance costs and obligations whose specifics depend on the applicable legal framework. The data collected in this connection also require protection.

The Federal Office of Civil Protection and Disaster Assistance (BBK) performs functions under the Critical Infrastructure Umbrella Act, including the registration of critical facilities. Alongside physical protection, this increases the importance of keeping baseline data up to date and analysing the results of inspections and identified vulnerabilities.

The BBK and the Federal Office for Information Security (BSI) perform functions within their respective statutory remits. Operational command in disaster management is governed by state law and local responsibilities.

Germany's federal system and the structures that follow from it nevertheless provide for a wide range of responsibilities and actors, both governmental and non-governmental, within and across levels of government when responding to major incidents and disasters. Some procedures for cooperation, assumption of responsibility and joint management are formally regulated. In practice, however, command structures, responsibilities and response measures have to be established afresh each time, creating recurring pressure to make ad hoc adjustments that above all cost time.

Diffuse responsibility, a focus on individual organisations' resources and other considerations often impede the mobilisation, initiation and implementation of fully coordinated measures. The final report on the so-called Ahr Valley disaster[6] and the findings from the COVID-19 pandemic highlight both the shortcomings and, above all, the immense challenges facing leaders and decision-makers. This is particularly true when multiple, complex incidents with secondary and knock-on effects unfold in parallel and/or at different times, and sound decisions have to be made quickly using the information available, which may have been inadequately shared.

The following figure[7] uses Germany's cybersecurity architecture to illustrate the evident complexity and many layers of authorities and actors with responsibility. The number of bodies involved increases the coordination required to establish a common operational picture. This inevitably raises questions about who must respond, when, with what resources and who should take the lead. In disasters and following major incidents, everyone involved faces similar coordination tasks. Resolving these questions takes valuable time. Essential information may be overlooked, making it harder to reach sound decisions.

Cybersecurity architecture

Overview · Enlarged detail views on pages 11–16

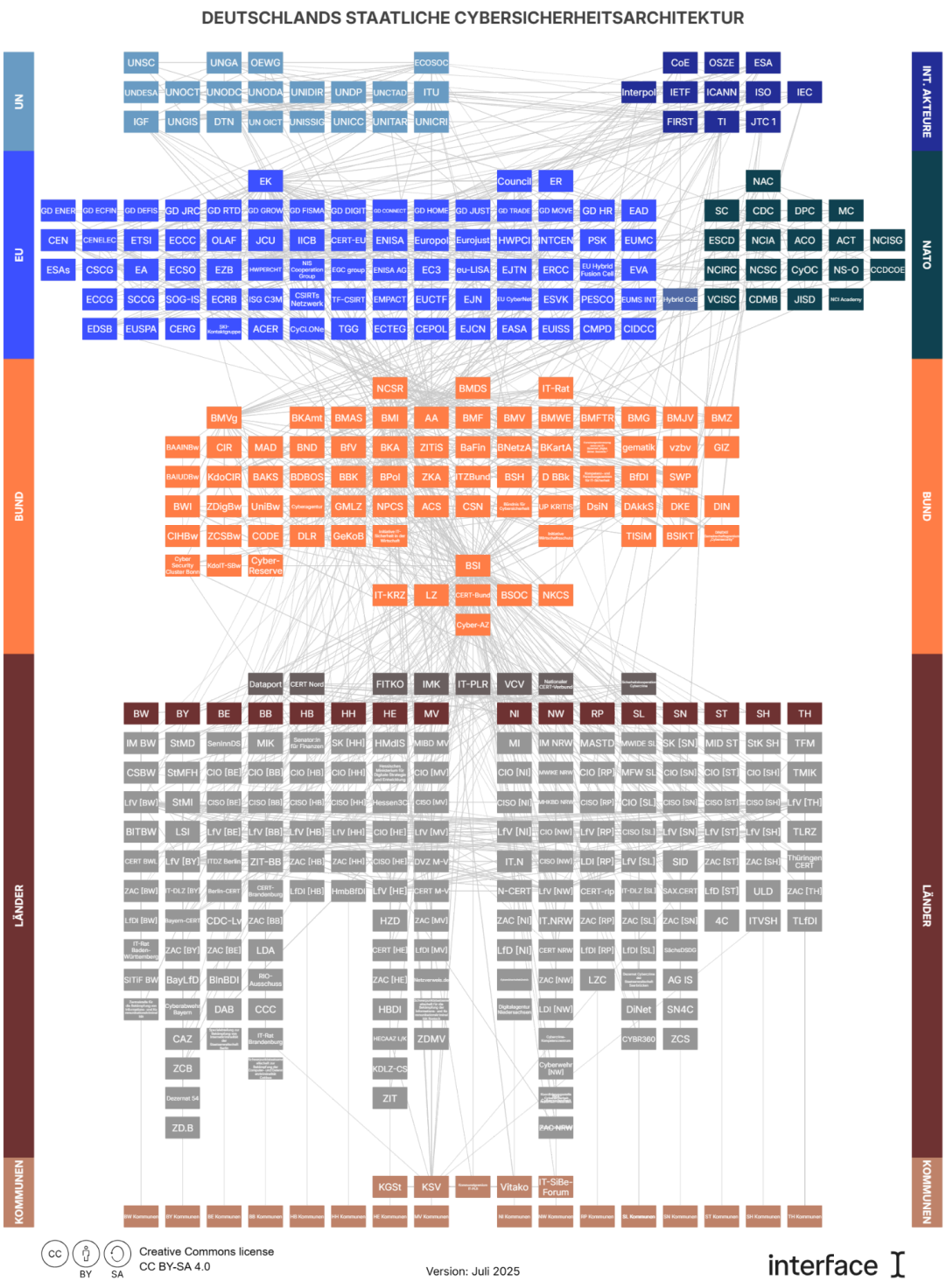


Figure 1 · interface · July 2025 version · CC BY-SA 4.0.

The overview shows the interconnections. Please refer to the appendix for individual entries.

Interactive source: cybersicherheitsarchitektur.de

By 2022 at the latest, the security situation in Europe had fundamentally changed. Critical infrastructure resilience is now also considered from a military perspective and incorporated into military defence planning. Even in the face of physical threats and destruction, the state and society must be able to function, withstand the impact and preserve their existence. The Operations Plan for Germany also takes into account the protection of infrastructure essential to defence.[8] Its relationship to the Critical Infrastructure Umbrella Act must be considered in the context of the relevant responsibilities and legal framework.

2. Are we well prepared for complex and rapidly changing situations?

Even in the absence of open hostilities, multiple major incidents, potentially with hybrid causes and with parallel or successive follow-on events and effects, place considerable demands and strain on staff and leaders with decision-making authority. A fictional example follows.

The figures and events below are assumptions for a fictional scenario. They do not constitute a forecast or an assessment of the site's actual safety. In a fictional scenario based on BASF's Ludwigshafen site, a chemical processing complex is assumed to employ about 35,000 people. Several explosions occur there, causing more than 7,000 casualties and releasing highly toxic pollution. This in turn requires the evacuation of more than 250,000 residents from a metropolitan area whose boundaries must be determined, forces the suspension of inland navigation and requires the closure of the airspace. A persistent temperature inversion prevents any significant exchange of air. Remaining in the area poses a health hazard to residents and emergency responders. Electricity and energy supplies have to be significantly restricted, either temporarily or permanently. Evacuation, shortages and police measures lead to social conflict in some areas, which in turn leads to disinformation campaigns on social media involving deepfakes and false information. The closure of transport routes for days disrupts supply chains, causing production outages outside the disaster area. Reports of drone overflights and indications of sabotage lead to a widening of the investigations…

Against the backdrop of this only partially sketched scenario, everyone involved and all experts face the decisive question of how a single command and response team, or more likely several, can make sound decisions under extreme time pressure and an urgent need to act, while physical exhaustion gradually increases and psychological strain persists. They must contend with a multitude of reports, leads, contradictions, uncertainties, data from diverse and often unverified sources, communication errors, assumptions and hypotheses from staff teams, options, and the expectations of an impatient and sometimes critical public. How can increasingly complex operational processes be directed and coordinated in crisis mode?

What, then, do incident response teams and crisis managers need?

The Green Paper submitted to the Federal Government in 2023 states:

> *In light of past experience and future challenges, the development of a round-the-clock, real-time interdisciplinary operational picture for Germany using forward-looking technologies is overdue as a basis for command and crisis management.*[9]

- The implementation of the Critical Infrastructure Umbrella Act can be expected to generate additional relevant data. Structured baseline data, updated measurement data and regular assessments and analyses provide the basis for a shared understanding of the situation.
- In a crisis or major incident, the operational and information picture will draw on these baseline data and rely increasingly on current incident data generated at different speeds and with varying levels of quality by a wide range of sources and sensors. To date, this has generally been handled using analogue processes, with people performing manual “swivel-chair” tasks for analysis and coordination.
- Friction still regularly arises from a focus on individual organisations’ resources and from silo thinking. This may recognise and emphasise the importance of each organisation’s own role, but it hinders the efficient development of a complete overview and an understanding appropriate to the situation. Data protection requirements across levels of government can in some cases delay or even interrupt the flow of information.
- Incident response teams are often formed ad hoc. Qualifications and experience in dealing with contradictory, incomplete and overlooked information vary, yet they determine the quality of command decisions and actions. Staff teams tire and need rest periods. Many responders work on rotation and serve as volunteers. Their level of professional proficiency for the task may vary.
- The Federal Agency for Technical Relief (THW), volunteer fire brigades, the German Red Cross (DRK) and related organisations such as Johanniter, Malteser and Arbeiter-Samariter-Bund rely heavily on volunteers. Holding multiple roles can create competing obligations in an emergency. It therefore needs to be established who can reliably commit to roles in situation assessment and command and has the training to perform them. This makes it harder to respond and act quickly and effectively.
- Recording the relevant memberships and skills requires a sound legal basis and compliance with data protection requirements.[10]

It is worth noting in passing that companies outside the scope of the Critical Infrastructure Umbrella Act also face comparable resilience requirements. Depending on their activities and the applicable legal framework, they are also subject to other statutory obligations. Potential scenarios present them with challenges that often threaten their very survival within a short time.

Beyond the purposes provided for by law, the question arises of how lawfully available data can be used to create a common operational picture. This requires, among other things, a defined, practised, equipped and professional command organisation. Several options are available, subject to federal, geographical, functional, organisational and, importantly, financial conditions and requirements.

3. Preventing poor crisis management from triggering a crisis of state and a loss of control

Command capability is indispensable in a crisis or disaster involving multiple, complex and sometimes fundamental threats, or even in war. Its importance extends well beyond the event itself.[11]

Poor crisis management based on inaccurate, delayed and incomplete information affects the immediate response and increasingly leads to political repercussions and public frustration. Citizens of a highly developed industrial country expect their democratically elected officeholders, who very often lead crisis and disaster response teams, to be able to respond and act and to manage crises well.

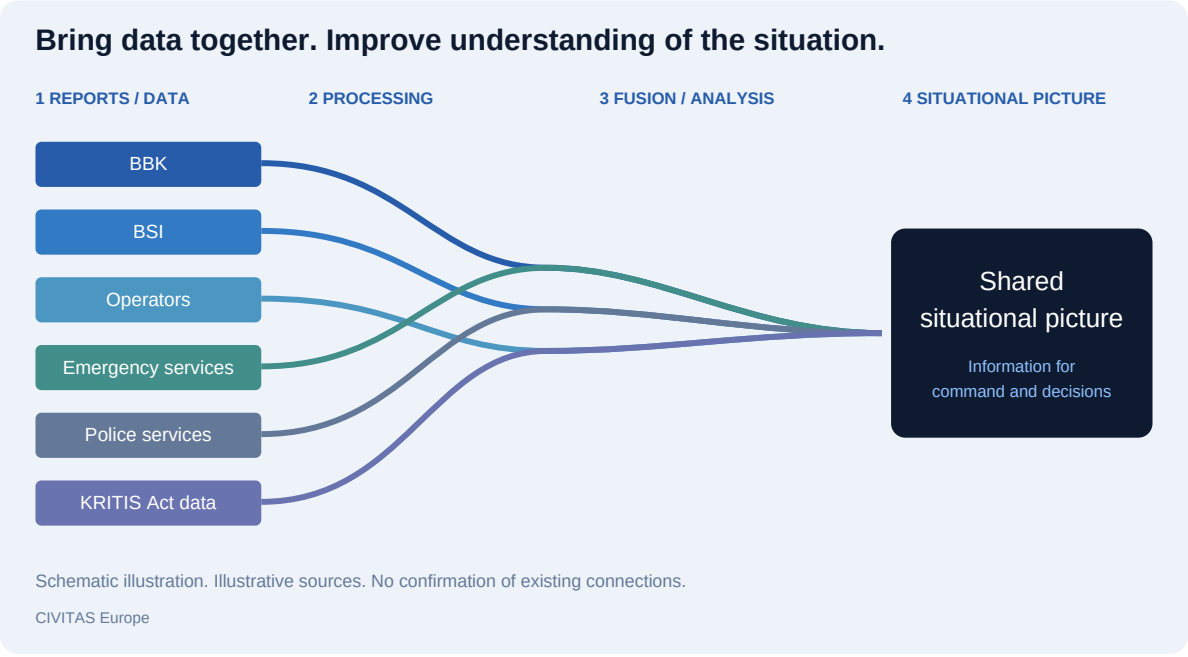
Where this capacity is lacking, there is a risk of losing public trust, which can erode many citizens' confidence in the state and lead to disillusionment and disengagement. The state and its institutions must, and can, ensure that damage to the resilience of critical infrastructure and to the safeguards for essential areas of life does not escalate into a crisis of the state and its institutions.

This calls for acquiring and expanding capabilities for political leaders and state institutions so they can respond quickly, appropriately and comprehensively in disasters, crises and war.

4. Modern technology strengthens resilience and crisis response

The good news is that a manageable yet comprehensive and coordinated approach makes it possible to develop a technological solution for the functional shortcomings and requirements identified above. Such a solution can also meet the need for a high degree of data sovereignty and control.

- Modern, readily available information and data processing combines existing, often structured baseline data, such as those to be generated under the Critical Infrastructure Umbrella Act, with current incident and measurement data. Inputs from a wide range of actors and sensors, together with data, descriptions, analyses and statements, form a unified, multilayered operational picture that can be traced at any time.
- Open-source information (OSINT) takes on new and significant importance in this context. News, images and instructions can all be analysed comprehensively and processed consistently at high speed. In a society where almost everyone has a mobile device, this is a significant source of information.
- Artificial intelligence helps structure large volumes of data and enables existing applications to be used and integrated with one another. A modular structure supplies the necessary information vertically and horizontally across all identified levels.
- Situation centres and decision-makers can receive continuously updated operational information. Timeliness, quality and availability depend on data sources, permissions and operating conditions. Automated, integrated and adaptable analytical applications can thus support decision-making and command with minimal delay.



Schematic illustration of how data from different reports and contributions are processed and fused in an open, scalable architecture. The organisations and datasets shown are examples of sources. The graphic does not indicate any existing technical connections.

- This reduces the strain on staffing resources. Conventional “swivel-chair” interfaces, often staffed by willing volunteers with varying qualifications, can be reduced, or the people staffing them can gain access to reliable, redundant and up-to-date reports and processed information. Decisions can now draw on a breadth of information of standardised quality that was previously unavailable, along with clear recommendations for action based on personnel and resources, space and time, and above all on visualisation and the analysis of threats and influencing factors. Worst-case scenarios can now be assessed using data.
- The modular design and open architecture allow a wide range of actors and responsible bodies to be included and connected regardless of level or across levels. Access to relevant information, or its basic availability, gives people at all levels greater confidence in their decisions and actions. A deep and broad understanding of the situation therefore helps people make sound decisions and act more quickly on site, in incident response teams and in decision centres.
- Scenarios and situations can be simulated with “real” data to prepare and support preventive measures. All levels benefit from deeper understanding and better preparation.

Future crisis response capabilities aimed at restoring and preserving critical infrastructure and areas of public life require superior command capability. Long available in a military context, modern information and data fusion has become indispensable in complex and hybrid crisis and disaster scenarios that unfold in rapid succession.

And it is available. In Germany, for its protection and preservation.

Sources and endnotes

1. According to the IISS, the number of confirmed Russian acts of sabotage against Europe's critical infrastructure rose by 246 per cent from 2023 to 2024. Charlie Edwards and Nate Seidenstein, *The Scale of Russian Sabotage Operations Against Europe's Critical Infrastructure*, August 2025, p. 9. IISS report

2. Bitkom, *Wirtschaftsschutz 2025*, summary. Study report

3. German Bundestag

4. BBK, FAQ on the Critical Infrastructure Umbrella Act, accessed 3 November 2026. BBK FAQ

5. German Bundestag

6. Final report on the flood disaster

7. interface, *Germany's Government Cybersecurity Architecture*, July 2025 version. Original graphic licensed under CC BY-SA 4.0, with enlarged excerpts in the appendix. Original graphic · Licence

8. Operations Plan for Germany

9. Zukunftsforum Öffentliche Sicherheit, from the Green Paper on the real-time interdisciplinary operational picture, March 2023.

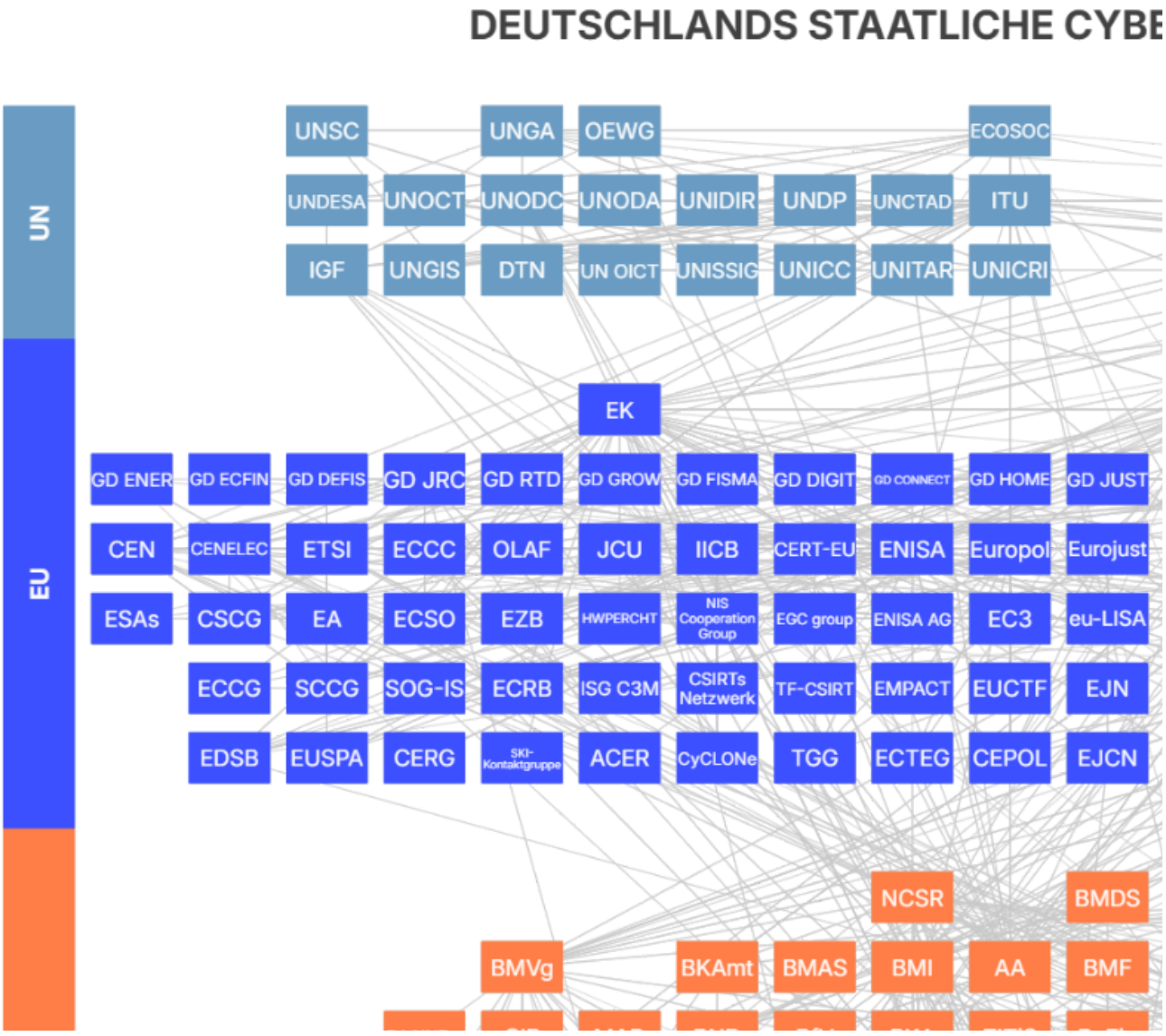
10. Section 26 of the Federal Data Protection Act. On the issue of multiple roles, see Julia Egleder, *Bereit für den Ernstfall?* [Ready for an Emergency?], *loyal*, 2 February 2026. Section 26 · Article

11. See the 2023 Green Paper on the interdisciplinary operational picture.

Figure 1 · Detail 1 of 6

Upper section · Left half

Unaltered excerpt from the original graphic. Adjacent areas overlap.



Position in the overview

1	2
3	4
5	6

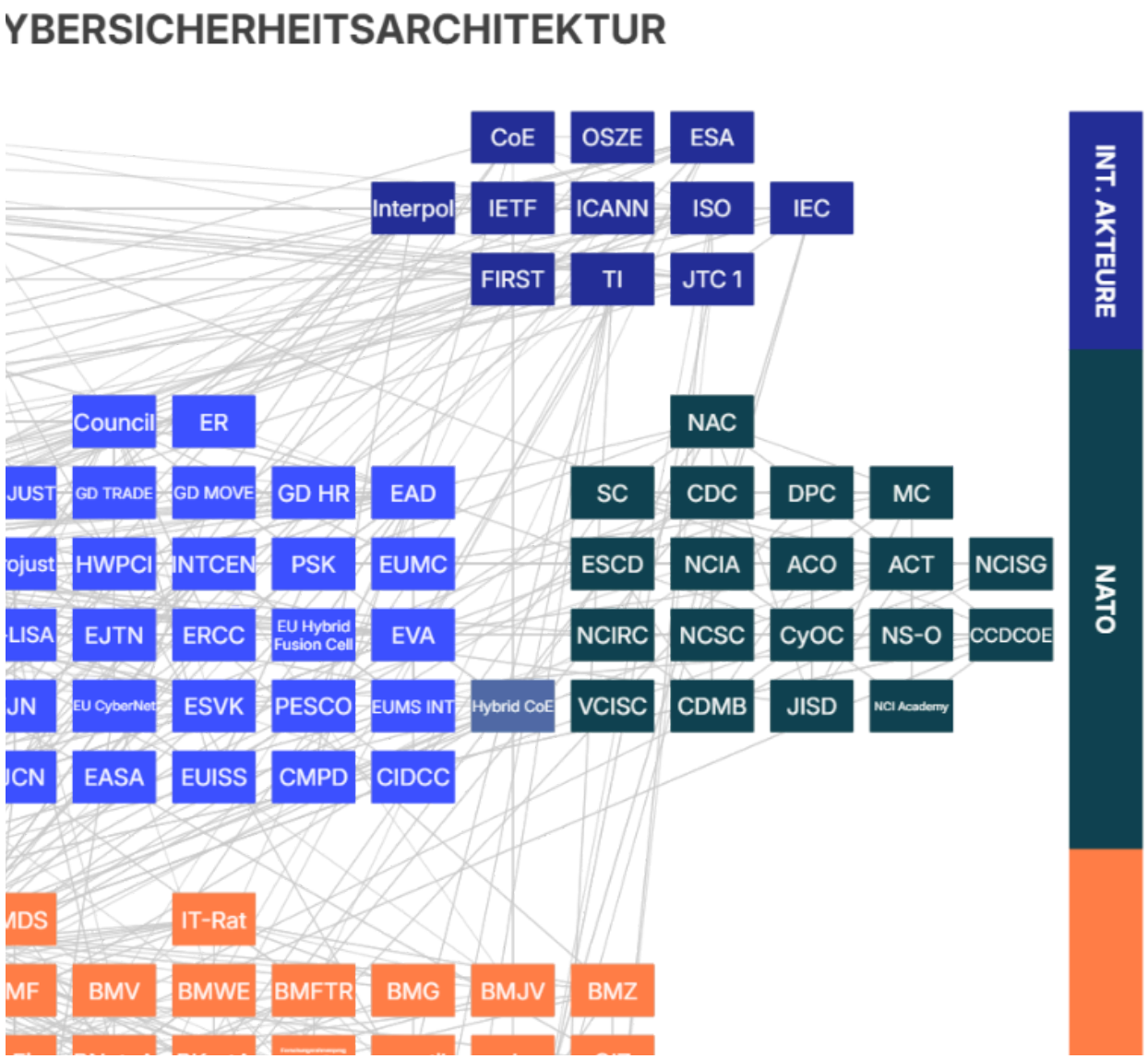
Return to the overview on page 4.

Source: interface · cybersicherheitsarchitektur.de · Version used in the original white paper

Figure 1 · Detail 2 of 6

Upper section · Right half

Unaltered excerpt from the original graphic. Adjacent areas overlap.



Position in the overview

1	2
3	4
5	6

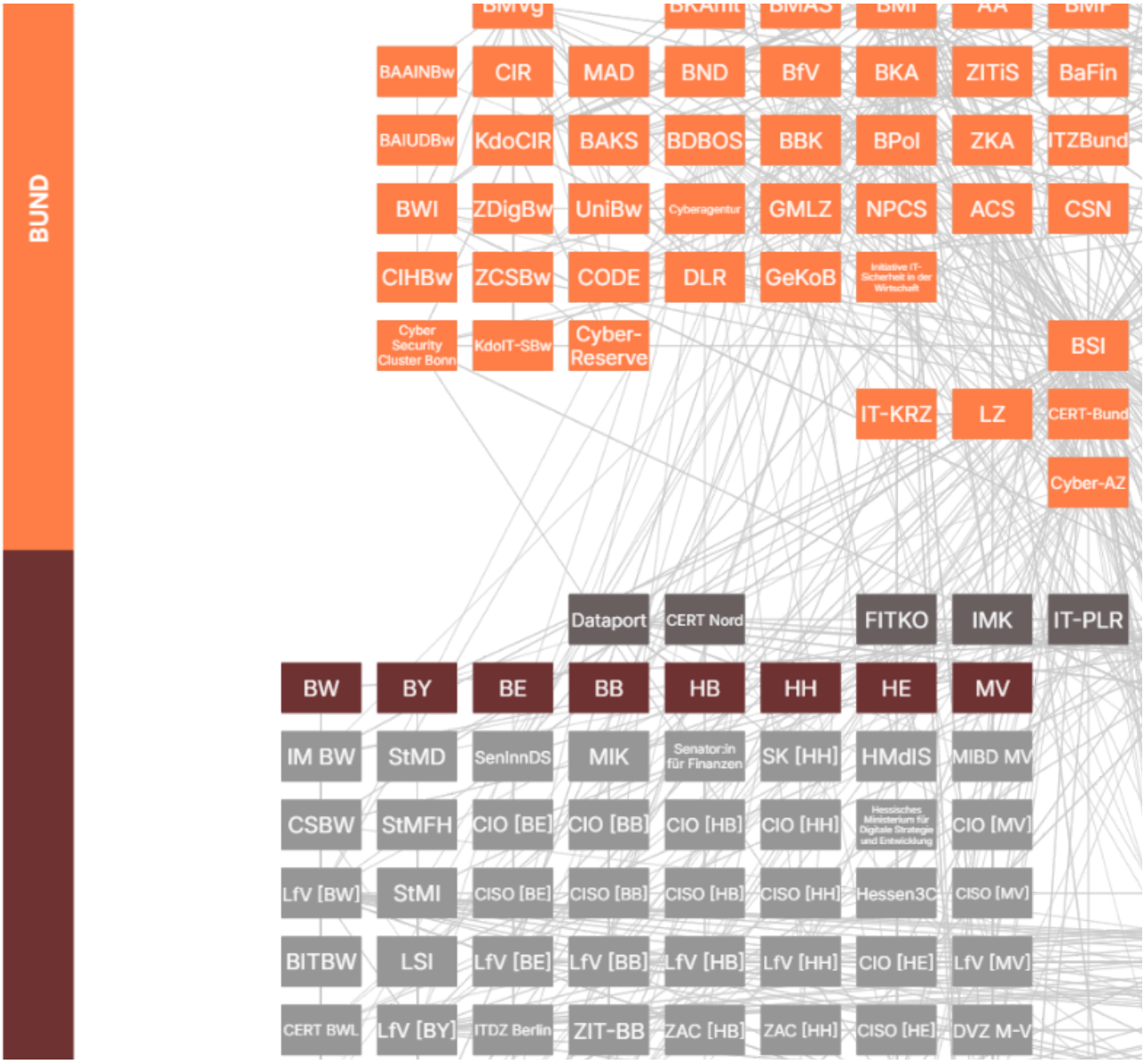
Return to the overview on page 4.

Source: interface · cybersicherheitsarchitektur.de · Version used in the original white paper

Figure 1 · Detail 3 of 6

Middle section · Left half

Unaltered excerpt from the original graphic. Adjacent areas overlap.



Position in the overview

1	2
3	4
5	6

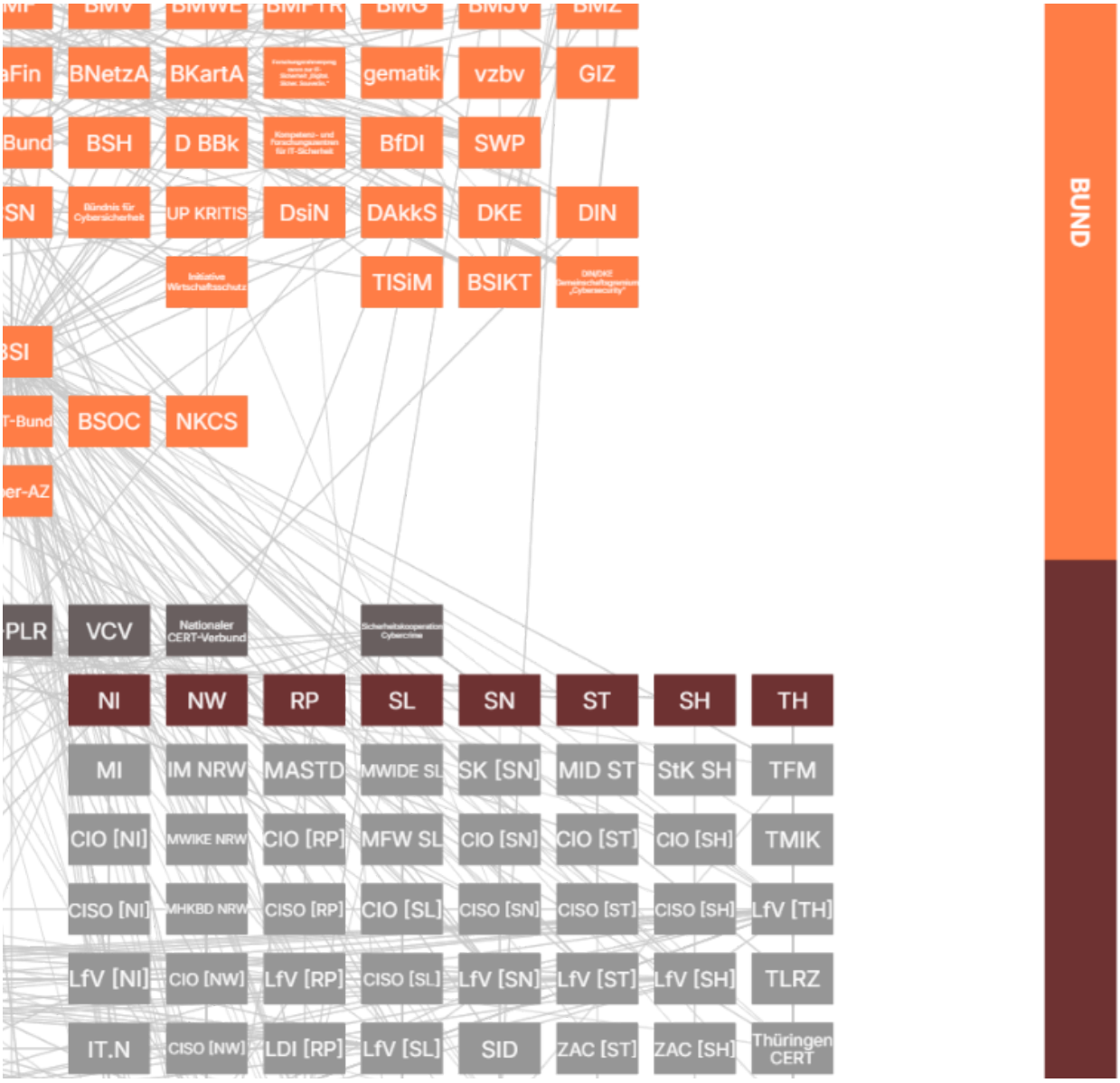
Return to the overview on page 4.

Source: interface · cybersicherheitsarchitektur.de · Version used in the original white paper

Figure 1 · Detail 4 of 6

Middle section · Right half

Unaltered excerpt from the original graphic. Adjacent areas overlap.



Position in the overview

1	2
3	4
5	6

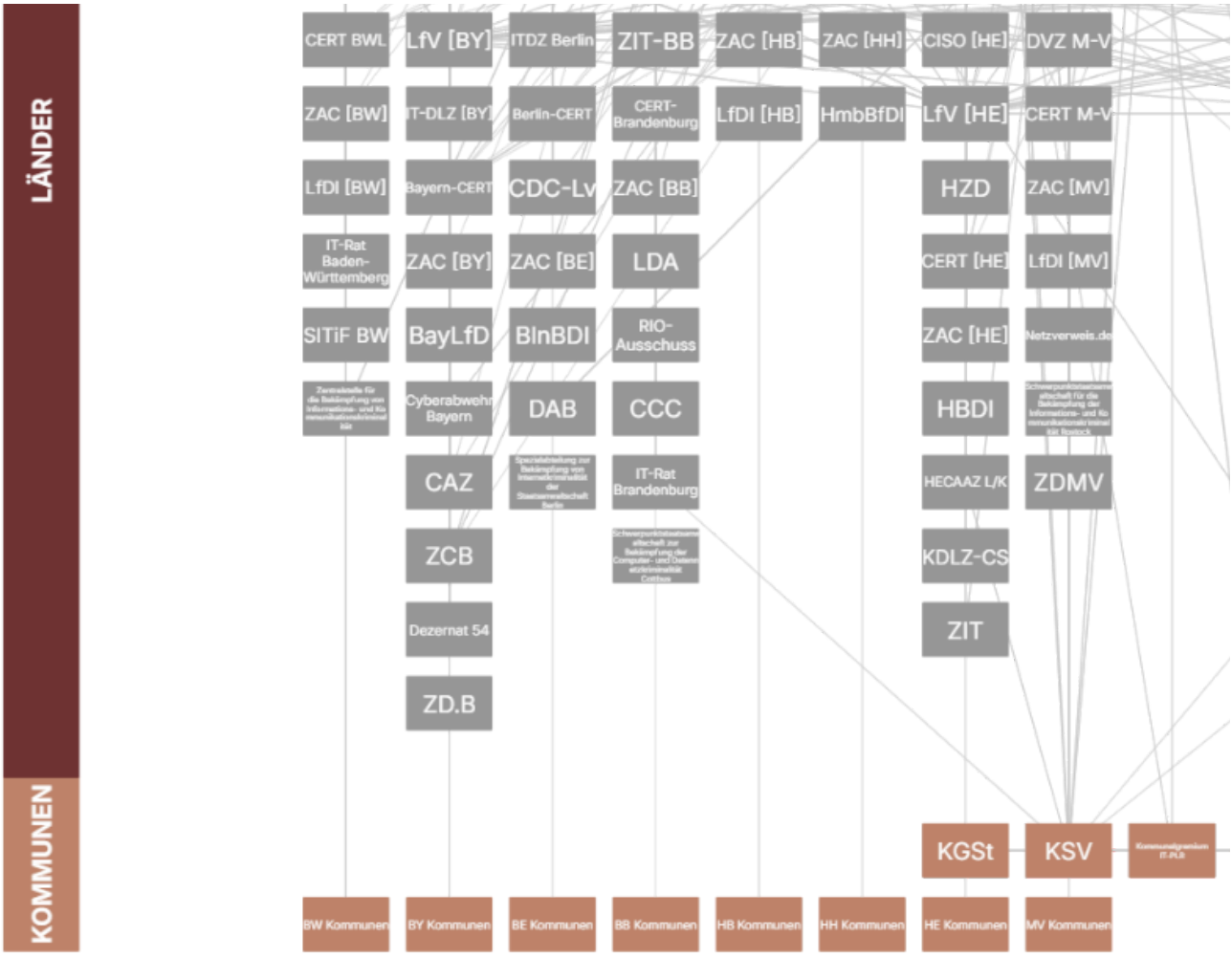
Return to the overview on page 4.

Source: interface · cybersicherheitsarchitektur.de · Version used in the original white paper

Figure 1 · Detail 5 of 6

Lower section · Left half

Unaltered excerpt from the original graphic. Adjacent areas overlap.



CC BY SA
Creative Commons license
CC BY-SA 4.0

Version: Juli 2

Position in the overview

1	2
3	4
5	6

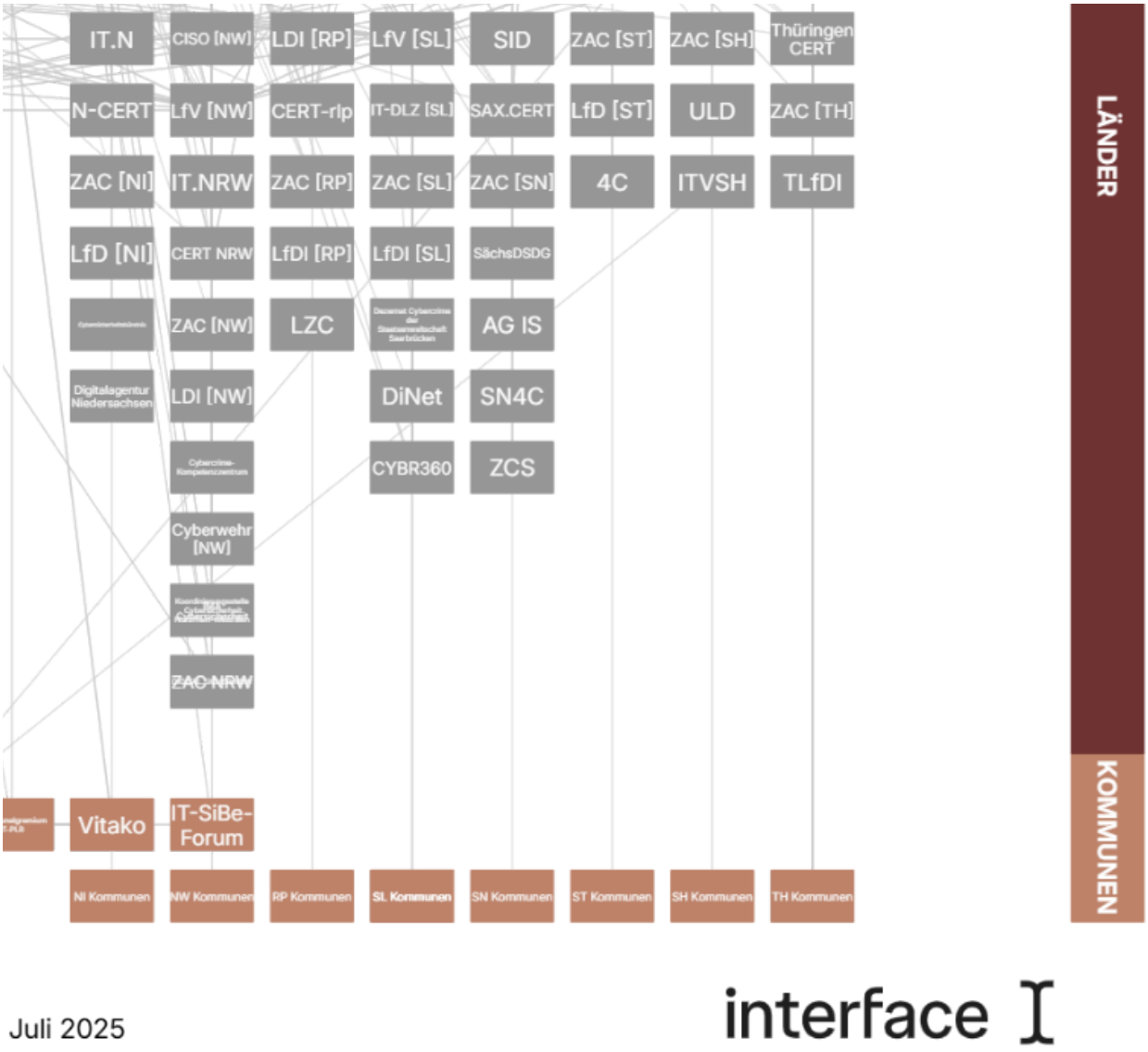
Return to the overview on page 4.

Source: interface · cybersicherheitsarchitektur.de · Version used in the original white paper

Figure 1 · Detail 6 of 6

Lower section · Right half

Unaltered excerpt from the original graphic. Adjacent areas overlap.



Position in the overview

1	2
3	4
5	6

Return to the overview on page 4.

Source: interface · cybersicherheitsarchitektur.de · Version used in the original white paper