Der rechtliche Rahmen von KRITIS – Aufbruch oder Stillstand?

Prof. Dr. Sven Eisenmenger[1]

I. Die NIS-2-Richtlinie und die CER-Richtlinie sowie ihre Umsetzung

Vor dem Hintergrund der auch rechtlichen Dimension der heutigen KRITIS-Tagung, erlauben Sie mir, dass ich in diesen Rahmen nachfolgend eine rechtliche Einführung aus dem Blickwinkel der Forschung gebe.

KRITIS sind ein unverzichtbarer Bestandteil für das Funktionieren des Gemeinwesens. Gleichzeitig sind KRITIS besonderen Gefahren physischer Art und Cybergefahren ausgesetzt. Dazu zählen Unfälle, Sabotage, Schadprogramme, Terrorismus oder Krieg sowie Naturphänomene wie Stürme, Hochwasser oder Pandemien. So kommt es auch zu Sabotageakten im Bereich Schifffahrt in Häfen, und im Bereich der maritimen Infrastrukturen zur Zerstörung von Unterseekabeln in der Ostsee. Im Bereich Schienenverkehr gibt es immer wieder Angriffe auf das Schienennetz der Deutschen Bahn und im Bereich Luftfahrt Aktionen sog. „Klimakleber" an verschiedenen Flughäfen bis hin zum GPS-Jamming und Cyberattacken.

KRITIS-Unternehmen bzw. die Wirtschaft müssen hier Vorsorge und Schutz, aber auch Schadensbewältigung betreiben (Resilienzmaßnahmen). Der Staat bzw. die staatlichen Akteure wiederum nehmen staatliche Präventions- und/oder Schadensbewältigungsaufgaben wahr.

Die Aufgaben sind nicht nur in praktischer Hinsicht fordernd. Auch der Rechtsrahmen zum physischen Schutz und zur Cybersicherheit ist überaus komplex und im Wandel begriffen. So hat der EU-Gesetzgeber mit der sog. CER- und der sog. NIS-2-Richtlinie weitere und neue Regelungen geschaffen, die auf den physischen Schutz und die Cybersicherheit von KRITIS zielen und in nationales Recht umzusetzen sind. Darüber hinaus besteht noch eine Vielzahl spezieller EU-Richtlinien und Verordnungen, auf die der Anhang der beiden genannten Richtlinien eingeht.[2] Ich werde mich hier in meiner Einführung auf die beiden Grundlagenrichtlinien „NIS-2"- und „CER" mit ihrer Umsetzung beschränken und der Frage nachgehen, ob wir aus rechtswissenschaftlicher Sicht einen Stillstand oder Aufbruch erleben.

1. Cybersicherheit

a) Unionsrecht

Die Richtlinie (EU) 2022/2555 vom 14.12.2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie)[3] regelt ausweislich des Art. 1 Abs. 1 NIS-2-RL Maßnahmen, mit denen unionsweit ein hohes gemeinsames Cybersicherheitsniveau sichergestellt werden soll, um so das Funktionieren des Binnenmarktes zu verbessern.

---

[1] *Prof. Dr. Sven Eisenmenger*, Professur für Öffentliches Recht an der Hochschule der Akademie der Polizei Hamburg und Leiter des Forschungsinstituts für Unternehmenssicherheit und Sicherheitswirtschaft (FORSI).
[2] S. dazu den Beitrag von *Schröder* in diesem Tagungsband (3. Teil).
[3] ABl. (EU) L 333 v. 27.12.2022, S. 80 ff., in der aktuellen Fassung.

Aufgelistet sind die Sektoren Energie, Verkehr, Bankwesen, Finanzmarktinfrastrukturen, Gesundheitswesen, Trinkwasser, Abwasser, Digitale Infrastruktur, Verwaltung von IKT-Diensten, Öffentliche Verwaltung und Weltraum (Anhang I der NIS-2-Richtlinie) sowie weitere kritische Sektoren im Anhang II.

Nach der Richtlinie muss jeder Mitgliedsstaat insbesondere eine nationale Cybersicherheitsstrategie verabschieden, die die strategischen Ziele enthält, Art. 7 NIS-2-Richtlinie. KRITIS-Betreiber müssen Risikomanagementmaßnahmen durchführen (Art. 21 NIS-2-Richtlinie), es bestehen Berichtspflichten bei Störungen (Art. 23 NIS-2-Richtlinie) und weitere Anforderungen.

b) Nationales Recht

Die Umsetzung hätte in Deutschland in Form eines Gesetzes bis 17.10.2024 erfolgen müssen. In einer Auflistung der EU vom 2.9.2025[4] hat Deutschland zwar noch kein umfassendes NIS-2-Umsetzungsgesetz realisiert (siehe sogleich), allerdings haben die Bundesländer erste Maßnahmen erlassen:

1. Thüringer Datenschutzgesetz

2. Hessisches Gesetz zum Schutz der elektronischen Verwaltung (Hessisches IT-Sicherheitsgesetz - HITSiG

3. Gesetz zur Änderung des Sächsischen Informationssicherheitsgesetzes und Gesetz zur Neuordnung der Informationssicherheit im Freistaat Sachsen

4.Verwaltungsvorschrift zur Umsetzung der NIS-2 Richtlinie in der saarländischen Landesverwaltung

5. Gesetz zur Änderung des Bayerischen Digitalgesetzes und des Gesetzes über die Bayerische Landesstiftung

6. Ministerialblatt der Landesregierung von Rheinland-Pfalz [spez. Vorschriften]

7. Umsetzung der NIS-2-Richtlinie in Niedersachsen

8. Umsetzung der NIS-2-Richtlinie in Niedersachsen; Bestimmung von Zuständigkeiten

9. Gemeinsamer Runderlass zur Umsetzung europarechtlicher Vorgaben für die Gewährleistung eines hohen gemeinsamen Cybersicherheitsniveaus in der Union

10. Verwaltungsvorschrift zur Umsetzung der NIS-2-Richtlinie in der Freien Hansestadt Bremen (VV NIS2Ums FHB)

11. Gesetz über die elektronische Verwaltung im Land Brandenburg

12. Festsetzung gemäß § 21 Absatz 2 Nummer 4 EGovG Berlin zur Umsetzung der Richtlinie (EU) 2022/2555

13. E-Government-Gesetz Berlin - EGovG Bln

14. Verordnung zur Umsetzung der NIS-2-Richtlinie im Land Brandenburg

[4] EURLEX, https://eur-lex.europa.eu/legal-content/DE/NIM/?uri=CELEX:32022L2555&qid=1756809004646 (abgerufen am 2.9.2025).

Auf Bundesebenebene wird derzeit das Gesetzgebungsverfahren zur Umsetzung der NIS-2-Richtlinie betrieben mit dem „Entwurf eines Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung“[5], das als Artikelgesetz rund 30 Gesetze ändern wird. Insbesondere im Entwurf des BSI-Gesetzes (BSIG) werden in §§ 28 ff. BSIG-E die Anforderungen der NIS-2-Richtlinie aufgegriffen und gespiegelt.

Nach den Vorschriften zum Anwendungsbereich (§§ 28 f. BSIG-E – dort auch mit Bezug u.a. zu „Besonders wichtigen und wichtigen Einrichtungen“) folgen ab §§ 30 ff. BSIG-E „Risikomanagement-, Melde-, Registrierungs-, Nachweis- und Unterrichtungspflichten“. Sie geben einen wesentlichen Ausschnitt der Unternehmenspflichten wieder.

2. Physische Resilienz

a) Unionsrecht

Die Richtlinie (EU) 2022/2557 vom 14.12.2022 über die Resilienz kritischer Einrichtungen und zur Aufhebung der Richtlinie 2008/114/EG[6] (CER-Richtlinie) zielt ausweislich ihres Art. 1 Abs. 1 lit. b darauf, Verpflichtungen für kritische Einrichtungen festzulegen, um ihre Resilienz und ihre Fähigkeit zur Erbringung ihrer Dienste zu verbessern. Während die NIS-2-Richtlinie auf die Cybersicherheit zielt, geht es in der CER-Richtlinie um die physische Sicherheit (Art. 1 Abs. 2 CER-Richtlinie). Unter Zugrundelegung des ErwGr 79 der NIS-2-Richtlinie zielt das „Cyberrecht“ anders ausgedrückt auf das Netz- und Informationssystem (auch physisch) als Ausschnitt der Gesamtanlage, während demzufolge die CER-Richtlinie sich auf alle restlichen körperlichen Einheiten der Gesamtanlage bezieht.

Die erfassten Sektoren in der CER-Richtlinie sind denen der NIS-2-Richtlinie sehr ähnlich und umfassen: Energie, Verkehr, Bankwesen, Finanzmarktinfrastrukturen, Gesundheit, Trinkwasser, Abwasser, Digitale Infrastruktur, Öffentliche Verwaltung und Weltraum sowie die Produktion, Verarbeitung und Vertrieb von Lebensmitten (vgl. den Anhang der CER-Richtlinie),

Nach der CER-Richtlinie muss jeder Mitgliedstaat insbesondere eine Strategie zur Verbesserung der Resilienz kritischer Einrichtungen bis zum 17.1.2026 verabschieden und eine Risikobewertung ebenso bis zum 17.1.2026 durchführen, Art. 4 f. CER-Richtlinie. Auf die kritischen Einrichtungen kommen verschiedene Verpflichtungen zu, wie Risikobewertungen (Art. 12 CER-Richtlinie), Resilienzmaßnahmen (Art. 13 CER-Richtlinie) und es bestehen Meldepflichten bei Störungen (Art. 15 CER-Richtlinie) sowie weitere Anforderungen.

b) Nationales Recht

Betrachtet man den Umsetzungsstand in Deutschland (die Richtlinie hätte bis 17.10.2024 durch Rechtsvorschriften in deutsches Recht überführt werden müssen), so ergeben sich bei einer Recherche dazu unter dem EU-Portal „Eurlex“ insgesamt „0 Maßnahmen“[7].

[5] BR-Drs. 369/25.
[6] ABl. (EU) L 333 v. 27.12.2024, S, 164 ff.
[7] Eurlex, https://eur-lex.europa.eu/legal-content/DE/NIM/?uri=CELEX:32022L2557&qid=1756887706815 (zuletzt abgerufen am 3.9.2025).

Allerdings ist ein neuer „Entwurf eines Gesetzes zur Umsetzung der Richtlinie (EU) 2022/2557 und zur Stärkung der Resilienz kritischer Anlagen“ auf den Weg gebracht (Regierungsentwurf vom 10.9.2025[8]). Dort enthalten ist insbesondere der Entwurf eines „Dachgesetzes zur Stärkung der physischen Resilienz kritischer Anlagen“.

Hinsichtlich des Anwendungsbereiches gilt, dass die erfassten kritischen Anlagen im Wesentlichen durch Rechtsverordnung konkretisiert werden (Katalog der kritischen Dienstleistungen gem. § 4 Abs. 3 KRITIS-DachG-E, Erheblichkeit der Anlage gem. § 5 KRITIS-DachG-E).

Auf Seiten der staatlichen Akteure soll u.a. ausweislich des § 1 KRITIS-DachG-E eine „Nationale KRITIS-Resilienzstrategie“ verabschiedet werden, außerdem sind auch nationale Risikoanalysen und Risikobewertungen durchzuführen (§ 11 KRITIS-DachG-E). Auf Seiten der KRITIS-Betreiber bestehen Registrierungs-, Risikoanalyse-/bewertungs-, Resilienzmaßnahmen-, Nachweis- und Meldepflichten (§§ 8 ff. KRITIS-DachG-E).

Die Gesetzesbegründung führt aus, es seien Schnittstellen zwischen physischem Schutz (KRITIS-DachG-E) und IT Sicherheit (Cybersicherheit) bzw. BSIG-E berücksichtigt, angeglichen und möglichst übereinstimmend geregelt.[9]

II. Bewertung

1. Grundlinie

Es ist zu begrüßen, dass in der EU und in Deutschland gesetzliche Anstrengungen zur Konsolidierung des KRITIS-Rechts unternommen werden und in Deutschland insbesondere mit dem KRITIS-DachG erstmalig der Versuch unternommen wird, ein übergreifendes Gesetz zu schaffen. Damit lässt sich zunächst mit Blick auf die Grundfrage dieses Beitrages zum KRITIS-Recht insgesamt feststellen: „Aufbruch ja, Stillstand nein“.

2. Unzureichende gesetzliche Vernetzung Cybersicherheit und physische Resilienz

Gleichwohl werfen die Umsetzungsregelungen in Deutschland auch Fragen auf. So werden die Regelungen zur Cybersicherheit in dem BSIG-E normiert. Das KRITIS-Dachgesetz mit seinem All-Gefahrenansatz tritt „neben“ die genannten Spezialgesetze und regelt im Ergebnis die physische Resilienz. Dies führt zu Abgrenzungsproblemen, die schon unionsrechtlich angelegt, aber keineswegs zwingend sind. Im Einzelnen:

Bereits auf der EU-Ebene wird zwischen der NIS-2- und der CER-Richtlinie ein wesentliches Manko deutlich: Die NIS-2-Richtlinie fokussiert auf „Netz-und Informationssysteme sowie ihr physisches Umfeld“ (ErwGr 79 der NIS-2-Richtlinie zum Bereich „Risikomanagementmaßnahmen“). Bereits auf dieser Ebene stellt sich doch die Frage: Wo hört der physische Schutz der NIS-2-Richtlinie auf und wo fängt der physische Schutz der CER-Richtlinie an? Dieses Beispiel zeigt, dass die Trennung von Cybersicherheit und physischer Resilienz künstlich ist

[8] Bundesministerium des Innern, Veröffentlichung vom 10.9.2025, https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/KM4/KRITIS-Dachgesetz.html (zuletzt abgerufen am 10.9.2025).
[9] KRITIS-DachG-Regierungsentwurf v. 10.9.2025, S. 1 f.

und zu erheblichen Auslegungsproblemen für die Praxis führen kann. Die Trennung beider Bereiche wird im nationalen Recht aufrechterhalten, weil die Materie in zwei Gesetzen, und zwar in dem BISG-E und dem KRITIS-DachG-E, getrennt fortgeführt wird.

Dabei ist im Übrigen noch nicht berücksichtigt, dass in beiden Rechtsbereichen auch die Begriffe „Schutz" und „Resilienz" unterschiedlich gebraucht werden. So taucht der Begriff „Resilienz" in der NIS-2-Richtlinie und im BSIG-E in einer Gesamtschau kaum auf, im Gegensatz dazu ist „Resilienz" in der CER-Richtlinie und im KRITIS-DachG-E ein Kernbegriff.

Auch ist es für die anwendende Praxis – gerade für die Unternehmen – sehr kompliziert und intransparent, bei Fragen der Cybersicherheit und der physischen Sicherheit, die so eng miteinander verbunden sind, mit zwei komplexen Gesetzen umgehen zu müssen.

Aus systematischer Sicht sollte Cybersicherheit und physische Sicherheit bzw. Cyberresilienz und physische Resilienz in einem Gesetz vereint werden. Dies würde auf das Ziel einzahlen, auch gesetzlich ein echtes „Dachgesetz" zu schaffen, das alle Materien in sich vereinigt und das nicht nur lediglich auf Kohärenz mit Fachgesetzen ausgerichtet ist.[10]

3. Unzureichende gesetzliche Vernetzung KRITIS und Zivile Verteidigung

Wir befassen uns aktuell in Deutschland intensiv mit dem Recht Kritischer Infrastrukturen einerseits, andererseits ist das Recht des äußeren Notstands (Operationsplan Deutschland, Ertüchtigung der Bundeswehr), also die Reform der militärischen und zivilen Verteidigung, Gegenstand der rechtspolitischen Debatte. Rechtssystematisch ist folgendes anzumerken:

Zu der Zivilen Verteidigung gehört unstrittig die Versorgung der Zivilbevölkerung der Bundeswehr mit den notwendigen Gütern und Leistungen (ab Ziff. 22 ff. der Rahmenrichtlinien für die Gesamtverteidigung). Dort geht es um die reformbedürftigen Sicherstellungs- und Vorsorgegesetze, die u.a. auch die Wirtschaft in die Pflicht nehmen.[11] In diesen Zusammenhang wird auch das Gesamtthema KRITIS eingeordnet. Die Bund/Länder offene Arbeitsgruppe Zivile Verteidigung/Zivil-Militärische Zusammenarbeit schreibt in ihrem Bericht vom 9. Mai 2025 an die Innenministerkonferenz:

> „*Der physische Schutz von kritischen Infrastrukturen (KRITIS) ist angesichts der komplexen geopolitischen Herausforderungen wichtiger denn je. Die Versorgung der Bevölkerung und der Streitkräfte mit kritischen Dienstleistungen wie Wasser, Strom und Lebensmitteln muss auch in Krisensituationen gewährleistet werden."* In der 20. Legislaturperiode sollte die Resilienz kritischer Infrastrukturen mit dem KRITIS-Dachgesetz gestärkt werden. Der Gesetzentwurf ist aufgrund der verkürzten Legislaturperiode der Diskontinuität anheimgefallen. Die Schaffung eines Bundesgesetzes mit sektorenübergreifenden Vorgaben zur Stärkung der Resilienz von KRITIS hat in der neuen Legislaturperiode unverändert höchste Priorität. Für die aus Bundessicht wichtigsten kritischen Infrastrukturen soll es eine Verpflichtung zum Ergreifen von physischen Maßnahmen zur Stärkung ihrer Resilienz geben, die auf Risikobewertungen und dem All-Gefahren-Ansatz beruhen, sowie eine Verpflichtung zur Meldung von Vorfällen. Mit nationalen

[10] S. dazu bereits *Eisenmenger* NVwZ 2023, 1206 (1203) und *Eisenmenger* in ders., FORSI-Jahresband 2023, 2024, 37 (49 f.).
[11] S. dazu *Eisenmenger,* GSZ 2025, 77 (78).