Nomos **KOMMENTAR**

Schröder | Hartl [Hrsg.]

Cyber Resilience Act

Cyberresilienz-Verordnung

Nomos

Nomos**KOMMENTAR**

Prof. Dr. Meinhard Schröder
Dr. Korbinian Hartl [Hrsg.]

Cyber Resilience Act

Cyberresilienz-Verordnung

RA **Dr. Tobias Ackermann**, München | RA **Dr. Korbinian Hartl**, München | RA **Stefan Hessel**, LL.M., Saarbrücken | ORR **Dr. Kai Hofmann**, Dresden | **Prof. Dr. Lukas Iffländer**, Hochschule für Technik und Wirtschaft Dresden | **Dr. Jonas Jossen**, Mag. rer. publ., Bundesamt für Sicherheit in der Informationstechnik (BSI) | **Jan Philip Kühne**, Universität Passau | StA **Julien Mehnert** | SyndikusRA **Dr. Christian Piovano**, Friedrichshafen | RA **Manuel Poncza**, Köln | RA **Stephan Schmidt**, FAIT-Recht, Mainz | RAin **Dr. Kristina Schreiber**, FAinVerwR, Köln | **Prof. Dr. Meinhard Schröder**, Universität Passau | RA **Dr. Paul Vogel**, LL.M. Eur., München | RA **Dr. Gerhard Wiebe**, Berlin

Nomos

Zitiervorschlag: NK-CRA/Bearbeiter Art ... Rn. ...

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

ISBN 978-3-7560-0246-7

1. Auflage 2026

Vorwort

Sehr geehrte Leserinnen, sehr geehrte Leser,

Cybersicherheit stellt nicht nur eine der größten Herausforderungen für die digitale Gesellschaft dar, sondern hat sich längst als eigenständiges, durchaus vielfältiges und fragmentiertes Rechtsgebiet etabliert. Mit der Cyberresilienz-Verordnung (CRA) hat der europäische Gesetzgeber nun einen Rahmen geschaffen, der bisherige Lücken im Cybersicherheits-Recht schließen soll: Vernetzte Produkte sind allgegenwärtig und werden in Zahl und Vielfalt in den kommenden Jahren nur weiter exponentiell zunehmen. Schwachstellen bergen erhebliche wirtschaftliche und gesellschaftliche Risiken. Inzwischen ist klar, dass die Gewährleistung von Cybersicherheit nicht allein eine Frage der Vertragsgestaltung, sektorspezifischer Sonderregulierung oder des Datenschutzes sein kann.

Mit dem CRA wachsen Produktrecht und Digitalgesetzgebung zusammen, was für die Praxis tiefgreifende Veränderungen bedeutet: Hersteller und andere Wirtschaftsakteure stehen vor neuen Pflichten, die weit über bisherige Anforderungen hinausgehen. Auch bleibt abzuwarten, wie die Rechtsprechung den CRA systematisch in das Gefüge der europäischen Digitalregulierung einordnen wird.

Angesichts dieser Unsicherheiten soll der Kommentar Ihnen eine umfassende Orientierung im CRA bieten. Unser Dank gebührt zunächst den Autorinnen und Autoren, die mit Ihrer Fachkompetenz und praktischen Erfahrung diesen Kommentar ermöglicht haben und tragen. Wir sind froh, dass Experten aus der rechtsanwaltlichen Praxis, „digitalnahen“" Behörden und der Wissenschaft bereit waren, ihr Wissen zu teilen und dieses Werk in Angriff zu nehmen.

Unser besonderer Dank gilt dem Nomos-Verlag für die immer entschlossene Unterstützung dieses Projekts und die verlässliche Begleitung bis zur Publikation. Hervorheben möchten wir insbesondere Herrn Dr. Ganzhorn, der die Konzeption des Kommentars maßgeblich gefördert, die Abstimmung zwischen Herausgebern, Autorinnen und Autoren mitkoordiniert und damit ganz wesentlich zum Gelingen des Werkes beigetragen hat.

Der Kommentar befindet sich auf dem Stand von Dezember 2025. Anregungen und Kritik sind herzlich willkommen.

Passau/München März 2026 *Meinhard Schröder und Korbinian Hartl*

Inhaltsverzeichnis

Kapitel III Konformität des Produkts mit digitalen Elementen

Kapitel IV Notifizierung von Konformitätsbewertungsstellen

Kapitel V Marktüberwachung und Durchsetzung

Autorinnen und Autoren

Dr. Tobias Ackermann Rechtsanwalt, München	Art. 47–50
Dr. Korbinian Hartl Rechtsanwalt, München	Art. 1 (mit *Schröder*)
Stefan Hessel, LL.M. Rechtsanwalt, Saarbrücken	Art. 3 Nr. 19, 27 Art. 32–34
Dr. Kai Hofmann ORR, Dresden	Art. 2 Art. 3 Nr. 1, 2, 23-25, 32, 34, 35, 47 Art. 3 Nr. 3, 5–11, 39 (mit *Iffländer*) Art. 4, 5 Art. 6–8 (mit *Iffländer*) Art. 9–12 Art. 13 Rn. 66–74 (mit *Iffländer*)
Prof. Dr. Lukas Iffländer Hochschule für Technik und Wirtschaft Dresden	Art. 3 Nr. 3, 5–11, 39 (mit *Hofmann*) Art. 6–8 (mit *Hofmann*) Art. 13 Rn. 66–74 (mit *Hofmann*)
Dr. Jonas Jossen, Mag. rer. publ. Bundesamt für Sicherheit in der Informationstechnik (BSI)	Art. 3 Nr. 26, 28 Art. 35–38, 51
Jan Philip Kühne Universität Passau	Art. 3 Nr. 18 Art. 59–71
Julien Mehnert Staatsanwalt	Art. 3 Nr. 12, 13, 15, 16, 20, 21, 40–46, 51 Art. 13 Rn. 1–65 Art. 14–19, 23 Anhang II, VI
Dr. Christian Piovano Syndikusrechtsanwalt, Friedrichshafen	Art. 31 Anhang VII
Manuel Poncza Rechtsanwalt, Köln	Art. 3 Nr. 17, 22, 30 Art. 20–22
Stephan Schmidt Rechtsanwalt, Fachanwalt für IT-Recht, Mainz	Art. 3 Nr. 4, 14, 36, 48 Art. 24–27
Dr. Kristina Schreiber Rechtsanwältin, Fachanwältin für Verwaltungsrecht, Köln	Art. 3 Nr. 33, 37, 38, 49, 50 Art. 52–58
Prof. Dr. Meinhard Schröder Universität Passau	Art. 1 (mit *Hartl*)
Dr. Paul Vogel, LL.M. Eur. Rechtsanwalt, München	Art. 3 Nr. 29 Art. 39–46
Dr. Gerhard Wiebe Rechtsanwalt, Berlin	Art. 3 Nr. 31 Art. 28–30

Verordnung (EU) 2024/2847 des Europäischen Parlaments und des Rates vom 23. Oktober 2024 über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen und zur Änderung der Verordnungen (EU) Nr. 168/2013 und (EU) 2019/1020 und der Richtlinie (EU) 2020/1828 (Cyberresilienz-Verordnung)

(Text von Bedeutung für den EWR)

(ABl. L, 2024/2847, 20.11.2024, ELI: http://data.europa.eu/eli/reg/2024/2847/oj);
ABl. L, 2025/90555, 2.7.2025; ABl. L, 2025/90828, 17.10.2025
(Celex-Nr. 32024R2847)
zuletzt geändert durch Art. 104 VO (EU) 2025/327 vom 11. Februar 2025
(ABl. L, 2025/327, 5.3.2025, ELI: http://data.europa.eu/eli/reg/2025/327/oj)

Kapitel I
Allgemeine Bestimmungen

Artikel 1 Gegenstand

Mit dieser Verordnung wird Folgendes festgelegt:

a) Vorschriften für die Bereitstellung auf dem Markt von Produkten mit digitalen Elementen, um die Cybersicherheit solcher Produkte zu gewährleisten;

b) grundlegende Cybersicherheitsanforderungen an die Konzeption, Entwicklung und Herstellung von Produkten mit digitalen Elementen sowie Pflichten der Wirtschaftsakteure in Bezug auf diese Produkte hinsichtlich der Cybersicherheit;

c) grundlegende Cybersicherheitsanforderungen an die von den Herstellern festgelegten Verfahren zur Behandlung von Schwachstellen, um die Cybersicherheit von Produkten mit digitalen Elementen während der erwarteten Nutzungsdauer der Produkte zu gewährleisten, sowie Pflichten der Wirtschaftsakteure in Bezug auf diese Verfahren;

d) Vorschriften für die Marktüberwachung, einschließlich Überwachung, und die Durchsetzung der in diesem Artikel genannten Vorschriften und Anforderungen.

Literatur: Biendl, Cybersicherheitsanforderungen nach dem Cyber Resilience Act der Europäischen Union, DB 2024, 1867; Biendl/Füllsack, Der finale Cyber Resilience Act im Überblick – Anwendungsbereich, Pflichten und Sanktionen, CR 2024, 376; Bressner/Gaden/Riediger, Der Cyber Resilience Act, DuD 2023, 327 ff.; Czychowski/Kroker, Handlungsempfehlungen für den Einsatz von Open Source Software zur Compliance mit dem CRA – Wie der Handlungsbedarf nach CRA optimal genutzt werden kann, CR 2025, 148; Dittrich/Heinelt, Compliance-Pflichten für Hersteller nach dem Cyber Resilience Act, RDi 2023, 309; Erdelt, Meldepflichten des Cyber Resilience Acts, ZfPC 2024, 176; Heckmann/Ziegler, Der Cyber Resilience Act: Ein Gesetz „mit digitalen Elementen", ITRB 2024, 159; Hessel/Callewaert, Der Cyber Resilience Act der EU-Kommission, K&R 2022, 789; Heynike/Taraz, Der Cyber Resilience Act, CCZ 2025, 92; Kreißl, Der Cyber Resilience Act: Neue Cybersicherheitsanforderungen für Produkte mit digitalen Elementen, ZfPC 2025, 223; Paschke/Fellenberg, Einblick in die Regelungsinhalte des Cyber Resilience Act, EuDIR 2025, 198; Piltz/Weiß/Zwerschke, Der Vorschlag für einen Cyber Resilience Act aus Sicht der DS-GVO, CR 2023, 154 und 289; Rennert, Mehr Cybersicherheit für vernetzte Produkte: Der Vorschlag der EU-Kommission für einen „Cyber Resilience Act". Eine Analyse vor dem Hintergrund jüngster Bedrohungen für die Cybersicherheit, ZfDR 2023, 206; Ruttloff/Wagner/Stilz, Der Entwurf des Cyber Resilience Act (CRA) und seine Auswirkungen auf das Gewährleistungs- und Produkthaftungsrecht, BB 2024, 1603; Scheibenflug/Monschke/Hildebrandt, Cloud-Dienste im Regelungsgeflecht von CRA und NIS2-Richtlinie – Warum Cloud-Dienste den Compliance-Anforderungen von CRA und NIS2-Richtlinie unterfallen, CR 2024, 712; Schöttle, Der Cyber Resilience Act: Hintergrund, Produktkategorien und Sicherheitsanforderungen. Einführung und Anwendungsbereiche der grundlegenden Pflichten, MMR 2024, 741; Schöttle, Der Cyber Resilience Act: Zeitliche Aspekte, Meldepflichten, Akteure und Sanktionen. Definition und die Aufgabe von Open Source Software-Stewards, MMR 2024, 834; Schweinoch/

Meßmer, Vorschlag der EU-Kommission für einen „Cyber Resilience Act", CR 2022, R112; Siglmüller, Cyber Resilience Act und Digital Operational Resilience Act – Lässt sich IT-Sicherheit rechtlich erzwingen?, ZfPC 2023, 221; Teichmann, Cyber Resilience Act – Produktsicherheit, SBOM und Herstellerhaftung entlang des Lebenszyklus, CCZ 2025, 165; Teichmann, Cybersicherheit als Produkteigenschaft – der Cyber Resilience Act der EU, NJW 2025, 2577; Teichmann, Der Cyber Resilience Act der EU, NVwZ 2025, 1662; Voigt/Falk, Der Cyber Resilience Act, MMR 2023, 88; Wiebe, Cybersicherheitsrecht 2.0 – Vorschlag eines Cyber Resilience Act, ZRP 2023, 73; Wiebe, Das neue Recht der Cyberresilienz, 2025; Wiebe/Daelen, Der Cyber Resilience Act aus produktsicherheitsrechtlicher Perspektive, EuZW 2023, 257; Wiebe/Daelen/Kerger, Der neue Cyber Resilience Act, K&R 2025, 79; Ziegler, Digitale Produktsicherheit: Der Vorschlag des Cyber Resilience Acts der EU-Kommission, jurisPR-ITR 2/2023; Zirnstein, Better cybersecurity due to increased regulation? The final European Cyber Resilience Act – The first comprehensive, horizontally applicable approach for more cybersecurity in digital products, CRi 2024, 65; Zirnstein, Der Entwurf des Cyber Resilience Act, CR 2022, 707.

Erwägungsgründe: 1–11

A. Allgemeines

I. Entstehungsgeschichte

1 Art. 1 hat im Vergleich zum **Entwurf der Kommission**[1] im Laufe des Gesetzgebungsverfahrens nur geringfügige Änderungen erfahren. In lit. c wurde die ursprünglich vorgeschlagene Formulierung „um die Cybersicherheit von Produkten mit digitalen Elementen während ihres gesamten Lebenszyklus zu gewährleisten" durch die schwächere Formulierung „um die Cybersicherheit von Produkten mit digitalen Elementen während der erwarteten Nutzungsdauer der Produkte zu gewährleisten" ersetzt (→ Rn. 23 ff.). Weiter wurde in lit. d nach dem Begriff der Marktüberwachung – sprachlich in der deutschen Fassung wenig verständlich (→ Rn. 27) – der Zusatz „einschließlich Überwachung" ergänzt und – rein redaktionell – die ursprüngliche Formulierung „der oben genannten Vorschriften und Anforderungen" durch die Formulierung „der in diesem Artikel genannten Vorschriften und Anforderungen" ersetzt.

2 In der **Cybersicherheitsstrategie** der Kommission 2020 war erstmals in Erwägung gezogen worden, „neue horizontale Vorschriften zur Verbesserung der Cybersicherheit aller vernetzten Produkte und zugehörigen Dienste im Binnenmarkt" zu erlassen.[2] Bis dahin hatte die Union zwar Cybersicherheit zunehmend als horizontales Thema verstanden, verbindliche Cybersicherheitsvorgaben aber vor allem für bestimmte Sektoren erlassen (insbesondere die NIS-Richtlinien). Mit dem CRA werden nun – gestützt auf die Binnenmarktkompetenz des Art. 114 AEUV – nahezu alle „Produkte mit digitalen Elementen" (→ Art. 3 Rn. 2 ff.), die nicht besonderen Anforderungen in anderen Rechtsakten unterliegen oder außerhalb der Kompetenzen des Unionsgesetzgebers liegen, mit Cybersicherheitsanforderungen belegt.

II. Sinn und Zweck

3 Art. 1 beschreibt den Gegenstand des CRA in vier Blöcken (zu den Details → Rn. 12 ff.). Die Bestimmung mag punktuell zur teleologischen Auslegung anderer Vorschriften herangezogen

1 COM(2022) 454 final.
2 „Die Cybersicherheitsstrategie der EU für die digitale Dekade", JOIN(2020) 18 final.

werden können; ihre eigentliche Bedeutung liegt darin, dem Rechtsanwender einen (sehr groben) **Überblick über die Inhalte** des CRA zu geben. Soweit also ein bestimmtes Thema in den Art. 2 ff. CRA geregelt ist und nach den üblichen Regeln der Normauslegung ein bestimmtes Ergebnis tragfähig ist, dürfte Art. 1 CRA dem im Einzelfall nicht entgegenstehen. Es wäre unlogisch anzunehmen, der Gesetzgeber hätte mit einer notwendig schlank formulierten Übersicht die Anwendung der eigentlich inhaltlichen Regelungen begrenzen wollen. Der argumentative Wert von Art. 1 CRA ist demnach stark eingeschränkt. Ein ähnliches Vorgehen hat der Gesetzgeber auch in anderen Digitalrechtsakten gewählt, zB in Art. 1 DA, der ebenfalls weitgehend eine Inhaltsübersicht enthält.[3]

Warum der CRA diese Inhalte aufweist, beschreibt der Unionsgesetzgeber in den ersten Erwägungsgründen: „Cybersicherheit bedeutet eine der größten Herausforderungen für die Union. Die Zahl und Vielfalt der vernetzten Geräte wird in den kommenden Jahren exponentiell zunehmen. Cyberangriffe sind ein Thema von öffentlichem Interesse, da sie sich nicht nur auf die Wirtschaft der Union, sondern auch auf die Demokratie sowie die Sicherheit und Gesundheit der Verbraucher kritisch auswirken."[4] Dieser Herausforderung stellt sich die Union durch **horizontale Cybersicherheitsvorgaben für Produkte mit digitalen Elementen** für den gesamten Binnenmarkt.[5] Sie möchte damit zwei Probleme angehen, „die hohe Kosten für die Nutzer und die Gesellschaft verursachen: ein geringes Maß an Cybersicherheit von Produkten mit digitalen Elementen, das sich in weitverbreiteten Schwachstellen und der unzureichenden und inkohärenten Bereitstellung von Sicherheitsaktualisierungen zu deren Behebung zeigt, sowie ein unzureichendes Verständnis und ein mangelnder Informationszugang der Nutzer, wodurch sie daran gehindert werden, Produkte mit angemessenen Cybersicherheitsmerkmalen auszuwählen oder sicher zu verwenden."[6] 4

Keine Erwähnung findet in Art. 1 der dem Rechtsakt seine (Kurz-)Bezeichnung gebende Begriff der **Cyberresilienz**. Auch sonst wird er, sieht man von Art. 33 Abs. 2 ab, wo „Reallabore für Cyberresilienz" geregelt werden, im operativen Teil des CRA nicht verwendet. Lediglich in den Erwägungsgründen ist gelegentlich von (Cyber-)Resilienz die Rede. Der Begriff der Resilienz stammt ursprünglich aus der Werkstoffkunde, fand dann Eingang in die Psychologie und schließlich ins Recht.[7] Versucht man ausgehend von dem originären Begriffsverständnis einen Unterschied zwischen IT- bzw. Cybersicherheit und Cyberresilienz zu definieren, fällt ins Auge, dass es bei der Resilienz im Unterschied zur Sicherheit nicht um die Abwehr von Gefahren geht, also darum, dass das Schutzgut unversehrt bleibt, sondern um dessen Fähigkeit, trotz etwaiger Störungen wieder in den Ursprungszustand zurückzukehren, zumindest aber seine Funktionsfähigkeit zu behalten. Diese besondere Akzentsetzung kommt im CRA allenfalls punktuell zum Ausdruck: Im Rahmen von „security by design" müssen mögliche Sicherheitsvorfälle mitbedacht werden, Pflichten zur Aufrechterhaltung der Cybersicherheit sollen über den gesamten Lebenszyklus eines Produkts dessen Brauchbarkeit sicherstellen, und eine Vielzahl von Akteuren wird, teilweise subsidiär, adressiert. Das ist allerdings auch im Bereich der klassischen IT-Sicherheit nichts völlig Neues (wenngleich es nun erstmals gesetzlich angeordnet wird). Anders als im Digital Operations Resilience Act (DORA),[8] wo die „operationale Resilienz", also die Aufrechterhaltung der Funktion im Vordergrund steht, wird der Begriff der Resilienz im CRA also weitgehend von seinen Wurzeln gelöst. Die Verwendung eines neuen Begriffs soll wohl vor allem zum Ausdruck bringen, dass mit den weitreichenden Vorgaben des CRA ein **neues Level an IT-Sicherheit** in der Union erreicht werden soll. 5

3 Vgl. BeckOK DatenschutzR/Veil, Stand 1.2.2025, DA Art. 1 Rn. 1.
4 Erwägungsgrund 1.
5 Erwägungsgründe 1, 2, 8.
6 Erwägungsgrund 1.
7 Vgl. zum Begriff etwa Alexander Nat. Hazards Earth Syst. Sci., 13 (2013), 2707 ff.; siehe auch die Beiträge in Karidi/Schneider/Gutwald (Hrsg.), Resilienz, 2018.
8 Verordnung (EU) 2022/2554 vom 14.12.2022, ABl. L 333, 1.

III. Systematische Einordnung

6 Beim CRA handelt es sich im Kern um **Produktrecht**, hier bezogen auf Produkte mit digitalen Elementen. Für diesen Bereich gilt seit 2008 der sogenannte „Neue Rechtsrahmen" (New Legislative Framework, NLF), ein Maßnahmenpaket, das aus verschiedenen Rechtsakten besteht. Zu nennen sind insofern zunächst die Verordnung (EG) Nr. 765/2008 mit Vorschriften über die Akkreditierung sowie der Beschluss Nr. 768/2008, der ua ein Muster für künftige Rechtsvorschriften zur Produktharmonisierung enthält. Zahlreiche Vorschriften des CRA orientieren sich an diesem Muster. Die ursprünglich auch in der Verordnung (EG) Nr. 765/2008 geregelte Marktüberwachung wurde zwischenzeitlich in der Verordnung (EU) 2019/1020 (Marktüberwachungsverordnung, MÜ-VO) separat geregelt; diese Verordnung gilt auch im Anwendungsbereich des CRA, wird allerdings durch diesen nach dem lex specialis-Grundsatz ergänzt und punktuell modifiziert. Zu den Details → Art. 52 Rn. 16 ff.

7 Der horizontale Ansatz des CRA wird in Art. 2 mithilfe von **Bereichsausnahmen** durchbrochen. Diese Bereichsausnahmen bestehen (bzw. können durch die Kommission im Wege der delegierten Rechtssetzung geschaffen werden, Art. 2 Abs. 5) einerseits, wo in spezielleren Vorschriften des Unionsrechts bereits Cybersicherheitsanforderungen vorgesehen sind (→ Art. 2 Rn. 29 ff.). Damit werden insbesondere im Medizin- und Verkehrsbereich Doppelanforderungen vermieden. Andererseits beachtet der Unionsgesetzgeber in Art. 2 Abs. 7 seine Kompetenzgrenzen: Der CRA gilt nicht für Produkte mit digitalen Elementen, die ausschließlich für Zwecke der nationalen Sicherheit oder für Verteidigungszwecke entwickelt oder geändert wurden, und auch nicht für Produkte, die speziell für die Verarbeitung von Verschlusssachen konzipiert sind. Diese Bereiche erweisen sich auch im Fall von Querschnittsthemen wie der IT-Sicherheit als weitgehend immun gegen einen europarechtlichen Zugriff.

8 Das Verhältnis des CRA zum allgemeinen Produktsicherheitsrecht wird in Art. 11 geregelt, der differenziert die Anwendbarkeit der **Allgemeinen Produktsicherheitsverordnung** (General Product Safety Regulation, GPSR[9]) regelt. Für Cybersecurity-Risiken gilt demnach vorrangig der CRA, für Nicht-Cybersecurity-Risiken gelten die (allgemeinen oder besonderen) Produktsicherheitsvorschriften neben dem CRA (vgl. Erwägungsgrund 50).

9 Das Verhältnis zur **KI-Verordnung**[10] wird in Art. 12 und Erwägungsgrund 51 beschrieben. Im Grundsatz stehen die Anforderungen beider Rechtsakte nebeneinander. Hinzuweisen ist aber darauf, dass eine Konformitätsbewertung nach dem CRA auch für die Beurteilung der Konformität gem. Art. 15 KI-VO nutzbar gemacht werden kann, sodass eine „Doppelbewertung" vermieden wird.

10 Das Verhältnis zur **NIS-2-Richtlinie**[11] wird in Erwägungsgrund 52 beschrieben. Grundsätzlich stehen die Vorgaben nebeneinander, was angesichts der unterschiedlichen Anknüpfungspunkte (einerseits Hersteller von Produkten und nachgelagerte Wirtschaftsakteure, andererseits Betreiber von kritischen Infrastrukturen) auch konsequent ist. Nicht übersehen werden darf aber, dass der CRA zahlreiche Bezugnahmen, auch in institutioneller Hinsicht (CSIRT usw), auf die NIS-2-Richtlinie und die durch diese sowie durch den **Cybersecurity Act**[12] geschaffenen (Behörden-)Strukturen enthält.

11 Das Verhältnis zur **Maschinenverordnung**[13] wird ausschließlich in Erwägungsgrund 53 beschrieben. Auch hier gilt im Grundsatz (und angesichts der Nicht-Regelung im operativen Teil beider Rechtsakte naheliegend), dass die Anforderungen nebeneinanderstehen. Anders als im Fall der

9 Verordnung (EU) 2023/988 des Europäischen Parlaments und des Rates vom 10.5.2023, ABl. L 135, 1.
10 Verordnung (EU) 2024/1689 des Europäischen Parlaments und des Rates vom 13.6.2024, ABl. L, 2024/1689 vom 12.7.2024.
11 Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14.12.2022, ABl. L 333, 80.
12 Verordnung (EU) 2019/881 des Europäischen Parlaments und des Rates vom 17.4.2019, ABl. L 151, 15.
13 Verordnung (EU) 2023/1230 des Europäischen Parlaments und des Rates vom 14.6.2023, ABl. L 165, 1.

KI-Verordnung ist die „Doppelverwendung" einer Konformitätsbewertung nicht ausdrücklich vorgesehen; der Gesetzgeber weist aber darauf hin, dass insbesondere über die Anwendung harmonisierter Normen Synergieeffekte erzielt werden können.

B. Kommentierung

I. Regelungen zur Bereitstellung von Produkten mit digitalen Elementen auf dem Markt (lit. a)

Der CRA knüpft an die Bereitstellung von Produkten auf dem Markt an (Art. 2 Abs. 1 CRA, dazu → Art. 2 Rn. 4, 7 und Art. 3 Nr. 22). Wesentliche Überlegung des Gesetzgebers war wohl, so durch den klaren Anknüpfungspunkt „Marktangebot" die Geltung der materiellen Anforderungen sicherzustellen.[14] 12

Alternativ hätten etwa auch – im Rahmen einer völlig anderen Gesetzeskonzeption – reine Anforderungen an die Verwender von Produkten mit digitalen Elementen gestellt werden können. Einen solchen im Vollzug dysfunktionalen Weg geht etwa die DS-GVO, die in Art. 32 DS-GVO zwar risikobasiert Anforderungen an die **Sicherheit der Verarbeitung personenbezogener Daten** stellt, dabei aber nicht den Hersteller von Produkten in den Blick nimmt, auch wenn diese eindeutig auf die Verarbeitung personenbezogener Daten ausgelegt sind, sondern den Anwender. 13

Regelungen zur Bereitstellung von **Produkten mit digitalen Elementen** auf dem Markt befinden sich zentral in Kapitel II. Zum Anwendungsbereich des CRA hinsichtlich der auf dem Markt bereitgestellten Produkte mit digitalen Elementen → Art. 2 Rn. 7 ff., zur Bereitstellung auf dem Markt bzw. Inverkehrbringen (als erstmaliger Bereitstellung auf dem Markt) Art. 3 Nr. 21 und 22. 14

Der CRA ist – und dies ist dem Gesetzgeber wichtig – gerade kein zB auf Industrieanlagen bezogenes Recht mit Fokus auf Maschinen und Lieferkettensicherheit. Gerade Verbraucherprodukte (zB Spielzeug, Babyphones, Wearables) sollen sicher sein (Erwägungsgrund 10). Der **Verbraucherschutz** findet sich auch in der Einstufung als „wichtige Produkte mit digitalen Elementen" wieder (dazu → Art. 2 Rn. 11). 15

II. Cybersicherheitsanforderungen bei Konzeption, Entwicklung und Herstellung (lit. b)

Cyberbedrohungen sind dynamisch, Cybersicherheit muss daher, um effektiv zu sein, „*by design*" gedacht werden. Eine nachträgliche „Härtung" oder der Einsatz ergänzender Sicherheitsprodukte ist nicht immer tauglich. Der Gesetzgeber möchte – insbesondere vor dem Hintergrund umfassend vernetzter Systeme – Cybersicherheit daher von Grund auf berücksichtigt wissen (Erwägungsgrund 10). 16

Zentrale Norm ist Art. 13 Abs. 1 (→ Art. 13 Rn. 5), demnach müssen Hersteller gewährleisten, dass ein Produkt mit digitalen Elementen gemäß den grundlegenden **Cybersicherheitsanforderungen** in Anhang I Teil I konzipiert, entwickelt und hergestellt worden ist. 17

In der Sache geht es um ein durchgehend hohes Sicherheitsniveau durch sichere Konzeption, fortlaufende Risikobewertung (Art. 13 Abs. 3), Dokumentation und Reaktion auf (erkannte) Schwachstellen. Ein zentraler Faktor bei der Auswahl vernetzter Produkte wird perspektivisch wohl dem sog. **Unterstützungszeitraum** zukommen (→ Art. 13 Rn. 23). 18

Einen ähnlichen herstellerbezogenen „by design"-Ansatz sieht das **Datenrecht** in Art. 3 Datenverordnung (Data Act) vor. Demnach müssen vernetzte Produkte im Sinne der Datenverordnung (Art. 2 Nr. 5 Data Act) so konzipiert und hergestellt sein, dass die relevanten Daten für den Nutzer 19

14 Vgl. Erwägungsgrund 10.

zugänglich sind. Cybersicherheitsanforderungen ergeben sich auch insoweit aus der Natur der Sache, da der Prozess schon im Eigeninteresse des Herstellers sicher ausgestaltet sein sollte.

20 Die KI-VO enthält in Art. 15 Abs. 1 eine ähnliche Vorgabe speziell zu **Hochrisiko-KI-Systemen**. Diese „müssen so konzipiert und entwickelt [sein], dass sie ein angemessenes Maß an Genauigkeit, Robustheit und Cybersicherheit erreichen und in dieser Hinsicht während ihres gesamten Lebenszyklus beständig funktionieren".

21 In der DS-GVO sieht Art. 25 Abs. 1 DS-GVO **Datenschutz durch Technikgestaltung** und damit konzeptionell auch Datensicherheit qua Produktkonzeption vor. Allerdings werden Hersteller in Art. 25 Abs. 1 DS-GVO nicht selbst verpflichtet. Eine rechtlich relevante „Vorfeldwirkung" auf die Hersteller müsste bislang – über bloße Appelle wie Erwägungsgrund 78 der DS-GVO hinaus – etwa durch zivilrechtliche Mangelbegriffe erzielt werden.[15]

22 Der Anhang I des CRA sieht in Absatz 2 lit. d–f Anforderungen an den **technischen Datenschutz** vor und steht so in Wechselwirkung mit Art. 32 DS-GVO. Der Grundsatz der Datenminimierung findet sich ausdrücklich in Anhang I Teil I Abs. 2 lit. g CRA.

III. Schwachstellenbehebung während der erwarteten Nutzungsdauer (lit. c)

23 Laufende **Sicherheitsupdates** sind für vernetzte Systeme unabdingbar. Gerade im deutschen Kauf- und Werkrecht mit dem Gefahrübergang als zentralem Übergabepunkt der geschuldeten Leistung waren nachlaufende Updatepflichten aber ein Fremdkörper. Die Rechtslage hierzu ist – rein mit Blick auf das BGB – umstritten. Jedenfalls gegenüber Verbrauchern bestehen mit § 327f Abs. 1 S. 2 BGB für digitale Produkte inzwischen Aktualisierungspflichten.

24 Der CRA adressiert eine Pflicht zur **Schwachstellenbehebung** speziell in Art. 13, insbesondere Abs. 8, in Verbindung mit Anhang I (Teil 2) (weiterführend → Art. 13 Rn. 21 ff.). In der Sache geht es um sichere, wirksame und zeitnahe Behebung von Schwachstellen nach einem definierten Prozess.

25 Art. 14 CRA sieht umfassende (behördliche) **Meldepflichten** (→ Art. 14 Rn. 1 ff.) und Informationen an betroffene Nutzer (→ Art. 14 Rn. 18), vor. Ausgangspunkt sind sog. „aktiv ausgenutzte Schwachstellen" (→ Art. 14 Rn. 3 und Art. 3 Nr. 42) oder „schwerwiegende Sicherheitsvorfälle" (→ Art. 14 Rn. 7 ff.).

26 Melde- und Informationspflichten können parallel nach der DS-GVO bei einer **Verletzung des Schutzes personenbezogener Daten** bestehen (Art. 4 Nr. 12 und Art. 35, 36 DS-GVO). Gerade bei einer Verletzung des Schutzes personenbezogener Daten und folgenden datenschutzrechtlichen Rechtsstreitigkeiten dürften Pflichten unter dem CRA zur technischen Sicherheit relevant werden. Der EuGH sieht die **Beweislast** für technische Sicherheit der Verarbeitung personenbezogener Daten beim Verantwortlichen im Sinne der DS-GVO.[16]

IV. Marktüberwachung und Durchsetzung (lit. d)

27 Der CRA enthält weiterhin Regelungen zur „**Marktüberwachung, einschließlich Überwachung**". Die Formulierung der deutschen Fassung ist so kaum verständlich; in der englischen Fassung ist – etwas klarer – die Rede von „rules on market surveillance, including monitoring". Da gleichwohl surveillance eine intensivere und finalere Form des monitoring ist, erscheint der Zusatz wenig hilfreich.

28 Der CRA enthält schließlich Vorschriften zur Durchsetzung, insbesondere zum Bußgeldrahmen (→ Art. 64 Rn. 31). Hier stand augenscheinlich, wie bei vielen neueren (Digital-)Rechtsakten,

15 Zu alledem auch weiterführend Kühling/Buchner/Hartung DS-GVO Art. 25 Rn. 13.
16 EuGH (Dritte Kammer) Urt. v. 25.1.2024 – C-687/21, NZA 2024, 320 (322).

die DS-GVO Pate. Ob die Zurückhaltung deutscher Aufsichtsbehörden bei Bußgeldern auch im Kontext des CRA fortgesetzt wird, bleibt abzuwarten.

Art. 65 CRA sieht die Möglichkeit von **Verbandsklagen** vor (→ Art. 65 Rn. 11). 29

C. Bewertung und Ausblick

Die frühere Strategie, Cybersicherheit (außer in kritischen Bereichen) als Teil der Produktqualität zu verstehen, die „der Markt" regelt, wird mit dem CRA zu Recht verabschiedet. Cybersicherheitslücken wirken über vertragliche Beziehungen hinaus, wenn etwa vernetzte Geräte zum Teil von Botnetzen werden. Cybersicherheit ist insofern eine **Frage des öffentlichen Interesses**, dessen sich der Gesetzgeber annehmen muss. 30

Ein weiterer positiver Effekt der Regulierung ist, dass die Frage, welche Cybersicherheitsstandards adäquat sind, nun nicht mehr fallweise von Gerichten beantwortet werden, sondern – zumindest im Ansatz – durch den Gesetzgeber. Das verbessert die **demokratische Legitimation** des Cybersicherheitsrechts. 31

Mit dem CRA ist das (Gesetzgebungs-)Programm der **Cybersicherheitsstrategie 2020** weitgehend abgeschlossen. Die wesentliche Aufgabe für die Kommission wird in der nächsten Zeit darin liegen, die im CRA enthaltenen Aufträge zur delegierten und Durchführungs-Rechtsetzung zu erfüllen und die Wirksamkeit des CRA zu evaluieren. 32

Artikel 2 Anwendungsbereich

(1) Diese Verordnung gilt für auf dem Markt bereitgestellte Produkte mit digitalen Elementen, deren bestimmungsgemäßer Zweck oder vernünftigerweise vorhersehbare Verwendung eine direkte oder indirekte logische oder physische Datenverbindung mit einem Gerät oder Netz einschließt.

(2) Diese Verordnung gilt nicht für Produkte mit digitalen Elementen, auf die folgende Rechtsakte der Union Anwendung finden:

a) Verordnung (EU) 2017/745,
b) Verordnung (EU) 2017/746,
c) Verordnung (EU) 2019/2144.

(3) Diese Verordnung gilt nicht für Produkte mit digitalen Elementen, die nach der Verordnung (EU) 2018/1139 zertifiziert worden sind.

(4) Diese Verordnung gilt nicht für Geräte, die in den Anwendungsbereich der Richtlinie 2014/90/EU des Europäischen Parlaments und des Rates[1] fallen.

(5) ***(1)*** **Die Anwendung dieser Verordnung auf Produkte mit digitalen Elementen, die unter andere Rechtsvorschriften der Union mit Anforderungen für alle oder einige der von den grundlegenden Cybersicherheitsanforderungen in Anhang I abgedeckten Risiken fallen, kann eingeschränkt oder ausgeschlossen werden, wenn**

a) eine solche Einschränkung oder ein solcher Ausschluss mit dem für diese Produkte geltenden allgemeinen Rechtsrahmen vereinbar ist und
b) mit den sektorspezifischen Vorschriften dasselbe Schutzniveau erreicht wird, wie es diese Verordnung gewährleistet, oder ein höheres.

1 **Amtl. Anm.:** Richtlinie 2014/90/EU des Europäischen Parlaments und des Rates vom 23. Juli 2014 über Schiffsausrüstung und zur Aufhebung der Richtlinie 96/98/EG des Rates (ABl. L 257 vom 28.8.2014, S. 146).

(2) Der Kommission wird die Befugnis übertragen, gemäß Artikel 61 zur Ergänzung dieser Verordnung delegierte Rechtsakte zu erlassen, in denen sie die Notwendigkeit einer solchen Einschränkung oder eines solchen Ausschlusses feststellt und gegebenenfalls die betreffenden Produkte und Vorschriften sowie den Umfang der Einschränkung festlegt.

(6) Diese Verordnung gilt nicht für Ersatzteile, die auf dem Markt bereitgestellt werden, um identische Komponenten in Produkten mit digitalen Elementen zu ersetzen, und die nach denselben Spezifikationen hergestellt werden wie die Bauteile, die sie ersetzen sollen.

(7) Diese Verordnung gilt nicht für Produkte mit digitalen Elementen, die ausschließlich für Zwecke der nationalen Sicherheit oder für Verteidigungszwecke entwickelt oder geändert wurden, und auch nicht für Produkte, die speziell für die Verarbeitung von Verschlusssachen konzipiert sind.

(8) Die in dieser Verordnung festgelegten Verpflichtungen umfassen nicht die Bereitstellung von Informationen, deren Offenlegung wesentlichen Interessen der Mitgliedstaaten im Bereich der nationalen Sicherheit, der öffentlichen Sicherheit oder der Verteidigung zuwiderlaufen würde.

Literatur: Arzt/Fischer/Kreutzer/Scheel/Schneider/Schreiber/Selzer, Der EU Cyber Resilience Act: Ein Überblick aus rechtlicher Sicht, Version 1.0, 2024; Becker, Stellungnahme für den BT-Innenausschuss, 22.10.2012, Ausschussdrucksache 17(4)585 B;; BSI, Lage der IT-Sicherheit in Deutschland 2024, 2024; KOM, Commission Staff Working Document, Impact Assessment Report [zum Vorschlag für die CRA], SWD(2022) 282 final, Brüssel 2022 (zitiert: Impact Assessment); Medical Device Coordination Group, MDCG 2019-16 Rev. 1, Guidance on Cybersecurity for medical devices, Juli 2020; Schantz/Wolff, Neues DatenschutzR, 2017; Schöttle, Der Cyber Resilience Act: Hintergrund, Produktkategorien und Sicherheitsanforderungen Einführung und Anwendungsbereiche der grundlegenden Pflichten, MMR 2024, 741.

Erwägungsgründe: 9, 11, 12, 15, 16, 17, 20,18, 24, 25, 26, 27, 28, 29, 30, 33, 53

A. Allgemeines

I. Entstehungsgeschichte

1 Der Kern der Regelung zum Anwendungsbereich war bereits im Entwurf der KOM enthalten. Insbesondere das Prinzip der **horizontalen Produktregulierung** blieb im Gesetzgebungsverfahren gleich. Der grundsätzliche Mechanismus (verbindungsfähige PdE) wurde um das Merkmal der Bereitstellung am Markt ergänzt. Diese Klarstellung ist sinnvoll, um die Produkte, die regulär unter den CRA fallen (zB FOSS-Geschäftsmodelle), von jenen zu unterscheiden, für die nur die Pflichten der Verwalter quelloffener Software gelten (Art. 24 CRA, FOSS-Projekte, → Rn. 20).

Im Übrigen wurden im Gesetzgebungsverfahren nur Ausnahmen ergänzt: 2

- Für Schiffsausrüstung (Abs. 4)
- Für Ersatzteile (Abs. 6)
- Für Sicherheitsinteressen (Abs. 8)

II. Sinn und Zweck

Die Norm regelt den Anwendungsbereich des CRA; nur in Bezug auf Produkte, die innerhalb dieses Bereichs liegen, entfalten die Pflichten der CRA ihre Wirkung. 3

Als horizontale Produktregulierung geht der Gesetzgeber dabei in zwei Schritten vor: Erst öffnet er den Anwendungsbereich maximal, also auf sämtliche PdE zur Verbindung mit einem Netz oder Gerät (→ Rn. 7 ff.). Im zweiten Schritt schränkt er die Anwendbarkeit dann sektorenweise und in Bezug auf einzelne Komponenten wieder ein (→ Rn. 29 ff.). Durch diesen **Opt-out-Ansatz** werden die wichtigsten Abgrenzungsfragen geklärt, ohne dass gleichzeitig Lücken im System der produktbezogenen Cybersicherheitsregulierung entstünden. 4

Wo keine Ausnahmen greifen, ist der CRA parallel zu der fraglichen Norm anzuwenden, selbst wenn sich dabei thematische Überschneidungen ergeben. Einige dieser Fälle hat der Gesetzgeber in den Erwägungsgründen klargestellt (→ Rn. 73 ff.). 5

III. Systematische Einordnung

Der Anwendungsbereich gehört zu den allgemeinen Bestimmungen und ist darum für sämtliche Kapitel der CRA von Bedeutung. Für Aspekte, die außerhalb des Anwendungsbereichs in Art. 2 CRA liegen, sind die Vorgaben des CRA schon grundsätzlich nicht von Belang. 6

B. Kommentierung

I. Originärer Anwendungsbereich (Abs. 1)

1. Relevante Begriffe. Art. 2 Abs. 1 CRA spannt den originären Anwendungsbereich der Norm auf, von dem im weiteren Verlauf Ausnahmen gemacht werden. Die wesentlichen Begriffe für den Anwendungsbereich sind nahezu sämtlich in den Begriffsbestimmungen enthalten. In der Reihenfolge des Art. 2 Abs. 1 CRA: 7

- Bereitstellen auf dem Markt, Art. 3 Nr. 22
- Produkte mit digitalen Elementen, Art. 3 Nr. 1
- Zweckbestimmung, Art. 3 Nr. 23
- Vernünftigerweise vorhersehbare Verwendung, Art. 3 Nr. 24
- Indirekte Verbindung, Art. 3 Nr. 10
- Logische Verbindung, Art. 3 Nr. 8
- Physische Verbindung, Art. 3 Nr. 9

Für eine detaillierte Beschreibung der jeweils erfassten Produkte und Tätigkeiten sei auf die Kommentierungen zu den einschlägigen Definitionen verwiesen. Folgende Grenzfälle und Klarstellungen sind besonders relevant: 8

- PdE meint schlicht **Hardware und/oder Software** von und für Computer – in allen Formen und Größen und unabhängig davon, ob sie für Unternehmer oder Verbraucher (Smart Home, Wearables) vorgesehen sind (PdE, Art. 3 Nr. 1).
- **Cloud-Dienste** sind nur insofern erfasst, als sie notwendig sind, eine Funktion des PdE zu unterstützen (Datenfernverarbeitung, Art. 3 Nr. 2).
- Das Lizenzmodell von Software spielt nur eine untergeordnete Rolle. **Freie und quelloffene Software** (→ Rn. 18) ist grundsätzlich ebenso erfasst wie proprietäre Software. Ob das Produkt entgeltlich oder unentgeltlich abgegeben wird, spielt keine Rolle. Ausnahmen gibt es nur, falls

die Abgabe nicht im Rahmen einer Geschäftstätigkeit erfolgt, wie dies bei der öffentlichen Verwaltung oder Non-Profit-Organisationen der Fall sein kann (Art. 3 Nr. 22).

9 Für die Kommentierung Art. 2 Abs. 1 CRA bleiben damit nur die Begriffe der direkten Verbindung sowie des Geräts oder Netzes.

10 **2. Direkte Verbindung mit einem Netz oder Gerät.** Der Begriff der direkten Verbindung erschließt sich ohne Weiteres aus der Definition der indirekten Verbindung. Dort geht es darum, dass ein PdE auch als Teil eines größeren Systems, das seinerseits mit einem Gerät oder Netz verbunden ist, in den Anwendungsbereich der CRA fällt. Direkt bedeutet also nur, dass dieser Zwischenschritt wegfällt. Es ist im Grunde eine Nicht-Voraussetzung und soll nur verdeutlichen, dass alle denkbaren Verbindungsarten für Art. 2 Abs. 1 CRA zählen.

11 **3. Verbindung mit einem Netz oder Gerät.** Der Begriff des Netzes oder Geräts wird im CRA nur über Umwege erläutert. Hauptanwendungsfall für ein Netz ist sicher das Internet. In den Erwägungsgründen zeigt sich das in ErwG 24, der „ein sicheres Internet" als ein Ziel der NIS-2-RL angibt, wobei die CRA den verantwortlichen Betreibern helfe, wenn diese auf sichere Weise entwickelte PdE einsetzen könnten. Ansonsten spielt das Internet nur für die Einordnung von Produkten als wichtige PdE eine Rolle, weil sich Anhang III Klasse I Nr. 12 auf „Modems für die Internetverbindung" bezieht und Nr. 18 auf „mit dem Internet verbundenes Spielzeug".

12 Einen weiteren Hinweis auf die **Netze** liefert die Verweiskette aus der Definition der Cybersicherheit (Art. 3 Nr. 3). Sie verweist auf „Netz- und Informationssysteme" (Art. 2 Nr. 2 CSA), die wiederum in Art. 6 Nr. 1 NIS-2-RL ua definiert werden als ein „elektronisches Kommunikationsnetz" im Sinne von Art. 2 Nr. 1 RL (EU) 2018/1972. Es liegt darum nahe, den Begriff des Netzes wie in der EECC-Richtlinie (EU) 2018/1972 zu verstehen (Art. 3 Nr. 3, → Art. 3 Rn. 28 f.). Er umfasst sämtliche Übertragungssysteme, die der Signalübertragung dienen, unabhängig von der Art der übertragenen Information: Leitungsnetze, mobile Netze, Netze für Hör- und Fernsehfunk sowie Kabelfernnetze – selbst Stromnetze, soweit sie zur Signalübertragung genutzt werden.

13 Legt man das zugrunde, ist der **Netzbegriff der CRA** maximal weit zu verstehen. Er umfasst vor allem auch Netze, die – ua aus Sicherheitsgründen – ggf. nicht mit dem Internet verbunden sind. Dazu zählen zB Netze für industrielle Steuerungssysteme, Kraftwerke[2] oder die Leit- und Sicherungstechnik der Bahn.[3] Selbst Rundfunknetze gehören dazu – wenn das betreffende PdE über eine Möglichkeit verfügt, zu senden.

14 Für eine **Einschränkung in Bezug auf rein empfangende Geräte bei Rundfunknetzen** spricht auch der Zweck des weiten Anwendungsbereichs, wie ihn ErwG 9 erläutert. Danach soll auch „als weniger kritisch geltende Hardware und Software" erfasst sein, weil sie sonst „eine Kompromittierung eines Geräts oder Netzes erleichtern". Zwar wurde der Vorschlag, den Anwendungsbereich der CRA auf bidirektionale Verbindungen zu beschränken,[4] nicht aufgegriffen. Für die in ErwG 9 genannte Kompromittierung braucht es aber zumindest eine sendende Verbindung ins Netz, über die Geräte, die als bloße Empfänger fungieren, nicht verfügen.

15 Dieser Gedanke lässt sich am Beispiel der Funkrundsteuerung von **Straßenlaternen** oder Photovoltaikanlagen verdeutlichen, zu der auf dem 38C3-Kongress[5] – durchaus umstrittene[6] – Sicherheitslücken diskutiert wurden. Das System basiert auf Langwellen; in Deutschland steuern zwei

2 Arzt et al., Der EU Cyber Resilience Act: Ein Überblick aus rechtlicher Sicht, Version 1.0, März 2024, S. 8 f.
3 Davon gehen zB auch die Verbände der Bahnindustrie (UNIFE) und der Bahnbetreiber (CER) aus.
4 ZVEI, Position on the proposal for a Cyber Resilience Act, 2023, https://www.zvei.org/fileadmin/user_upload/Presse_und_Medien/Publikationen/2023/Februar/Cyber_Resilience_ACt/2023-02-09_ZVEI_Position_Paper_Cyber_Resilience_Act_CRA.pdf, S. 4.
5 Vortrag von Bräunlein und Melette auf dem 38C2 vom 28.12.2024, BlinkenCity: Radio-Controlling Street Lamps and Power Plants, https://media.ccc.de/v./38c3-blinkencity-radio-controlling-street-lamps-and-power-plants.
6 Spiegel vom 28.12.2024, Könnten Hacker Blackouts über Funk auslösen?; Golem.de vom 29.12.2024, https://www.golem.de/news/rundsteuerempfaenger-gehackt-laesst-sich-ueber-funksignale-ein-blackout-herbeifuehren-2412-192013.html.

Stichwortverzeichnis

Die **fetten** Zahlen verweisen auf den Paragrafen, die mageren auf die Randnummer.