International Cybersecurity Law Review (2023) 4:1–19
https://doi.org/10.1365/s43439-022-00077-4

Kritikalität: Von der BSI-KritisV zur NIS2-Richtlinie

Valentin Vogel · Nicolas Ziegler

Eingegangen: 21. November 2022 / Angenommen: 8. Dezember 2022 / Online publiziert: 16. Januar 2023

Zusammenfassung Naturkatastrophen, Cyberattacken und nicht zuletzt der Angriffskrieg Russlands gegen die Ukraine verdeutlichen zunehmend die Bedeutung kritischer Infrastrukturen für einen handlungsfähigen Staat und eine funktionsfähige Gesellschaft. Obwohl sich Politik und Rechtswissenschaften bereits seit mehreren Jahrzehnten mit dem Begriff der kritischen Infrastrukturen befassen, gibt es eine an Rechtsfolgen geknüpfte Legaldefinition im deutschen Recht erst mit dem IT-Sicherheitsgesetz von 2015 und auch nur für den Bereich der IT-Sicherheit. Dies erfolgte vorgreifend zur Umsetzung der NIS-Richtlinie aus dem Jahr 2016. Auch wenn dadurch die Resilienz erhöht wurde, offenbart die nationale Umsetzung derzeit einige Schwächen: Die Begriffe Kritikalität und kritische Infrastrukturen offenbaren normative und tatsächliche Herausforderungen, die angesichts der zugrunde liegenden Risiko-Prognose-Entscheidung nicht vollständig aufgelöst werden können. Die Systematik der Verweiskette zwischen dem BSIG, der BSI-KritisV und einschlägigen Fachgesetzen ist geprägt von fehlender Klarheit und Harmonisierung. Zuletzt bietet der starke Fokus auf hohe Schwellenwerte bei der Einordnung kritischer Infrastrukturen Raum für Kritik. Mit der kürzlich in finaler Fassung beschlossenen NIS2-Richtlinie ergeben sich zukünftig zahlreiche Änderungen für die Einordnung kritischer Infrastrukturen. Der Beitrag erörtert die bisherige Rechtslage in Deutschland unter Herausarbeitung von Kritik, bevor er die Änderungen der NIS2-Richtlinie mit dem Fokus auf der Begriffsbestimmung darstellt und im Hinblick auf die zuvor geäußerte Kritik bewertet.

Valentin Vogel · ✉ Nicolas Ziegler
Lehrstuhl für Recht und Sicherheit der Digitalisierung an der School of Social Sciences and Technology, Department Governance, Technische Universität München, München, Deutschland
E-Mail: nicolas.ziegler@tum.de

Valentin Vogel
E-Mail: valentin.vogel@tum.de

Schlüsselwörter NIS-Richtlinie · Kritische Infrastrukturen · Schwellenwerte · Kritikalität · Sektoren

The definition of critical infrastructures: from the BSI-KritisV to the NIS2-Directive

Abstract Natural disasters, cyber attacks and, not least, Russia's war of aggression against Ukraine are increasingly highlighting the importance of critical infrastructures for a state capable of action and a functioning society. Although politicians and legal scholars have been dealing with the concept of critical infrastructures for several decades, a definition linked to legal consequences did not exist in German law until the Cyber Security Act of 2015, and then only for the area of cyber security. This was done in anticipation of the implementation of the Network and Information Security Directive (NIS Directive) from 2016. Even though this increased resilience, the national implementation currently reveals some weaknesses: The terms cruciality and critical infrastructure reveal normative and actual challenges that cannot be fully resolved due to the underlying risk prediction decision. The systematics of the chain of references between the BSIG ("Gesetz über das Bundesamt für Sicherheit in der Informationstechnik"), the BSI KritisV ("Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz"), and relevant specialized laws is characterized by a lack of clarity and harmonization. Finally, the strong focus on high threshold values in the classification of critical infrastructures offers room for criticism. The NIS2 Directive, which was recently adopted in its final version, will result in numerous changes for the classification of critical infrastructures in the future. The article discusses the current legal situation in Germany, highlighting criticisms, before presenting the changes in the NIS-2 Directive with a focus on the definition of crucial infrastructure and evaluating them in light of the criticisms previously expressed.

Keywords NIS Directive · Critical infrastructures · Thresholds · Criticality · Sectors

1 Einleitung

Die Sabotageakte gegen die Nord-Stream-Pipelines im September 2022 haben die Verletzbarkeit kritischer Infrastrukturen in Deutschland und Europa ins Licht der öffentlichen Debatte katapultiert. Bisher haben Diskussionen hierüber die damit befassten Fachkreise selten verlassen. Weitgehend unbemerkt von breiter öffentlicher Aufmerksamkeit hat die EU-Kommission in 2020 mit der Richtlinie über die Resilienz kritischer Einrichtungen (CER-Richtlinie)[1] und der Richtlinie über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau (NIS2-Richtlinie)[2] zwei hierzu zentrale Rechtsakte vorgeschlagen. Beide haben das Ziel, zur Widerstandsfähigkeit

[1] COM(2020) 829 final.

[2] COM(2020) 823 final.

der kritischen europäischen Infrastrukturen beizutragen.[3] Während sich die CER-Richtlinie auf physische Gefahren fokussiert, hat die NIS2-Richtlinie die Cybersicherheit kritischer Infrastrukturen zum Gegenstand und soll als Überarbeitung die Richtlinie über die Sicherheit von Netz- und Informationssystemen (NIS-Richtlinie)[4] ersetzen. Dieser Beitrag widmet sich der grundlegenden Frage, nach welchen Kriterien im unionalen und nationalen deutschen Recht bestimmt wird, welche Unternehmen oder Stellen als kritische Infrastruktur gelten und welche Änderungen die NIS2-Richtlinie für den Begriff der kritischen Infrastrukturen bereithält. Zunächst geht der Beitrag auf die Herausforderungen (Abschn. 2.1) und den gegenwärtigen Stand einer normativen Verankerung des Begriffs der Kritikalität ein (Abschn. 2.2). Darauf aufbauend wird dargestellt, wie kritische Infrastrukturen im Sinne des IT-Sicherheitsrechts historisch (Abschn. 3.1) und de lege lata definiert werden (Abschn. 3.2), welche Folgen dies hat (Abschn. 3.3) und was an der derzeitigen Regelung kritikwürdig ist (Abschn. 4). Schlussendlich werden die Änderungen durch die NIS2-Richtlinie dargestellt (Abschn. 5.) und im Gesamtkontext zur bisherigen Rechtslage und bestehender Kritik bewertet (Abschn. 6).

2 Kritikalität als (Rechts) Begriff

2.1 Normative Herausforderung der Begriffsbestimmung

Eine besondere Herausforderung im Kontext von Kritikalität und kritischen Infrastrukturen ist die Komplexität der Begriffe. Uneinheitliche Definitionen und verschiedene Darstellungen im deutschen und unionalen Raum verdeutlichen zunehmend die Erforderlichkeit begrifflicher Klarheit, um auch jenseits von Auflistungen und Anhängen zu Gesetzestexten normativ erschließen zu können, was eine Infrastruktur kritisch macht. Viel zu oft wird „das Kritische“ an Infrastrukturen als selbstverständlich vorausgesetzt, wobei die begriffliche Redundanz einer kritischen Infrastruktur hierzu beiträgt: Welche Infrastruktur kann unkritisch sein?[5] Eine Definition von Kritikalität vermag der Blindheit entgegenzuwirken, die gegenüber Infrastrukturen herrscht, solange sie reibungslos funktionieren. Erst bei Störungen würden sie wieder „sichtbar“.[6] Eine allgemeingültige Definition wird es aber nicht uneingeschränkt geben können, da es sich letztlich um das Ergebnis einer Risiko-Prognose-Entscheidung handelt, über deren Richtigkeit man erst im Schadensfall Gewissheit erhält.[7] Dennoch steht das Recht – wie auch beim Begriff der Kunst in Art. 5 Abs. 3 S. 1 GG – vor der Notwendigkeit, einen Begriff zu finden: Denn die Einordnung als kritische Infrastruktur ist nach der Welle der Infrastrukturprivatisierungen in den 1990er-Jahren Anknüpfungspunkt hoheitlich angeordneter Mindestvoraussetzungen

[3] [7].

[4] RL (EU) 2016/1148, Abl. L 194/1 ff.

[5] Vgl. [6, S. 19].

[6] aaO S. 20.

[7] Vgl. [8, S. 171].

an staatlichen Schutz.[8] Hierfür ist der Staat nach der dem Sozialstaatsprinzip aus Art. 20 Abs. 1 GG folgenden Schutzpflicht der sog. Infrastrukturverantwortung auch verpflichtet. Darunter versteht man die Pflicht zur Bereitstellung der für die Daseinsvorsorge essenziellen Einrichtungen.[9] Sie verpflichtet den Staat zum Monitoring technischer Entwicklungen und nötigenfalls regulativen Eingriffen zur sicheren Gewährleistung der Versorgung, da der Staat die nötigen Infrastrukturen (z.B. Strom, Gas, Wasser) nicht selbst bereitstellen muss und es in der Regel auch nicht mehr tut.[10]

2.2 Begriffliche Ausgangslage

Im deutschen Rechtsraum lässt sich die begriffliche Komplexität auf mehrere Entwicklungen zurückführen. Der Begriff der kritischen Infrastrukturen und das dafür geläufige Akronym KRITIS geht in Deutschland bereits auf erste systematische Entwicklungen in den 1990er- und 2000er-Jahren zurück. Im Jahr 1997 entstand die im Bundesinnenministerium (BMI) verortete und später begriffsprägende Arbeitsgruppe AG KRITIS[11], die im Rahmen ihrer Tätigkeit erstmals sieben kritische Sektoren identifizierte.[12] Dieser Entwicklung folgend, ist der Ausgangspunkt sämtlicher Definitionen der Kritikalität im deutschen Recht die des BMI, wonach kritische Infrastrukturen „Organisationen und Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen [sind], bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden.“[13] Die Definition hat jedoch nur empfehlenden Charakter und begründet i.W. keine unmittelbar verankerten Rechte oder Pflichten für Betreiber zum Schutz kritischer Infrastrukturen. Auch weitere, teils internationale, Entwicklungen, Strategien oder Gesetze im Bereich des Bevölkerungsschutzes und der Cybersicherheit beeinflussten das Begriffsverständnis für KRITIS zunehmend. Trotz des verfolgten All-Gefahrenansatz im Bevölkerungsschutz ergaben sich klare unmittelbaren Pflichten und mit Rechtsfolgen verknüpfte Definitionen im deutschen Recht aber erst im Kontext der IT-Sicherheit. Diese bietet derzeit den zentralen Referenzpunkt für die Bestimmung kritischer Infrastrukturen und soll vorliegend im Fokus stehen.

[8] [10, S. 133 f.].

[9] *Wittreck* in Dreier, GG-Kommentar, 3. Aufl. 2015 [5], Art. 20 GG (Sozialstaat) Rn. 32 unter Verweis auf BVerfGE 38, 258 (270 f.); 45, 63 (78); 66, 248 (258).

[10] Vielmehr ist es unter dem verwaltungsrechtlichen Topos des „Gewährleistungsstaates“ üblich geworden, dass Infrastrukturen von Privaten betrieben werden, der Staat jedoch eine regulative Verantwortung für den ordnungsgemäßen Betrieb behält. Siehe hierzu bei [19, S. 241 ff., 24, S. 266 ff.].

[11] Diese ist abzugrenzen von der AG Kritis (https://ag.kritis.info/) welche ein Zusammenschluss unabhängiger Experten der Cybersicherheitsbranche ist.

[12] Vgl. zur Geschichte des Schutzes kritischer Infrastrukturen im Bevölkerungsschutz und den KRITIS-Strategien Bundesamt für Bevölkerungsschutz und Katastrophenhilfe [2, S. 17].

[13] BMI, Nationale Strategie zum Schutz Kritischer Infrastrukturen (KRITIS-Strategie), [3, S. 3].

3 Kritische Infrastrukturen im IT-Sicherheitsrecht

3.1 Gesetzeshistorie

Die Klassifikation von kritischen Infrastrukturen im Bereich der IT-Sicherheit basiert auf der unionsrechtlichen NIS-RL von 2016 und dem nationalen IT-Sicherheitsgesetz aus dem Jahr 2015. Die NIS-RL befand sich zum entsprechenden Zeitraum im Gesetzgebungsverfahren und etablierte erstmals auf europäischer Ebene IT-Sicherheitsanforderungen für sog. Betreiber wesentlicher Dienste und Anbieter digitaler Dienste unter Festlegung mehrerer kritischer Sektoren. Betreiber wesentlicher Dienste sind nach Art. 4 Nr. 4 i. V. m. Art. 5 Abs. 2 NIS-RL öffentliche oder private Einrichtungen, deren Dienste für die Aufrechterhaltung kritischer gesellschaftlicher oder wirtschaftlicher Tätigkeiten unerlässlich sind, wobei die Bereitstellung der Dienste vom Netz- und Informationssystem abhängig ist und ein Sicherheitsvorfall eine erhebliche Störung der Bereitstellung der Dienste bewirken würde. Ferner spezifiziert Art. 4 Nr. 4 i. V. m. Anhang II der NIS-RL die zu erfassenden Sektoren[14] und Arten. Bei der Einordnung von erheblichen Störungen im Kontext der Bestimmung von kritischen Infrastrukturen nach Art. 5 Abs. 2 lit. c NIS-RL sollen durch die Mitgliedsstaaten gem. Art. 6 Abs. 1, 2 NIS-RL sektorübergreifende und sektorspezifische quantitative[15] und qualitative[16] Merkmale berücksichtigt werden.

Aufgrund der angespannten Sicherheitslage entschied man sich in Deutschland dafür, das Gesetzgebungsverfahren der europäischen NIS-RL nicht abzuwarten und bereits vorgreifend eigene Regelungen zu schaffen, die sich an dem damaligen Entwurf der Richtlinie orientieren sollten.[17] So trat bereits 2015, noch vor Inkrafttreten der NIS-RL 2016, das IT-Sicherheitsgesetz (IT-SiG 1.0) in Kraft, das als Artikelgesetz u. a. das BSIG wesentlich änderte und später durch die BSI-KritisV vom 22.04.2016 konkretisiert wurde.[18] Begrifflich orientierte man sich bei der Umsetzung jedoch nicht an den in der NIS-RL genannten Betreibern wesentlicher Dienste, sondern am bereits bestehenden Begriff der kritischen Infrastruktur. Bei der Bestimmung der betroffenen Dienste setzte man die qualitativen und quantitativen Elemente so um, dass zunächst qualitativ kritische Dienstleistungen zu bestimmen sind, deren Ausfall oder Beeinträchtigung quantitativ wesentliche Folgen für wichtige Schutzgüter und die Funktionsfähigkeit des Gemeinwesens hätte.[19] Dies wird durch die quantitative Bestimmung eines kumulativ zu erfüllenden Schwellenwerts für die Zahl an versorgten Personen umgesetzt, der sektor- und anlagenspezifisch

[14] In der NIS-RL sind die folgenden Sektoren benannt: Trinkwasser, Energie, digitale Infrastruktur, Bankwesen, Finanzmarktstrukturen, Gesundheitswesen und Verkehr.

[15] Insb. die Zahl der Nutzer von Einrichtungen bzw. angebotenen Diensten nach Art. 6 Abs. 1 lit. a sowie die Bedeutung der Einrichtung für die Aufrechterhaltung des Dienstes nach Art. 6 Abs. 1 lit. f, wobei hier Schwellenwerte vorgesehen sind, wie Art. 5 Abs. 7 lit. d zeigt.

[16] Die Abhängigkeit anderer Sektoren (lit. b), mögliche Auswirkungen (lit. c), der Marktanteil (lit. d) oder die geographische Ausbreitung eines möglicherweise betroffenen Gebiets (lit. e).

[17] [21, S. 429].

[18] BGBl. I S. 958.

[19] BT-Drs. 18/4096, S. 30 f.

festgelegt wird.[20] Da Deutschland die Richtlinie in weiten Teilen bereits vorgreifend umgesetzt hatte, erfolgte die verbleibende Überführung in nationales Recht durch das NIS-Umsetzungsgesetz im Jahr 2017[21] mit besonderem Fokus auf die bis dahin unzureichend umgesetzte Implementierung von Anbietern digitaler Dienste. In den erfassten Sektoren ging das IT-SiG 1.0 bereits deutlich weiter als die mindestharmonisierende NIS-RL.[22] Zuletzt erfolgten mit dem IT-Sicherheitsgesetz 2.0 weitere Anpassungen, wobei mit der Siedlungsabfallentsorgung auch ein weiterer kritischer Sektor nach § 2 Abs. 10 S. 1 Nr. 1 BSIG hinzugetreten ist.[23]

3.2 Bestimmung kritischer Infrastruktur nach dem BSIG

Die Systematik der Einordnung als kritische Infrastruktur im so umgesetzten nationalen Recht erfolgt grob vereinfacht dargestellt in drei Stufen: Es muss eine kritische Dienstleistung in einem der acht (kritischen) Sektoren nach § 2 Abs. 10 S. 1 Nr. 1 BSIG vorliegen, zu deren Erbringung eine Anlage einer in der BSI-KritisV zugeordneten Anlagenkategorie betrieben wird und deren Versorgungsgrad durch Bemessung der entsprechenden Schwellenwerte (i.d.R. 500.000 versorgte Personen) als bedeutend anzusehen ist.[24] Dabei erfolgt die Bestimmung grds. nicht durch subordinationsrechtlich-behördliche Festsetzung, sondern durch den Betreiber selbst,[25] wobei dieser auch zur Mitwirkung verpflichtet werden kann, vgl. § 8b Abs. 3a BSIG. Betrachtet man die Dogmatik der gewählten Lösung im BSIG und der BSI-KritisV jedoch genauer, stellt sie sich komplexer dar:

Ausgangspunkt ist die Legaldefinition in § 2 Abs. 10 S. 1 BSIG. Danach werden kritische Infrastrukturen bestimmt als Einrichtungen, Anlagen oder Teile davon, die einem der dort genannten Sektoren angehören (§ 2 Abs. 10 S. 1 Nr. 1 BSIG) und kumulativ von hoher Bedeutung für das Funktionieren des Gemeinwesens sind, weil durch ihren Ausfall oder ihre Beeinträchtigung Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden (§ 2 Abs. 10 S. 1 Nr. 2 BSIG). Die nähere Auslegung des unbestimmten Rechtsbegriffs der kritischen Infrastrukturen soll gem. § 2 Abs. 10 S. 2 BSIG durch Rechtsverordnung (BSI-KritisV) aufgrund der Verordnungsermächtigung in § 10 Abs. 1 BSIG erfolgen.[26] Nach dieser Verordnungsermächtigung sollen kritische Infrastrukturen „unter Festlegung“ von kritischen Dienstleistungen und bedeutenden Versorgungsgraden bestimmt werden, wobei sich deren Bedeutung durch Schwellenwerte messen lassen. Daraus lassen sich die Tatbestandsmerkmale der kritischen Dienstleistung und eines bedeutenden

[20] Kritisch zur gewählten Lösung [21, S. 429].

[21] BGBl. 2017 I 1885.

[22] [22, S. 355 (356)].

[23] Eine Konkretisierung des Sektors durch Aufnahme in die BSI-KritisV oder Aufnahme in eine überarbeitete BSI-KritisV 2.0 ist zum Zeitpunkt der Bearbeitung noch nicht erfolgt.

[24] Siehe hierzu nur *Beucher/Fromageau/Ehlen* in [14], Kap. 12 Rn. 11 f.; sowie *Fischer* in [12], § 13 Rn. 43.

[25] *Fischer* in [12], § 13 Rn. 36 ff.; 61 ff.; § 8b Abs. 3a BSIG formuliert seit seiner Einführung durch das IT-Sicherheitsgesetz 2.0 eine absichernde Mitwirkungspflicht.

[26] Ob die Verordnungsermächtigung mit Art. 80 Abs. 1 S. 2 GG vereinbar ist, kann bezweifelt werden.

Versorgungsgrads erahnen, wenngleich die Konkretisierung nicht in der Verordnung, sondern in der Verordnungsermächtigung erfolgt. Die BSI-KritisV bietet in ihren Begriffsbestimmungen nach § 1 BSI-KritisV keine weitere Definition kritischer Infrastrukturen. In den jeweils sektorspezifischen Normen der Verordnung werden diese aber als Anlagen oder Teile davon definiert, die einer im Anhang der Verordnung zugewiesenen Kategorie zuzuordnen sind und die den dafür zugeschriebenen Schwellenwert überschreiten. Anlagen sind gem. § 1 Abs. 1 Nr. 1 BSI-KritisV u. a. Betriebsstätten, Einrichtungen, Maschinen oder IT-Dienste, die für die Erbringung einer kritischen Dienstleistung notwendig sind,[27] sodass zunächst kritische Dienstleistungen festzulegen sind. Dies sind nach der Legaldefinition in § 1 Abs. 1 Nr. 3 BSI-KritisV Dienstleistungen zur Versorgung der Allgemeinheit in den jeweiligen Sektoren, deren Ausfall oder Beeinträchtigung zu erheblichen Versorgungsengpässen oder zu Gefährdungen der öffentlichen Sicherheit führen würde. Die nähere Bestimmung kritischer Dienstleistungen erfolgt in der BSI-KritisV für jeden Sektor durch Aufzählung der maßgeblichen Dienstleistungen (z. B. Stromversorgung) und deren weitere Unterteilung. Liegt eine Anlage vor, muss diese einer im Anhang der BSI-KritisV zugewiesenen Kategorie zugeordnet werden und mit den entsprechenden Schwellenwerten abgeglichen werden. Schwellenwerte sind nach § 1 Abs. 1 Nr. 5 BSI-KritisV Werte, bei deren Erreichen oder Überschreiten der Versorgungsgrad einer Anlage oder Teilen davon als bedeutend im Sinne von § 10 Abs. 1 S. 1. BSIG anzusehen ist.[28] Dafür enthält die BSI-KritisV tabellarische Anlagen, die verbindliche Schwellenwerte für einzelne Unterkategorien festlegen, die sich an den in den sektorspezifischen Normen weiter unterteilten Dienstleistungen orientieren. Die genaue Berechnung der Schwellenwerte wird im jeweiligen Teil 2 der Anlage näher festgelegt, wo von einem Regelschwellenwert von 500.000 zu versorgenden Personen ausgegangen wird, um einen bedeutenden Versorgungsgrad zu begründen. Wiederum abweichende und vorrangige Regelungen zu den Begriffsbestimmungen ergeben sich für solche kritische Infrastrukturen, die bereits in anderen Gesetzen definiert sind, z. B. in § 3 EnWG im Energiesektor, vgl. Anhang 1 Teil 1 Nr. 1 BSI-KritisV.

3.3 Folgen der Bestimmung als kritische Infrastruktur

Liegt eine kritische Infrastruktur vor, treffen die Betreiber unmittelbar Pflichten nach § 8a Abs. 1 BSIG. Betreiber sind nach § 1 Abs. 1 Nr. 2 BSI-KritisV natürliche oder juristische Personen, die unter Berücksichtigung der rechtlichen, wirtschaftlichen und tatsächlichen Umstände bestimmenden Einfluss auf die Beschaffenheit und den Betrieb einer Anlage oder Teilen davon ausüben. Die Pflichten erfassen u. a. die Einführung angemessener organisatorischer und technischer Maßnahmen zum Schutz der IT-Sicherheit. Ausnahmen davon finden sich in § 8d BSIG. Von der

[27] Zu beachten ist dabei, dass einer Anlage nach § 1 Abs. 2 BSI-KritisV alle Anlagenteile und Verfahrensschritte zuzurechnen sind, die zum Betrieb notwendig sind, sowie Nebeneinrichtungen, die mit den Anlageteilen und Verfahrensschritten in betriebstechnischem Zusammenhang stehen und für die Erbringung einer kritischen Dienstleistung notwendig sind.

[28] Dabei unterliegt deren Zustandekommen nach § 10 Abs. 1 S. 3 BSIG jedoch keiner Akteneinsicht.

Verpflichtung nach § 8a/b BSIG ausgenommen sind neben spezialgesetzlich doppelt regulierten Unternehmen (z. B. § 11 EnWG) insbesondere Kleinstunternehmen. Die Definition orientiert sich gem. § 8d Abs. 1 S. 1 BSIG an der KMU-Definition der Kommission[29] für Kleinstunternehmen. Kleinstunternehmen sind nach Art. 2 Abs. 3 der Empfehlung solche mit weniger als 10 Mitarbeitenden und einem Jahresumsatz bis zu 2 Mio. EUR. Nach Art. 3 Abs. 4 kann ein Unternehmen aber dann nicht als KMU angesehen werden, wenn 25 % oder mehr seines Kapitals oder seiner Stimmrechte von öffentlichen Stellen kontrolliert werden. Unternehmen mit entsprechender öffentlicher Beteiligung müssten die Verpflichtungen also auch erfüllen, wenn sie eigentlich als KMU gelten. Zu beachten ist aber, dass nach § 8d Abs. 1 S. 2 BSIG Art. 3 Abs. 4 der Empfehlung nicht anzuwenden ist. Dadurch können Unternehmen mit entsprechender öffentlicher Beteiligung auch als KMU eingeordnet werden und sind von IT-Sicherheitspflichten somit freigestellt.[30] Aus der NIS-RL selbst ergibt sich nach Art. 16 Abs. 11 eine Einschränkung bei Kleinst- und Kleinunternehmen dagegen nur für Anbieter digitaler Dienste[31], wobei zumindest diesbezüglich keine Ausnahme des Art. 3 Abs. 4 der Empfehlung normiert ist. Mit der Nichtanwendbarkeit von Art. 3 Abs. 4 der Empfehlung klammert der deutsche Umsetzungsgesetzgeber Kleinstunternehmen mit öffentlicher Beteiligung zwar nicht aus dem Begriff kritischer Infrastrukturen aus, befreit sie jedoch von den für kritische Infrastrukturen geltenden Pflichten. Die deutsche Rechtslage liegt daher bzgl. dem Sicherheitsniveau von Netz- und Informationssystemen unterhalb der NIS-RL.

4 Kritik am bestehenden System

4.1 Begriff

Anhand des Definitionsversuchs kritischer Infrastrukturen in der KRITIS-Strategie des BMI von 2009[32] wird eine Unterscheidung zwischen systemischer und konsequenzbasierter Kritikalität deutlich: Bei der systemischen Kritikalität steht die Gesamtbedeutung für eine infrastrukturelle Versorgung im Vordergrund, bei der konsequenzbasierten die übergeordnete gesellschaftliche Relevanz.[33] Die Definition kritischer Infrastrukturen nach dem BSIG i. V. m. BSI-KritisV geht hierbei konsequenzbasiert vor und etabliert in § 2 Abs. 10 S. 1 Nr. 2 BSIG und jeweils dem Abs. 1 in §§ 2 bis 8 der BSI-KritisV den unbestimmten Rechtsbegriff der Bedeutung für das Funktionieren des Gemeinwesens als entscheidendes Merkmal. Auffällig ist hierbei, dass der Fokus einseitig auf Vulnerabilität liegt, wohingegen Anlagen oder Dienstleistungen, die Krisen bewältigbar[34] machen, nicht in der BSI-KritisV enthal-

[29] Empfehlung 2003/361/EG der Kommission vom 06.06.2003.

[30] So auch *Buchberger* in [18], BSIG § 8d Rn. 2.

[31] Siehe hierzu auch ErwGr. 53 NIS-RL.

[32] Siehe o. Fn. 13.

[33] Vgl. hierzu näher bei [6, S. 30 f].

[34] Siehe zu diesem Vorschlag [1, S. 37].

ten sind. Die in den Anlagen zur BSI-KritisV enthaltenen Schwellenwerte fußen auf wertenden Maßstäben und laden den Kritikalitätsbegriff normativ auf. Dennoch ist dieses kasuistische Vorgehen richtig, da eine Definition ohne sie aufgrund der schier unüberblickbaren Interdependenzen zwischen den Infrastrukturen unbrauchbar und ausufernd wäre.[35] Wohl aufgrund dieser Schwierigkeiten vermeidet das deutsche Recht, außerhalb des IT-Sicherheitsrechts, andere Definitionen der Kritikalität zu entwickeln und verweist häufig auf § 2 Abs. 10 BSIG. Auffällig ist der Verweis auf § 2 Abs. 10 BSIG in der außenwirtschaftsrechtlichen Investitionskontrolle in § 55a Abs. 1 Nr. 1 AWV. Sieht man sich die Aufzählung des § 55a AWV näher an, so wird man darin wenig finden, was man im allgemeinen Sprachgebrauch nicht als kritische Infrastruktur bezeichnen würde. Die Begrenztheit der derzeitigen Definition fällt ständig ins Auge: Auch wenn die BMI-Definition von 2009 zentral für die Formulierung im BSIG und der BSI-KritisV war, so bleibt sie in einer zentralen Stelle unbeachtet. Warum staatliche Einrichtungen nach dem BSIG kein Sektor der kritischen Infrastrukturen sein soll, erschließt sich weder aus dem systemischen, noch dem konsequenzbasierten Ansatz. Dieser blinde Fleck in der IT-Sicherheitsregulierung kann eigentlich nur dadurch erklärt werden, dass der Staat entgegen jeder (empirischen) Vernunft die Anforderungen an Betreiber kritischer Infrastrukturen aus § 8a BSIG für sich selbst als lästig betrachtet. Zwar werden Stellen des Bundes unabhängig von ihrer Einordnung als kritische Infrastruktur nach § 8 BSIG adressiert, doch ermöglicht § 8 Abs. 1 S. 2 BSIG Abweichungen selbst für Mindeststandards und vermag am eben getroffenen Urteil nichts zu ändern. Auch vor dem Hintergrund, dass der im BSIG fehlende Sektor der öffentlichen Verwaltung in der BMI-Definition erfasst ist, muss hinterfragt werden, inwieweit die uneinheitlich verwendeten Definitionen und Sektorzuteilungen von BMI und BSI der Schaffung von Rechtsklarheit und einheitlichen Strukturen dienen. Dies gilt umso mehr mit Blick auf ein möglicherweise zukünftiges KRITIS-Dachgesetz zum physischen Schutz kritischer Infrastrukturen.[36] Es braucht einen übergreifenden Gleichlauf der Sektoren und angesprochenen Stellen für physischen und sicherheitsrechtlichen Schutz, um die Resilienz kritischer Infrastrukturen in ihrer Gesamtheit effektiv zu stärken. Ein Gleichlauf darf aber nicht die Reduktion auf den kleinsten gemeinsamen Nenner bedeuten, sondern muss Sektoren wie die öffentliche Verwaltung als Ganzes integrieren.[37]

4.2 Systematische Kritik der Umsetzung in deutsches Recht

Auffällig beim Umgang mit den bestehenden nationalen Regelungen ist die an vielen Stellen unübersichtliche[38] und teilweise uneinheitliche Umsetzung der An-

[35] So auch [6, S. 34 f].

[36] Vgl. zu diesem aktuellen Vorhaben https://www.bmi.bund.de/DE/themen/bevoelkerungsschutz/schutz-kritischer-infrastrukturen/schutz-kritischer-infrastrukturen-node.html (abgerufen am 05.12.2022).

[37] Siehe zur fehlenden Einordnung der Öffentlichen Verwaltung als KRITIS kritisch *Begerow/Fekete/Lechleuthner/Rhyner* in [9, S. 16].

[38] Teilweise auch fehlerhaft: So verweist beispielhaft der Anhang 1 in der BSI-KritisV auf § 2 Abs. 5 Nr. 1, 2, wobei dies Abs. 6 sein müsste.

forderungen im IT-Sicherheitsrecht. Dies betrifft die wechselseitigen Regelungen von BSIG/BSI-KritisV mit fachgesetzlichen Pflichten solcher KRITIS-Betreiber, die auch anderen sektorspezifischen Pflichten unterliegen. Veranschaulicht werden kann das an Energieversorgungsnetzen. Können diese innerhalb der Systematik im BSI als kritische Infrastruktur identifiziert werden, muss folgend geprüft werden, ob sie nicht auch Regelungen nach § 11 EnWG unterfallen. Ist dies der Fall, sind zentrale Pflichten wie nach § 8a Abs. 1, 1a BSIG im Wesentlichen nicht anwendbar.[39] Vielmehr finden sich dann im vorrangigen § 11 EnWG eigenständige (und vom BSIG abweichende) Pflichten, obwohl es sich fraglos um eine kritische Infrastruktur handelt. Von der Anwendung ausgenommen ist daneben auch die Meldepflicht für (erhebliche) Störungen an das BSI nach § 8d Abs. 3 Nr. 2 i. V. m. § 8b Abs. 4, 4a BSIG. Gleichwohl finden sich für solche Energieversorgungsnetze, die auch als KRITIS nach dem BSIG gelten, in § 11 Abs. 1b, c EnWG besondere Pflichten,[40] darunter jene zuvor ausgeschlossene Meldeverpflichtung aus dem BSIG nahezu im Wortlaut, wobei jedoch das Wort kritische Infrastruktur mit Energieversorgungsnetzen ersetzt wird. Wünschenswert wäre hier eine Harmonisierung sowie Strukturierung der Begrifflichkeiten und Verweisketten der Fachgesetze.

Eine Harmonisierung sollte derweil nicht nur zwischen BMI und BSI, Fachgesetzen und dem BSIG, sondern auch zwischen dem BSIG und der BSI-KritisV angestrebt werden. Gerade vor dem Hintergrund der Definition und Bestimmung von kritischen Infrastrukturen erschwert die derzeitige Verweiskette eine dogmatisch klar nachzuvollziehende Lösung.

Die Verweiskette des § 2 Abs. 10 S. 2 BSIG i. V. m. § 10 Abs. 1 S. 1 BSIG soll den unbestimmten Rechtsbegriff der kritischen Infrastruktur konkretisieren. Für eine werthaltige begriffliche Klarheit sorgt die BSI-KritisV aber nicht. Lediglich die Verordnungsermächtigung des § 10 Abs. 1 S. 1 BSIG spricht hierzu. Danach sollen kritische Infrastrukturen in der RVO unter Festlegung von kritischen Dienstleistungen und einem bedeutenden Versorgungsgrad bestimmt werden, ohne dass diese klar als Tatbestandsmerkmale formuliert werden, oder die Ausfüllung der unbestimmten Rechtsbegriffe in § 2 Abs. 10 Nr. 2 BSIG aufgegriffen wird. Auch in der BSI-KritisV findet sich in den Begriffsbestimmungen nach § 1 BSI-KritisV keine Definition kritischer Infrastrukturen, die alle bisherigen Merkmale gebündelt zusammenführt. Dieser beschränkt sich auf Definitionen zu u. a. kritischen Dienstleistungen, Anlagen oder Schwellenwerten, wobei für kritische Dienstleistungen erstmals der Wortlaut der Definition aus § 2 Abs. 10 Nr. 2 BSIG wieder aufgenommen wird, ohne ihn zu konkretisieren.[41]

Die eigentliche Konkretisierung erfolgt dann in den sektorspezifischen Normen der Verordnung. Dabei verweisen die Bestimmungen aber nicht, wie zu erwarten, auf die normative Ausfüllung in § 1 Abs. 1 Nr. 3 BSI-KritisV, sondern nehmen

[39] Für die Pflicht zur Umsetzung IT-sicherheitsrechtlicher Maßnahmen ergibt sich das aus dem Ausschluss von § 8a Abs. 1 BSIG nach § 8d Abs. 2 Nr. 2 BSIG.

[40] Vgl. zur Darstellung *Beucher/Fromageau/Ehlen* in Kipker, Cybersecurity, 1. Aufl. 2020, Kap. 12 Rn. 114.

[41] Dienstleistungen, die zur Versorgung der Allgemeinheit dienen und deren Ausfall oder Beeinträchtigung zu erheblichen Versorgungsengpässen oder Gefährdungen der öffentlichen Sicherheit führen würde.

Bezug auf das Funktionieren des Gemeinwesens in § 2 Abs. 10 S. 1 Nr. 2 BSIG, das sich nur durch weiteren Verweis über § 10 Abs. 1 S. 1 BSIG erschließen lässt. Obwohl es keine Begriffsdefinition für kritische Infrastrukturen in § 1 BSI-KritisV gibt, definieren die sektorspezifischen Normen im jeweils letzten Absatz den Begriff kritische Infrastrukturen im jeweiligen Sektor. Auch hier erfolgt jedoch keine Zusammenführung der normativen Tatbestandsmerkmale. Vielmehr liegen kritische Infrastrukturen danach vor, wenn sie einer Kategorie im Anhang zuzuordnen sind und einen Schwellenwert überschreiten, wenngleich eine Einordnung in Kategorien oder die dogmatisch nähere Zusammenführung bis dahin noch nicht erfolgt ist. So verschleiert die derzeitige Regelung jede qualitative Zuschreibung von Kritikalität hinter Tabellen und Zahlen: Was an einer kritischen Infrastruktur kritisch sein soll, steht daher letztlich im Gusto des Verordnungsgebers. Die Definition der kritischen Infrastrukturen täuscht ein arbeitsteiliges Regelungssystem zwischen Legislative und Exekutive daher letztlich nur vor. Aufgrund der klaren Schwellenwerte der BSI-KritisV entscheidet die Verordnung letztlich alleine über die Kritikalität. Dass die Zuweisung der Kritikalität daher noch vom Parlamentsgesetz des BSIG gesteuert wird, ist allenfalls frommer Wunsch. Angesichts der Bedeutung kritischer Infrastrukturen und im Lichte der Wesentlichkeitstheorie[42] nach Art. 20 GG ist dies mehr als nur bedenklich.

Dieses gestörte Zusammenspiel der Ermächtigungsgrundlage von § 2 Abs. 10 S. 2 BSIG i. V. m. § 10 Abs. 1 S. 2 BSIG und der BSI-KritisV führt zur vollkommenen Konturlosigkeit der Definition kritischer Infrastrukturen in § 2 Abs. 10 BSIG: Nach § 2 Abs. 10 S. 2 BSIG soll die BSI-KritisV kritische Infrastrukturen „näher" bestimmen. Das eigentlich kumulativ gestaltete Verhältnis zwischen § 2 Abs. 10 S. 1 Nr. 1 und Nr. 2 BSIG leidet aber an einer Schieflage zugunsten einer quantitativen Bestimmung der Kritikalität. Ein komplexitätsreduzierender und gleichzeitig begriffliche Klarheit schaffender Ausweg wäre es, die Verweiskette mit einer konkreten Definition kritischer Infrastruktur zu vereinfachen und an diese Definition kasuistische Detailregelungen in einer Verordnung anzuknüpfen. Diese kann weiterhin einen Schwerpunkt auf quantitative Festlegungen setzen, sofern qualitativen Maßstäben in der gesetzlichen Definition in hinreichend justiziabler Weise Rechnung getragen wird. So würden zentrale Entscheidungen durch das BSIG getroffen und Details auf dem Verordnungswege geregelt, sodass der Wesentlichkeitsgrundsatz Beachtung findet.

4.3 Fokus auf Schwellenwerte und quantitative Bestimmung

Das eben dargestellte Ergebnis dieser Ausgestaltung, der faktisch rein quantitative Ansatz zur Bestimmung kritischer Infrastrukturen, gilt es als zielführende Umsetzung der NIS-RL zu hinterfragen. Die NIS-RL gibt für die Bestimmung einen Katalog aus qualitativen und quantitativen Merkmalen vor, die nach Art. 4 Nr. 4 i. V. m. Art. 5 Abs. 2 und Annex II der NIS-Richtlinie nicht zwingend kumulativ erfüllt sein müssen, sondern gerade verschiedene Merkmale für die individuelle Bestimmung von Kritikalität zur Hand geben. Obwohl man sich in Deutschland nach der

[42] Siehe für Einzelheiten hierzu bei *Kotzur* in [23], GG Art. 20 Rn. 156.

Gesetzesbegründung dafür entschied, qualitative und quantitative Elemente durch die normative Begriffsdefinition von Einrichtungen mit hoher Bedeutung für das Gemeinwesen und die zu erreichenden Schwellenwerte gleichermaßen einzubinden, realisiert sich in der Umsetzung ein vordergründig rein quantitativer Ansatz.[43] Denn die Voraussetzungen müssen kumulativ vorliegen, sodass bei Unterschreiten eines bedeutenden Versorgungsgrads durch Erreichen des Schwellenwerts eine Einordnung als kritische Infrastruktur de facto ausscheidet, auch wenn mehrere qualitative Elemente für eine kritische Einordnung sprechen und diese normativ leicht zu begründen wäre. Mit den Sektorstudien des BSI lagen auch qualitative Daten zur Bestimmung der BSI-KritisV vor.[44] Sie dogmatisch aufzubereiten und in Normtext zu gießen wäre anspruchsvoll aber lohnenswert gewesen.

Die Problematik spitzt sich durch sehr hoch angesetzte Regelschwellenwerte mit 500.000 versorgten Personen weiter zu, die aus rechtspolitischer Sicht überdacht werden sollten:

Gerade Sektoren wie die Wasserversorgung sind durch zahlreiche kleine kommunale Versorger geprägt, sodass insgesamt überhaupt nur 1 % der Unternehmen den Regelschwellenwert von 500.000 erreichen; in einigen Bundesländern lässt sich kein Unternehmen im Bereich der Wasserversorgung finden, das den Schwellenwert überschreitet.[45] Dies ist auch mit Blick auf andere Sektoren problematisch, sobald man den Fokus auf die wenigen Ballungsräume verlässt; so waren die bei der Flutkatastrophe im Ahrtal betroffene Infrastrukturen (Stromversorgung, Wasser) aufgrund der geringeren Versorgungsbedeutung nicht als kritische Infrastruktur zu werten[46], wenngleich sich für die betroffene Bevölkerung in den folgenden Monaten die Versorgung mit Wasser, Strom und Nahrung als bedeutendes Problem herausstellte. Eine solche Lösung kann auch dazu führen, dass solche Infrastrukturen vom Anwendungsbereich ausgeschlossen werden, deren Ausfall durch mittelbare Auswirkungen bzw. Domino- oder Kaskadeneffekte kritische Folgen in anderen Sektoren verursachen können.[47] Gerade solche Effekte können aber nicht nur quantitativ bestimmt werden, sondern ergeben sich aus (unterschiedlich starken) Interdependenzen verschiedener Sektoren und Einrichtungen.[48]

[43] So i.E. auch [11, S. 372 (374)]; a.A. ([17, S. 648] Fn. 33).

[44] Siehe [17, S. 648 (651)].

[45] *Fischer* in [12], § 13 Rn. 43;
Begerow/Fekete/Lechleuthner/Rhyner in [9, S. 17].

[46] S. dazu *Fischer* in [12], § 13 Rn. 43;
Begerow/Fekete/Lechleuthner/Rhyner in [9, S. 16].

[47] [21, S. 429] und [11, S. 372 (374)].

[48] Dieses Merkmal wurde in der NIS-RL als qualitatives Merkmal bereits angeführt.

5 Änderungen durch die NIS2-RL

Am 16.12.2020 hat die EU-Kommission den Entwurf der Richtlinie vorgestellt. Am 13.05.2022 haben Rat und Parlament eine Einigung im Trilog erzielt,[49] die der federführende ITRE-Ausschuss am 13.07.2022 angenommen hat. Das Parlament hat der endgültigen Fassung im Plenum am 10.11.2022 zugestimmt, der Rat am 28.11.2022. Eine Veröffentlichung im Amtsblatt ist zum Zeitpunkt der Einreichung des Beitrags noch nicht erfolgt (nunmehr jedoch mit der Richtlinie 2022/2555 geschehen). Im Anschluss an die formelle Annahme durch Rat und Parlament haben die Mitgliedsstaaten 21 Monate Zeit für die Umsetzung in nationales Recht.

5.1 Überblick der Neuregelung

Neben zentralen Änderungen im Anwendungsbereich gegenüber der NIS-RL, zur Sicherstellung eines hohen gemeinsamen Cybersicherheitsniveaus in der Union (Art. 1 Abs. 1 NIS2-RL) regelt die NIS2-Richtlinie Pflichten zum Austausch von Cybersicherheitsinformationen neu und normiert, wie auch schon die NIS-RL, die Pflicht für Mitgliedsstaaten Cybersicherheitsstrategien zu verabschieden, sowie nationale Behörden und Reaktionsteams für IT-Sicherheitsvorfälle zu benennen. Aufgrund des Gegenstands dieser Abhandlung konzentriert sich die weitere Betrachtung hier jedoch auf die in Art. 1 Abs. 2 lit. b NIS2-RL vorgesehene Ausweitung der kritischen Infrastrukturen, die zur Meldung von Vorfällen und einem Cybersicherheitsrisikomanagement verpflichtet werden sollen.

5.2 Ausweitung des Begriffs der kritischen Infrastruktur

Auch wenn sich der Terminus der kritischen Infrastruktur in der NIS2-Richtlinie an keiner Stelle finden lässt, geht es der Richtlinie genau um diese.[50] Während sich der deutsche Gesetzgeber bei der Umsetzung der NIS-RL für den Begriff der kritischen Infrastruktur entschied, wählte diese den Terminus „wesentliche Dienste“ (Art. 14 NIS-RL). Die Begrifflichkeiten weichen im Ergebnis aber nur leicht voneinander ab.[51] Die NIS2-Richtlinie etabliert nun die Begriffe der „wesentlichen Einrichtungen“ und der „wichtigen Einrichtungen“, um kritische Infrastrukturen zu definieren. Von der Unterscheidung zwischen wesentlichen Diensten und digitalen Diensten löst sich die NIS2-RL ausdrücklich.[52]

[49] https://ec.europa.eu/commission/presscorner/detail/de/IP_22_2985; https://www.consilium.europa.eu/de/press/press-releases/2022/05/13/renforcer-la-cybersecurite-et-la-resilience-a-l-echelle-de-l-ue-accord-provisoire-du-conseil-et-du-parlement-europeen/pdf (abgerufen am 05.12.2022).

[50] COM(2020) 823 final, S. 2.

[51] Siehe zur begrifflichen Umsetzung durch den deutschen Gesetzgeber u. a. *Buchberger* in [18], BSIG § 2 Rn. 12; [17, S. 648 (650)]; [11, S. 372 (373)]; [22, S. 355 (356)] sowie [16, S. 148 (149)]mit einer übersichtlichen Gegenüberstellung der jeweils erfassten Sektoren.

[52] ErwGr. 6 NIS2-RL.

5.2.1 Systematik und Schwellenwerte

Die Begriffe der wesentlichen und wichtigen Einrichtungen definiert die NIS2-Richtlinie in Art. 3 Abs. 1 und Abs. 2 und damit außerhalb der restlichen Begriffsbestimmungen in Art. 6. In der Vorschlagsfassung der Kommission waren diese noch systematisch gelungen in Art. 4 Abs. 25 und 26 geregelt, die recht lapidar in den Anhang I für die wesentlichen Einrichtungen, und in Anhang II für die wichtigen Einrichtungen verweisen. Mit der endgültigen Fassung haben sich diese Definitionen allerdings verkompliziert:

Art. 3 Abs. 1 NIS2-RL verweist für die wesentlichen Einrichtungen nicht mehr ausschließlich auf den Anhang I, sondern benennt auch einzelne Adressaten in den lit. b bis g, unter ständiger Bezugnahme zum Anwendungsbereich in Art. 2 Abs. 2 NIS2-RL. Der Anhang I regelt nun auch nicht mehr exklusiv wesentliche Einrichtungen, sondern enthält „Sektoren mit hoher Kritikalität". Besonders hervorzuheben ist hier Art. 3 Abs. 1 lit. d NIS2-RL, der Einrichtungen der öffentlichen Verwaltung nach Art. 2 Abs. 2 lit. f Zif. i NIS2-RL einbezieht. Nach Art. 3 Abs. 1 lit. e NIS2-RL finden sich wesentliche Einrichtungen auch im Anhang II unter den „sonstigen kritischen Sektoren", wenn die Mitgliedsstaaten sie nach Art. 2 Abs. 2 lit. b bis e als wesentliche Einrichtungen eingestuft haben. Wichtige Einrichtungen im Sinne des Art. 3 Abs. 2 NIS2-RL sind in den Anhängen I und II zu finden, sofern sie nicht bereits wesentliche Einrichtungen nach Abs. 1 sind. Dabei beschränkt sich die Begriffsbestimmung hinsichtlich der Kritikalität auf den bloßen Verweis in die Anhänge I und II zur Richtlinie. Auch dort ist keine weitere Erläuterung zu finden, sondern lediglich eine tabellarische Aufzählung. Damit fehlt dem Normtext jede normative Zuschreibung, wie sie die NIS-RL mit der Unerlässlichkeit eines Dienstes für die Aufrechterhaltung kritischer gesellschaftlicher und/oder wirtschaftlicher Tätigkeiten bei Art. 4 Nr. 4 i. V. m. Art. 5 Abs. 2 NIS-RL beispielsweise etabliert hat. Die Erwägungsgründe sind hier aber aufschlussreicher.

Zwischen „wesentlichen" und „wichtigen" Einrichtungen gibt es ein Rangverhältnis[53]: Dieses ist abhängig vom „Grad der Kritikalität des Sektors [...] sowie dem Grad der Abhängigkeit anderer Sektoren."[54] Die NIS2-RL hat also erstmals auch die systemische und nicht nur die konsequenzbasierte Kritikalität im Blick. Zwischen den wesentlichen und wichtigen Einrichtungen besteht kein Unterschied hinsichtlich der Risikomanagementanforderungen und Meldepflichten, jedoch beim Aufsichts- und Sanktionsregime. Kapitel IV der NIS2-RL, insb. Art. 21 und 23, gelten daher für beide Kategorien von Einrichtungen, während Kapitel VII wesentliche Einrichtungen in Art. 32 deutlich mehr Aufsichtsmaßnahmen unterwirft als wichtige Einrichtungen in Art. 33.

Weiter sieht die NIS2-RL keinen Ermittlungsprozess zur Einstufung der Kritikalität durch die Mitgliedsstaaten mehr vor, wie ihn Art. 5 Abs. 1 NIS-RL ermöglicht hat.[55] Eine Umsetzung mittels Versorgungsschwellenwerten, wie sie die BSI-KritisV ermöglichte, bleibt dem nationalen Gesetzgeber zugunsten einer Harmoni-

[53] Dieses wird im englischen Wortlaut der Richtlinie „essential" und „important" auch deutlicher.

[54] ErwGr. 15 NIS2-RL.

[55] ErwGr. 7 NIS2-RL.

sierung der Cybersicherheitsanforderungen im Binnenmarkt verwehrt. Als einziges Kriterium für das Überschreiten einer Kritikalitätsschwelle dient daher in Zukunft die unionsrechtliche KMU-Definition[56]. Denn nach Art. 2 Abs. 1 S. 1 NIS2-RL finden die Regelungen über wesentliche und wichtige Einrichtungen keine Anwendung auf kleine und Kleinstunternehmen. Gegenüber der Kommissionsfassung ist dies nun aber nicht mehr negativ, sondern positiv formuliert, also ab der Schwelle der mittleren Unternehmen. Nach Art. 2 der europäischen KMU-Definition liegt die Grenze daher bei 50 Mitarbeitern oder einem Jahresumsatz oder einer Jahresbilanz ab 10. Mio EUR. Ausgenommen ist dabei[57] analog zur aktuellen deutschen Regelung im BSIG nach Art. 2 Abs. 1 S. 2 NIS2-RL insb. Art. 3 Abs. 4 der KMU-Empfehlung, sodass die Einordnung als KMU und Ausnahme von der Verpflichtung unabhängig von einer Beteiligung öffentlicher Unternehmen gilt. Maßgeblich ist vielmehr allein der Schwellenwert der Mitarbeiter und des Umsatzes. Für bestimmte Einrichtungen sieht Art. 2 Abs. 2 vor, dass sie unabhängig ihrer Größe im Anwendungsbereich der Richtlinie sein sollen. Die gilt beispielweise auch für die öffentliche Verwaltung nach Art. 2 Abs. 2 lit. f NIS2-RL. Auffällig ist in diesem Zusammenhang, dass mit Art. 2 Abs. 1 und Art. 3 Abs. 1 lit. a NIS2-RL nun doppelt an die Schwelle KMU-Definition angeknüpft wird, was regelungstechnisch nicht notwendig gewesen wäre.

5.2.2 Sektoren

Handlungsleitend beim Entstehungsprozess der NIS2-RL war die Erkenntnis, dass der Anwendungsbereich der NIS-RL durch zunehmende Digitalisierung zu eng wurde.[58] Primäres Instrument zur Verbesserung eines gemeinsamen Cybersicherheitsniveaus in der Union ist die Ausweitung der erfassten Sektoren, um einen größeren Teil der Wirtschaft abzudecken.[59] Entsprechend der neu eingeführten Unterteilung in wesentliche und wichtige Einrichtungen kommen einige neue kritische Sektoren hinzu: Bei den wesentlichen Einrichtungen im Anhang 1 der RL werden die Abwasserwirtschaft (Nr. 7), die Verwaltung von IKT-Diensten (Nr. 9), die öffentliche Verwaltung (Nr. 10) und der Sektor Weltraum (Nr. 11) hinzugefügt. Auch der Teilsektor Wasserstoff ist neu. In den Sektoren der Gesundheit und der digitalen Infrastruktur sind auch zahlreiche bisher nicht erfasste Einrichtungen erstmalig erfasst. Weitere Sektoren, die den wichtigen Einrichtungen zugeordnet werden, finden sich in Anhang II mit Post- und Kurierdiensten, der Abfallbewirtschaftung, der Produktion, Herstellung und dem Handel mit chemischen Stoffen, der Vertrieb von Lebensmitteln, das verarbeitende Gewerbe, Anbieter digitaler Dienste sowie Forschung.[60]

[56] Empfehlung 2003/361/EG der Kommission vom 6. Mai 2003 betreffend die Definition der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen (ABl. L 124 vom 20.05.2003, S. 36).

[57] Auch nach Empfehlung der kommunalen Spitzenverbände, vgl. [4].

[58] So ausdrücklich COM(2020) 823 final, S. 5.

[59] ErwGr. 6 der NIS2-RL.

[60] Siehe für eine anschauliche Übersicht zu den Sektoren der NIS2-RL mit Abweichungen durch die aktuelle Fassung der Richtlinie hier: [15].

Was den Sektor der öffentlichen Verwaltung betrifft, kann der Richtlinie jedoch aus Kompetenzgründen eine umfassende Regelung der öffentlichen Verwaltung nicht gelingen: Art. 2 Abs. 7 NIS2-RL klammert den Bereich der Sicherheitsbehörden aus.[61] Auch die Definition der Einrichtungen der öffentlichen Verwaltung in Art. 6 Abs. 35 NIS2-RL klammert mit Justiz, Parlamenten und Zentralbanken definitiv essenzielle staatliche Einrichtungen aus. Als Binnenmarktmaßnahme[62] auf Basis des Art. 114 AEUV fordert Art. 6 Abs. 35 lit. d NIS2-RL die Befugnis, europäische Grundfreiheiten zu beschränken, um Einrichtung der öffentlichen Verwaltung im Sinne der Richtlinie zu sein. Die Auslegung dieser „Befugnis" entscheidet in erheblichem Maße über den Anwendungsbereich.

Obwohl sich der Anwendungsbereich erheblich erweitert, sind einige der mit der NIS2-RL neu hinzukommenden Sektoren bereits umgesetzt. Dies betrifft insbesondere auch die Regelungen, die für Unternehmen im besonderen öffentlichen Interesse nach § 8f BSIG gelten. Diese erfassen bisher nach § 2 Abs. 14 BSIG drei Arten von Unternehmen: Solche, die Güter nach § 60 Abs. 1 Nr. 1, 3 AWV herstellen (Rüstungsbetriebe[63] und Hersteller von IT-Sicherheitsfunktionen für staatliche Verschlusssachen), die nach der Wertschöpfung größten Unternehmen oder Zulieferer sowie insb. Chemiebetriebe nach der Störfall-VO. Für diese finden sich bereits wesentliche Regelungen, die jedoch durch die Einordnung als kritische Infrastruktur angepasst werden müssen und weitergehende Pflichten für die Betreiber nach sich ziehen. Erhebliche Erweiterungen ergeben sich durch die Aufnahme des produzierenden Gewerbes und des industriellen Sektors. Als Teilsektoren werden dazu die Herstellung von Medizinprodukten, Datenverarbeitungsgeräten sowie elektronischen und optischen Erzeugnissen, elektrischen Ausrüstungen, der Maschinenbau, die Herstellung von Kfz(-Teilen) und der Fahrzeugbau benannt. Hier dürfte sich der Anwendungsbereich im Vergleich zu den bisherigen Unternehmen insgesamt erheblich erweitern und viele mittelständische Unternehmen gänzlich neu betreffen. Gar nicht umgesetzt sind bisher die Sektoren Forschung, sowie die öffentliche Verwaltung. Für diese kann – wenn auch nur für Stellen des Bundes – bisher nur an die allgemeinen IT-Sicherheitsregelungen wie §§ 4 und 8 BSIG angeknüpft werden. § 8 Abs. 1 S. 1 Nr. 3 BSIG zeigt aber auch eine verpasste Chance der NIS2-RL auf: Hiernach sind bereits heute auch Mindeststandards an öffentliche Unternehmen des Bundes zu stellen, die IT-Dienstleistungen für die Bundesverwaltung erbringen. Anknüpfend an den systemischen Kritikalitätsbegriff (s. oben) handelt es sich bei derartigen Unternehmen – und das nicht nur auf Bundesebene – um kritische Infrastrukturen, die im Anhang I zur NIS2-RL bei den digitalen Infrastrukturen unter Nr. 8 explizit Berücksichtigung hätten finden können. Störungen bei den IT-Dienstleistern der Verwaltung können die Arbeitsfähigkeit dieser nämlich im großen Umfang einschränken. Da Unternehmen Adressaten einer Regelung wären, würden Kompetenzen hier eine geringere Rolle spielen und umfassendere Regelungen ermöglichen.

[61] Siehe hierzu auch Art. 2 Abs. 6 NIS2-RL.

[62] Dass die NIS2-RL vorrangig eine Binnenmarktmaßnahme ist, verdeutlicht Art. 1 Abs. 1 NIS2-RL in seiner endgültigen Fassung gegenüber der Fassung im Vorschlag der Kommission.

[63] *Deusch/Eggendorfer* in [20], 50.1 Rn. 415.

6 Bewertung der Änderungen und Ausblick

Auch wenn durch die IT-Sicherheitsgesetze in Deutschland bereits einige der neuen Sektoren nach der NIS2-RL ganz oder teilweise umgesetzt sind – insbesondere durch die Unternehmen im besonderen öffentlichen Interesse – wird es zu massiven Ausweitungen bei IT-Sicherheitspflichten kommen. Angesichts der oben geübten Kritik ist zu begrüßen, dass große Teile der öffentlichen Verwaltung ohne Rücksicht auf die Größe der jeweiligen Verwaltungseinheit künftig zur kritischen Infrastruktur zählen. Die oben beschriebenen Einschränkungen bei der Definition von Einrichtungen der öffentlichen Verwaltung trüben dieses Bild jedoch. Sie sind kompetenziell zwar folgerichtig, sollten den deutschen Gesetzgeber aber im Sinne der notwendigen Resilienz staatlicher Stellen nicht dazu verleiten, allein die nach Art. 5 NIS2-RL erforderliche Mindestharmonisierung umzusetzen. Insbesondere Art. 2 Abs. 5 NIS2-RL ermutigt die Mitgliedsstaaten jedenfalls zu diesem Schritt.

Einen echten Beitrag zu einem unionsweit einheitlichen Begriff kritischer Infrastruktur stellt die Verwendung der Schwellenwerte der europäischen KMU-Definition dar. Schatten dieser Lösung ist jedoch, dass Mitarbeiter und Umsatz – gerade im ländlichen Raum, aber auch aufgrund zunehmender Automatisierung – als Kennzahlen nicht zwingend geeignet sind, kritische Infrastrukturen zu identifizieren. Was die Nichtanwendbarkeit des Art. 3 Abs. 4 der europäischen KMU-Definition durch Art. 2 Abs. 1 S. 2 NIS2-RL[64] angeht, so wird das Niveau der IT-Sicherheit eher gesenkt, da viele kommunale Unternehmen der Daseinsvorsorge so gänzlich dem Anwendungsbereich entgehen dürften. Die kommunalen Spitzenverbände argumentieren hier mit dem Verhältnismäßigkeitsprinzip, da kleine Versorger mit Pflichten überbürdet sein könnten.[65] Dies überzeugt deshalb nicht, weil die Notwendigkeit staatlicher Beteiligung oft Indiz ist, dass Infrastrukturen nicht wirtschaftlich betrieben werden können. Die betroffenen, oft ländlich geprägten, Regionen würde ein Ausfall der Infrastruktur daher besonders hart treffen. Weshalb auch hier die Anforderungen an ausreichende IT-Sicherheit verhältnismäßig sind.

Abschließend gilt zu sagen, dass die NIS2-RL die von Risikomanagementanforderungen und Meldungen Betroffenen ausweiten wird. Zu einem klaren Begriff kritischer Infrastruktur wird die Richtlinie jedoch nicht beitragen: Einen normativ fassbaren Begriff enthält die NIS2-RL nicht. Welche Infrastrukturen wirklich kritisch sind, bestimmt zukünftig eine Aufzählung von Sektoren. Einen Impuls zur qualitativen Begriffsbildung kritischer Infrastrukturen setzt die NIS2-RL daher leider nicht, sondern ist von einem wenig überzeugenden, eher verwirrenden Zusammenspiel der Art. 2 und 3, sowie der Anhänge zur Richtlinie geprägt. Die Kommissionsfassung der NIS2-RL enthielt zwar keine qualitativen Zuschreibungen, hätte jedoch zu einer Vereinfachung des Begriffs der kritischen Infrastrukturen bei der nationalen Umsetzung eingeladen. Die Definition von wesentlichen und wichtigen Einrichtungen der endgültigen Fassung setzt jedoch einige Anreize, die Komplexität infrastruktureller Vulnerabilitäten und Interdependenzen beim Begriff der kritischen Infrastruktur im

[64] S. 3 wurde erst im Rahmen der Trilog-Verhandlungen in den Richtlinientext aufgenommen.

[65] Vgl. https://www.vku.de/fileadmin/user_upload/Verbandsseite/Themen/Digitalisierung/NIS_Position_paper_BV_VKU_DE.pdf, S. 4 (abgerufen am 05.12.2022).

deutschen Recht nachzubilden. Eine normative Bestimmung der Kritikalität wird dadurch unnötig erschwert. Auch die CER-Richtlinie wird nach ihrem derzeitigen Stand wohl keinen gewinnbringenden begrifflichen Beitrag leisten. Anlass zu Optimismus bietet aber das aktuelle Vorhaben der Bundesregierung zur Schaffung eines KRITIS-Dachgesetzes: Nach den Eckpunkten[66] des BMI für dieses Vorhaben soll zentraler Regelungsgehalt des Gesetzes werden, kritische Infrastrukturen systematisch und umfassend zu identifizieren und hierbei auch qualitative Kriterien zu berücksichtigen. Unter Einhaltung der europarechtlichen Anforderungen durch die CER- und NIS2-Richtlinie, besteht also die Chance eine dogmatisch befriedigende Antwort darauf zu finden, was an kritischen Infrastrukturen genau kritisch ist. Möge zumindest der deutsche Gesetzgeber sie nutzen, wenn es der europäische schon nicht vermag.

Funding Open Access funding enabled and organized by Projekt DEAL.

Literatur

1. Bouchon (2006) The vulnerability of interdependent critical infrastructures systems: epistemological and conceptual state-of-the-art
2. Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (2020) 10-Jahre KRITIS-Strategie, Stand Februar 2020
3. Bundesministerium des Innern und für Heimat (2009) Nationale Strategie zum Schutz Kritischer Infrastrukturen (KRITIS-Strategie)
4. Bundesvereinigung der Kommunalen Spitzenverbände Stellungnahme für eine Richtlinie über Maßnahmen für ein hohes gemeinsames Maß an Cybersicherheit in der gesamten Union (NIS 2) vom 16.12.2020. https://www.vku.de/fileadmin/user_upload/Verbandsseite/Themen/Digitalisierung/NIS_Position_paper_BV_VKU_DE.pdf. Zugegriffen: 5. Dez. 2022
5. Dreier (2015) Grundgesetz-Kommentar, 3. Aufl. Mohr Siebeck
6. Engels (2018) Relevante Beziehungen. Vom Nutzen des Kritkalitätskonzepts für Geisteswissenschaftler. In: Engels, Nordmann (Hrsg) Was heißt Kritikalität? Zu einem Schlüsselbegriff der Debatte um Kritische Infrastrukturen. transcript
7. Europäische Kommission Kritische Infrastruktur: Kommission beschleunigt Arbeiten. https://ec.europa.eu/commission/presscorner/detail/de/ip_22_6238. Zugegriffen: 5. Dez. 2022

[66] In Entwurfsfassung abrufbar unter: https://intrapol.org/wp-content/uploads/2022/11/Eckpunkte-fuer-ein-KRITIS-Dachgesetz-Stand-25.11.2022.pdf. Siehe eine erste Bewertung bei [13].

8. Fekete (2018) Relevanzbewertungsbefähigung und Ohnmachtserfahrung: Infrastruktur, Wissen und Zeitkritikalität in Engels/Nordmann (Hrsg.), Was heißt Kritikalität? Zu einem Schlüsselbegriff der Debatte um Kritische Infrastrukturen. transcript
9. Fekete (2022) Kritische Infrastruktur und Versorgung der Bevölkerung, 1. Aufl.
10. Folkers (2018) Was ist kritisch an Kritischer Infrastruktur? Kriegswichtigkeit, Lebenswichtigkeit, Systemwichtigkeit und die Infrastrukturen der Kritik. In: Engels, Nordmann (Hrsg) Was heißt Kritikalität? Zu einem Schlüsselbegriff der Debatte um Kritische Infrastrukturen. transcript
11. Gehrmann, Klett (2017) IT-Sicherheit in Unternehmen – Weiterhin viel Unsicherheit bei der Umsetzung des IT-Sicherheitsgesetzes. K&R 2017, 372 ff.
12. Hornung, Schallbruch (2021) IT-Sicherheitsrecht, Praxishandbuch, 1. Aufl. Nomos
13. Kipker, Dittrich (2022) Neues BMI-Eckpunktepapier für ein KRITIS-Dachgesetz: Mehr physischer Schutz für Kritische Infrastrukturen. MMR-Aktuell 2022, 454186
14. Kipker (2020) Cybersecurity, 1. Aufl. C.H. Beck
15. Openkritis https://www.openkritis.de/it-sicherheitsgesetz/eu-nis-2-direktive-kritis.html. Zugegriffen: 5. Dez. 2022
16. Rosenthal, Trautwein (2017) NIS-Richtlinie und IT-Sicherheitsgesetz in 2017. PinG 2017, 148 ff.
17. Schallbruch (2017) IT-Sicherheitsrecht – Schutz kritischer Infrastrukturen und staatlicher IT-Systeme: Zur Entwicklung des IT-Sicherheitsrechts in der 18. Wahlperiode (Teil 1). CR 2017, 648 ff.
18. Schenke, Graulich, Ruthig (2019) Sicherheitsrecht des Bundes, 2. Aufl. C.H. Beck
19. Schoch (2008) Gewährleistungsverwaltung: Stärkung der Privatrechtsgesellschaft? NVwZ 2008, 241 ff.
20. Taeger, Pohle (2022) Computerrechtshandbuch, Informationstechnologie in der Rechts- und Wirtschaftspraxis. 37. EL. C.H. Beck
21. Voigt (2016) Dauerbrenner IT-Sicherheit – Nun macht Brüssel Druck. MMR 2016, 429 ff.
22. Voigt, Gehrmann (2016) Die europäische NIS-Richtlinie: Neue Vorgaben zur Netz- und IT-Sicherheit. ZD 2016, 355 ff.
23. v. Münch, Kunig (2021) Grundgesetz-Kommentar, 7. Aufl. C.H. Beck
24. Voßkuhle (2003), Beteiligung Privater an der Wahrnehmung öffentlicher Aufgaben und staatliche Verantwortung. VVDStRL 62, S. 266 ff.