In the Crosshairs

Regulatory Requirements for the Resilience of Critical Infrastructure

16 April 2025

"We are no longer at peace – we are under daily attack." – Lieutenant General André Bodemann

Germany is increasingly the target of low-threshold (hybrid) attacks. These range from disinformation and espionage to sabotage. Critical infrastructure is frequently affected – such as energy and water supply, transportation, and information and communication technology. As a result, the **resilience of companies**, particularly those operating **critical infrastructure**, is coming into sharper focus in legal regulations. This is reason enough to examine to what extent businesses in Germany are currently and will in the future be held responsible for protecting themselves against such attacks and responding appropriately.

The Status Quo: Multiple Regulations Focused on IT Security

A comprehensive law to ensure a minimum level of resilience of economic operators does not yet exist. Instead, to the largest extent, various protective aspects have been enshrined for different sectors individually in specific sectoral laws. This has resulted in a myriad of **multiple regulations** of sector-specific requirements without any overarching systematic.

The only pinpoint of a more consistent approach so far has been **IT security**. The BSI Act ***(BSIG)*** obligates operators of critical infrastructures to take appropriate measures to ensure, among other things, the integrity of their systems. The BSI-KritisV defines who qualifies as an operator. However, outside of IT security, there are currently no **cross-sectoral** requirements for the physical resilience of critical infrastructure.

Besides the BSIG, there are certain sector-specific requirements to increase economic operators' resilience. However, also these requirements to a large degree pertain to cyber security. For example, providers of public telecommunications networks and services are obligated under the Telecommunications Act (*TKG*, § 165 paras. 2 and 3), and operators of energy facilities and supply networks under the Energy Industry Act (*EnWG*, § 11 paras. 1a ff.), to ensure appropriate protection of their IT systems. The IT security catalogs issued by the Federal Network Agency (BNetzA) specify both the requirements and who falls under the regulations.

While these **sector-specific** regulations are primarily aimed at ensuring supply security during normal operations and enabling a quick recovery in the event of disruptions, they

also contribute indirectly to resilience against hybrid threats. For example, pharmaceutical companies are required to ensure continuous availability of medicines under § 52b AMG.

New Cross-Sector Initiatives: NIS-2 and the KRITIS Umbrella Act

However, this inconsistent approach will at least partially change in the future. Directive (EU) 2022/2555 (the so-called ***NIS-2 Directive***) aims to further strengthen **IT security** across the EU. It introduces new categories ("essential" and "important" entities) and significantly expands the scope – from around 2,000 to up to 30,000 affected companies. The former German government's draft bill to implement the NIS-2 Directive aimed to comprehensively reform the BSI Act but did not dissolve overlapping regulations in the EnWG and TKG. The coalition failed to pass the implementation law, even though the implementation deadline expired in October 2024. In light of the infringement proceedings now initiated by the European Commission against Germany, the new federal government is under pressure to act.

The same applies to the **KRITIS Umbrella Act** (KRITIS-Dachgesetz). This draft law was intended to introduce, for the first time, independent and cross-sectoral **requirements for the physical resilience** of critical infrastructure while also implementing Directive (EU) 2022/2557 (the so-called ***CER Directive***). Its aim was to require operators of critical infrastructure to conduct risk assessments, prepare resilience plans, and develop sector-specific resilience standards – ultimately mandating appropriate and proportionate measures to physically protect their assets. This act, too, was not passed. However, since the CER Directive also had to be transposed by October 2024, there is urgent need for action here as well.

Conclusion

So far, resilience requirements have primarily focused on IT security. The NIS-2 Directive tightens these requirements and brings significantly more companies into scope but has yet to be implemented. Beyond IT security, no cross-sectoral requirements currently exist. The KRITIS Umbrella Act would have changed that but was not enacted. Thus, the implementation of the CER Directive also remains pending.

Due to the principle of discontinuity, these legislative efforts must be reintroduced in the new Bundestag. What is clear: Given the current threat landscape, future regulations will increasingly take a holistic approach to IT security and physical resilience. Companies should prepare for this early on.

BLOMSTEIN provides comprehensive advice on matters of defense and security and closely monitors current legislative developments. Please do not hesitate to contact Christopher Wolters and Leonard von Rummel if you have any questions.

***