THERESA RATH / FELIX EKARDT / ALEXANDER SCHIELA

# Cybersicherheit in der Energiewende und das EU-Recht

## Aktuelle Entwicklungen und kritische Reflexion

Kritische Infrastruktur

Die Energie- und Klimawende geht mit einer zunehmenden Digitalisierung insbesondere des Stromnetzes einher. Dies birgt die Gefahr von Cyberattacken, die schlimmstenfalls die Versorgungssicherheit gefährden können. Dieser Beitrag beleuchtet mögliche Arten und Folgen von Cyberattacken auf dem Energiemarkt sowie den europäischen Rechtsrahmen de lege lata, wobei auch die im Zuge des Ukraine-Kriegs relevanten Rechtsänderungen näher analysiert werden. Dabei werden auch verbleibende Regelungsbedarfe betrachtet, ebenso wie der Umstand, dass letztlich Energieeinsparung und Dezentralisierung immer wichtiger – auch – zur Herstellung von Cybersicherheit werden. Lesedauer: ●● Minuten

## I. Problemstellung

Seit einiger Zeit verändert die Digitalisierung das Zusammenleben und das Wirtschaften zunehmend grundlegend und evoziert dabei große Chancen wie auch große Risiken sowohl für Märkte als auch für den demokratischen Diskurs in ihrem weiten Spannungsbogen zwischen möglichen Machtkonzentrationen und möglicher verstärkter Partizipation an politischen und ökonomischen Entscheidungsprozessen. Ebenso global bedeutsam ist die Herausforderung, wie nachhaltige, also dauerhaft und global durchhaltbare Lebens- und Wirtschaftsweisen etabliert werden können. Klimawandel, Biodiversitätsverluste, gestörte Nährstoffkreisläufe, Wasserknappheit und Belastungen der Umweltmedien sind dabei einige der elementaren, meist unter dem Rubrum Nachhaltigkeit verhandelten Herausforderungen.[1] Nachhaltige und digitale Transformation und ihr Gelingen oder Scheitern haben beide das Potenzial, die Demokratie zu untergraben, in einem Fall wegen der Zerstörung des demokratischen Diskurses, im anderen Fall wegen der Zerstörung der physischen Lebensgrundlagen. Umgekehrt kann auch eine verschlafene und sodann in kurzer Zeit mit radikalen Einschränkungen vollzogene Nachhaltigkeitswende die liberale Demokratie untergraben – und ebenso kann auch die Regulierung der Digitalisierung diktatorische Züge annehmen, wenn die Digitalisierung etwa gezielt für den Aufbau eines Überwachungsstaats genutzt wird. Insofern besteht für beide Transformationen eine doppelte Freiheitsgefährdung. Die Herausforderung für die nachhaltige, wie auch für die digitale Transformation besteht darin, beide Gefährdungen abzuwehren.

Gem. Art. 2 Abs. 1 Paris-Abkommen (PA) muss die globale Erwärmung auf deutlich unter 2 Grad Celsius begrenzt werden und dabei eine Obergrenze von 1,5 Grad angestrebt werden.[2] Um einem 1,5-Grad-Pfad gerecht zu werden, sind weitreichende Änderungen auf dem Energiemarkt notwendig, insbesondere ein baldiger völliger Ausstieg aus den fossilen Brennstoffen (bei Strom, Wärme, Mobilität, Landwirtschaft, Zement und Kunststoffen), neben einer tiefgreifenden Umstellung im Agrar- und Tierhaltungssektor.[3] Im Zuge des Ausbaus der erneuerbaren Energien ist eine zunehmende Digitalisierung insbesondere des Stromnetzes erforderlich. Dies ist insbesondere auf die Dezentralität und Volatilität der erneuerbaren Energien zurückzuführen, welche die Netzbetreiber vor neue Herausforderungen stellen. Die voranschreitende Digitalisierung – deren ambivalente ökologische Effekte andernorts mehrfach untersucht wurden[4] – bringt jedoch auch das Risiko von Angriffen auf digitale Bestandteile des Stromnetzes mit sich.

Bisher lag der Fokus bei Cybersicherheit in Stromnetzen insbesondere auf den Mittel- und Hochspannungsnetzen, da vor allem Großkraftwerke in das Stromnetz einspeisten.[5] Der Ausbau der erneuerbaren Energien führt zu neuen Akteurskategorien am Energiemarkt – sog. Prosumer oder Flexumer –, zu bidirektionalen Leistungsflüssen im Stromnetz und, auf Grund der Volatilität der erneuerbaren Energien, zu einer komplexeren Netzsteuerung und -überwachung. Das Stromnetz entwickelt sich zu einem Smart Grid; Maßnahmen zum Last- und Einspeisemanagement im Stromnetz verändern sich dadurch.[6] Dies gilt insbesondere auch vor dem Hintergrund der Sektorkopplung, da nach und nach auch Bedarfe aus den Sektoren Verkehr und Wärme über elektrifizierte Anwendungen gedeckt werden, etwa durch den Einsatz von Wärmepumpen oder den Rückgriff auf Elektromobilität.[7] Die Notwendigkeit von Anwendungen zur Cybersicherheit verlagert sich somit von einigen großen Anlagen hin zu zahlreichen kleinen Einzelanlagen und von der Mittel- und Hochspannungsebene auf die Verteilernetze. Während ein Angriff auf eine einzelne dieser verhältnismäßig kleinen Anlagen kaum eine Auswirkung auf die Stabilität des Netzes haben mag, spielen die Verflechtung und mögliche Wechselwirkungen zwischen mehreren dieser Einzelanlagen eine Rolle bei der Gefährdung der Systemsicherheit.[8] Dies gilt umso mehr, als vor dem Hintergrund des Kriegs in Osteuropa Energieversorgungsaspekte Teil der Auseinandersetzung werden. Auch die Art der Kriegsführung hat sich in den letzten Jahren wesentlich verändert. Cyberangriffe spielen eine zunehmende Rolle, wie sich et-

**1** Zu diesem Transformationsprozessen und ihren Verbindungslinien Ekardt ZNER 2022, 433 ff.; Garske/Bau/Ekardt Sustainability 2021, 4652; Ekardt/Rath ZNER 2022, 211 ff.

**2** Näher zu Inhalt, Rechtsverbindlichkeit und (drastischer) Reichweite Ekardt/Bärenwaldt/Heyl Environments 2022, 112; Wieding/Stubenrauch/Ekardt Sustainability 2020, 8858; Ekardt/Wieding/Zorn Sustainability 2018, 2812; aufgegriffen in BVerfGE 157, 30 ff.; dazu teils kritisch (weil in einigen Punkten zu defensiv) Ekardt/Heyl Nature Climate Change 2022, 697 ff.; Ekardt/Heß NVwZ 2021, 1421 ff.

**3** Näher dazu Weishaupt/Ekardt/Garske/Stubenrauch/Wieding Sustainability 2020, 2053; Ekardt/Bärenwaldt/Heyl Environments 2022, 112; Ekardt, Sustainability: Transformation, Governance, Ethics, Law, 2019.

**4** Garske/Bau/Ekardt Sustainability 2021, 4652; Ekardt/Rath ZNER 2022, 211 ff.

**5** Böswetter/Bader/Henze u.a., EnerCrypt – Cyberinnovationen für das sichere Energiesystem der Zukunft, 2021, S. 2.

**6** Etezadzadeh, Smart City Made in Germany/Volk/Konermann, 2020, S. 292 f.; TU Berlin, Digitalisierung in der Energiewirtschaft/ Ritschel/Sprengel/Walther, 2021, S. 52 f.

**7** Böswetter/Bader/Henze u.a., EnerCrypt – Cyberinnovationen für das sichere Energiesystem der Zukunft, 2021, S. 2.

**8** Böswetter/Bader/Henze u.a., EnerCrypt – Cyberinnovationen für das sichere Energiesystem der Zukunft, 2021, S. 3; Krebs/Hagenweiler, Energieresilienz und Klimaschutz – Energiesysteme, kritische Infrastrukturen und Nachhaltigkeitsziele, 2021, S. 14 f.

wa an einem Angriff von russischer Seite auf das ukrainische Stromnetz eindrucksvoll zeigte, in dessen Folge mehrere tausend Haushalte in der Ukraine von der Stromversorgung getrennt wurden.[9] Gleiches gilt für die Angriffe auf das Stromnetz des AKW Saporischschja. Auch in Deutschland vermerkte das Bundesamt für Sicherheit in der Informationstechnik (BSI) steigende Zahlen von Cyberattacken auf Kritische Infrastruktureinrichtungen.[10] Doch nicht nur die Möglichkeit von Cyberangriffen, sondern auch die insgesamt gesteigerte Komplexität des Stromnetzes und die dadurch erhöhte Anfälligkeit für Störungen durch Extremwetterereignisse oder menschliches Versagen erhöhen das Bedürfnis nach technologischen Lösungen für ein reibungsloses Funktionieren der Anlagen und des Netzes, um die Aufrechterhaltung der Versorgungssicherheit gewährleisten zu können.[11]

Aus alledem ergeben sich mögliche Anforderungen an eine energiewendetauglich begriffene Cybersicherheit. Aktuelle und bereits bestehende gesetzliche Regelungen auf EU-Ebene, die darauf zu reagieren versuchen, werden im vorliegenden Beitrag näher beleuchtet. Um die Wirksamkeit des Instrumentariums zumindest abschätzen zu können, werden die Gefährdungslagen dabei vorab kurz analysiert.

## II. Arten und Auswirkungen von Cyberangriffen auf dem Energiemarkt

Zum besseren Verständnis der eben geschilderten Gefährdungslagen sollen nachstehend die verbreitetsten Arten von Cyberangriffen kurz erläutert werden. Es wird sich zeigen, dass die jeweilige Angriffsweise auf eine Vielzahl von Zielen auf allen möglichen Ebenen der Energieversorgung angewandt werden kann.

### 1. DDOS-Angriffe, Ransomware, komponentenbasierte Angriffe, Phishing

Bei Distributed Denial of Service(DDOS)-Angriffen werden Systeme dadurch zum Absturz gebracht, dass sie mit einer übergroßen Anzahl von gleichzeitigen Anfragen überlastet werden.[12] Die Hacker bedienen sich dabei oft sog. Botnets, also Netzwerken von hunderten oder gar tausenden infiltrierten Computern, die sie fernsteuern und so gleichzeitig „auf Knopfdruck" zum Angriff auf das jeweilige Ziel veranlassen können.[13] Infolge des Absturzes des Systems ist dieses dann nicht mehr erreichbar, sodass jegliche Überwachungs- und Steuerungsmöglichkeit verloren geht.[14] Die möglichen Angriffsszenarien sind vielfältig. So können etwa DDOS-Angriffe auf die Internetanbindung einzelner oder mehrerer zentraler Komponenten[15] eines Energienetzwerks, zB deren Server, gestartet werden. Deren Zusammenbruch hat dann uU den Zusammenbruch des gesamten Energienetzwerks zur Folge. Ebenso kann eine Offensive auf die Schnittstellen einzelner Netzwerkkomponenten zielen, was den Abbruch der Kommunikation zwischen den Komponenten herbeiführt. Mess- und Steuerdaten etwa können dann nicht mehr transferiert werden.

Im Energieversorgungsbereich sehr empfindlich wirken kann ferner der Einsatz von Ransomware (engl. ransom = Lösegeld). Ransomware ist der Überbegriff für alle Arten von Schadprogrammen, die den Zugriff auf Daten oder Systeme einschränken oder unterbinden.[16] Nach Aufspielen der Ransomware wird typischerweise vom Systembetreiber ein Lösegeld für die Freischaltung des Systems gefordert.[17] Ergänzend laden die Hacker oft sensible Systemdaten aus dem Netzwerk herunter, deren Leak dann als zusätzliches Druckmittel genutzt wird.[18] Energieversorgern kann durch das Blockieren zB die Kontrolle über ihre technischen Einrichtungen gänzlich entzogen werden. Auch die oben beschriebene zunehmende Dezentralität der Energieversorgung trägt zur quantitativen Erhöhung der potenziellen Angriffsziele bei. Denn immer mehr eingesetzte Anlagen und Geräte bedeuten immer mehr Geräte-Schnittstellen als Einfallstore für Cyberkriminelle. Auf die Größe der Anlage kommt es dabei nicht zwingend an: So kann etwa das Abschalten mehrerer kleiner Anlagen mittels Botnets die gleiche Gefährdung der Systemsicherheit zur Folge haben wie der Blackout einer großen Anlage.[19]

Die erhöhte Akteurs- und Gerätezahl im Energiebereich macht auch komponentenbasierte Supply-Chain-Angriffe relevant. Dabei zielen Hacker mit ihrem Angriff bewusst auf ein bestimmtes Glied der Lieferkette, um so den nachfolgenden Rest der Kette zu infiltrieren.[20] Kleine Nischenhersteller, die als Zulieferer für die großen Energieerzeuger, Netzbetreiber etc fungieren, haben oftmals weit schwächere Sicherheitssysteme als die großen Energiekonzerne. Gelingt es den Hackern, die Schadsoftware bereits an diesem Punkt der Lieferkette einzuschleusen, werden die infizierten Produkte, zB Software-Module, an die nächste Stufe der Lieferkette weitergeliefert und ermöglichen den Hackern dann auch dort den Zugang.[21] Ebenfalls komponentenbasiert ist die Nutzung von Remote-Zugängen für Cyberattacken. Remote-Zugänge stellen „Hintertüren" dar, die in allen möglichen technischen Einrichtungen eingebaut werden, damit der Hersteller aus der Ferne darauf zugreifen kann, vor allem zu Wartungszwecken.[22] Dabei können die Kriminellen entweder einen direkten Angriff auf den Wartungszugang starten, um diesen zu infiltrieren oder auch schlicht zu blockieren; oder sie greifen die IT-Systeme des Geräteherstellers an und erhalten über diese dann „normalen" Zugriff auf die Remote-Zugänge aller Geräte.[23]

Schließlich sind noch diejenigen Attacken zu nennen, die den schwächsten Teil eines jeden technischen Systems ausnutzen: den Faktor Mensch. Gemeint sind Phishing-Angriffe, wo mittels Social Engineering gezielt versucht wird, Menschen über die Identität und Beweggründe des Hackers zu täuschen und sie so

---

**9** Hierzu Barda Wirtschaftsinformatik & Management 2022, 32 (34); Smith Journal of Energy & Natural Resources Law, 36:4, 373 (377).

**10** Krebs/Hagenweiler, Energieresilienz und Klimaschutz – Energiesysteme, kritische Infrastrukturen und Nachhaltigkeitsziele, 2021, S. 18; vgl. hierzu außerdem mit Blick auf den Russland-Ukraine-Konflikt Bundesamt für Verfassungsschutz, Sicherheitshinweis für die Wirtschaft – Betreff: Krieg in der Ukraine, 2022.

**11** Mit einem Überblick zu möglichen Störursachen Krebs/Hagenweiler, Energieresilienz und Klimaschutz – Energiesysteme, kritische Infrastrukturen und Nachhaltigkeitsziele, 2021, S. 13 ff.

**12** Gupta/Dahiya, Distributed Denial of Service (DDOS) Attacks – Classification, Attacks, Challenges and Countermeasures, 2021, S. 2; Dawson/Omar, New Threats and Countermeasures in Digital Crime and Cyber Terrorism, 2015, S. 77 f.; mit einem Überblick zu den aktuellsten Cybervorfällen Dittrich MMR 2022, 1039.

**13** Sauter, The Coming Swarm: DDoS Actions, Hacktivism, and Civil Disobedience on the Internet, 2014, S. 11; Gupta/Sheng, Machine Learning for Computer and Cyber Security 2019, S. 134.

**14** Munk, The Rise of Politically Motivated Cyber Attacks, 2022, S. 65; Pohlmann, Cyber-Sicherheit, 2022, S. 475 f.

**15** Bundesamt für Sicherheit in der Informationstechnik, Industrial Control System Security, 2022, S. 10.

**16** Jenkinson, Ransomware and Cybercrime, 2022, S. 2; Munk, The Rise of Politically Motivated Cyber Attacks, 2022, S. 64.

**17** Pohlmann, Cyber-Sicherheit, 2022, S. 7; Oakley/Butler/York u.a., Theoretical Cybersecurity, 2022, S. 184 f.; Donaldson/Williams/Siegel, Understanding Security Issues, 2018, S. 17.

**18** Hassan, Ransomware Revealed, 2019, S. 7; Bundesamt für Sicherheit in der Informationstechnik, Bericht zum Digitalen Verbraucherschutz 2021, 2022, S. 20.

**19** UFE, UFE's position on the European Commission's proposal for a Directive on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148, 2021, S. 2.

**20** European Union Agency for Cybersecurity, ENISA Threat Landscape For Supply Chain Attacks, 2021, S. 6; Pohlmann, Cyber-Sicherheit, 2022, S. 46 f.

**21** Martinez/Duran International Journal of Safety and Security Engineering 2021, 537; Munk, The Rise of Politically Motivated Cyber Attacks, 2022, S. 69.

**22** Bundesamt für Sicherheit in der Informationstechnik, Industrial Control System Security, 2022, S. 8.

**23** Bundesamt für Sicherheit in der Informationstechnik, Industrial Control System Security, 2022, S. 12.

zur Herausgabe von sensiblen Daten, insbesondere Passwörter und Zugangsdaten, zu bewegen oder auch zur Installation von Schadsoftware auf dem eigenen Computer.[24]

### 2. Beispiele für energiesystemrelevante Angriffe

Ein Beispiel für das soeben abstrakt Dargestellte bereits vor der jetzigen kriegerischen Konfrontation war der Hackerangriff auf das Stromnetz der Ukraine im Dezember 2015. Dabei attackierten Hacker, die dem Umfeld des russischen Staats zugeschrieben werden, am 23.12.2015 insgesamt drei ukrainische Stromversorger, wobei sie jedoch nur bei einem (Prykarpattyaoblenergo) erfolgreich waren.[25] Der Angriff war über Monate vorbereitet: Zunächst gelangten die Hacker mittels manipulierter Microsoft-Office-Dokumente, die sie an Prykarpattyaoblenergo-Mitarbeiter sandten, in das Verwaltungsnetzwerk des Stromversorgers. Von dort arbeiteten sie sich über mehrere Wochen hinweg in die mit der Verwaltung verbundene IT-Umgebung der Netzleittechnik. Als sie diese schließlich infiltriert hatten, trennten sie mehrere Umspannwerke per Fernwirkung vom Netz. Dies führte zu einem Stromausfall bei circa 230.000 Prykarpattyaoblenergo-Kunden. Parallel löschten die Hacker wichtige Wiederherstellungsdateien im System des Stromversorgers, um so einen Systemneustart zu erschweren. Ferner legten sie den telefonischen Kundendienst des Versorgers mittels eines DDOS-Angriffs lahm. Zwar konnte die Stromversorgung trotz dieses Angriffs auf mehreren Ebenen bereits nach drei Stunden wiederhergestellt werden; doch zeigt sich an dem Beispiel recht anschaulich, welche technischen Möglichkeiten für Cyberkriminelle bereits vor sieben Jahren bestanden.

Auch im April[26] und Juli 2022[27] kam es zu weiteren russischen Angriffen auf das ukrainische Stromnetz, diese waren jedoch erfolglos. Eine weitere Cyberoffensive von russischer Seite erfolgte jüngst auf das Computersystem der Verwaltung von Litauen.[28] Hacker der russischen Vereinigung Killnet starteten dabei massive DDOS-Angriffe u.a. auf das nationale Datentransfernetzwerk, welches u.a. auch für die Erhaltung von kritischen Infrastrukturen zuständig ist. Die Attacken wurden von Sicherheitsexperten lediglich als „Test" eingestuft; es seien jedoch weitere Attacken auf staatliche Ziele, insbesondere auch im Energiebereich, zu erwarten.

Ein aktueller Hackerangriff unter Verwendung von Ransomware fand im Jahr 2021 auf die Colonial Pipeline in den USA statt.[29] Die Colonial Pipeline ist mit 8.800 km Länge die größte Kraftstoffleitung der USA und transportiert täglich circa 2,5 Mio. Barrel Öl quer über die Ostküste der Vereinigten Staaten. Am 7.5.2021 kontaktierten die unbekannten Hacker die Colonial Pipeline und gaben an, das Netzwerk der Pipeline infiltriert zu haben. Zuvor waren sie am 29.4.2021 mittels eines geleakten Mitarbeiter-Passworts in das System gelangt.[30] Sie drohten damit, die Versorgungsleitungen abzuschalten, und forderten ein Lösegeld von insgesamt 4,4 Mio. USD für die Freigabe des Netzwerks. Ferner hatten sie zuvor knapp 100 GB an sensiblen Daten aus dem Netzwerk heruntergeladen und gaben an, diese zu veröffentlichen, sollte Colonial den geforderten Betrag nicht zahlen. Colonial begann unmittelbar danach damit, das Pipeline-System selbstständig für mehrere Tage herunterzufahren. In der Folge kam es zu erheblichen Versorgungsengpässen an der Ostküste der USA: Tankstellen ging das Benzin aus, es bildeten sich lange Schlangen und panikartige Kämpfe um Benzin brachen zwischen den betroffenen Bürgern aus. Einige Tage nach der Attacke wurde das Lösegeld in Bitcoins von Colonial an die Kriminellen gezahlt. Erst im Anschluss fand man heraus, dass die Hacker lediglich die Informationstechnologie gekapert hatten, jedoch nicht bis in das operative System, welches den tatsächlichen Kraftstoffffluss in den Leitungen steuert, vorgedrungen waren. In das Colonial-Netzwerk gelangt waren die Hacker mittels eines geleakten Passworts eines inaktiven Mitarbeiter-Accounts, mit dem jedoch immer noch auf das System zugegriffen werden konnte. Das Passwort stammte aus einem Leak aus dem Darknet; der Mitarbeiter hatte das gleiche Passwort auch anderenorts verwendet, wo es dann Teil eines geleakten Passwort-Pakets wurde. Damit konnten sich die Kriminellen einfach mittels Nutzernamen und Passwort in dem Netzwerk anmelden und dieses infiltrieren. Hier veranschaulicht sich der Schwäche-Faktor Mensch: Auch die technisch besten Sicherheitssysteme versagen, wenn in personeller Hinsicht Defizite im Umgang mit Cybersicherheit bestehen.

## III. Analyse der Entwicklung des rechtlichen Steuerungsrahmens auf EU-Ebene

### 1. NIS-RL

Im Jahr 2016 ist die RL (EU) 2016/1148 des europäischen Parlaments und des Rates über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union (NIS-RL)[31] in Kraft getreten. Durch diese RL wurde für die Mitgliedstaaten die Pflicht geschaffen, eine nationale Strategie für die Sicherheit von Netz- und Informationssystemen festzulegen (hierzu Art. 7 NIS-RL). Dies ist für Deutschland die „Cybersicherheitsstrategie für Deutschland 2021", welche die „Cybersicherheitsstrategie für Deutschland 2016" ersetzt und den ressortübergreifenden strategischen

---

**24** Erbschloe, Social Engineering, 2020, S. 1 f.; Pohlmann, Cyber-Sicherheit, 2022, S. 197.

**25** Shehod, Ukraine Power Grid Cyberattack and US Susceptibility: Cybersecurity Implications of Smart Grid Advancements in the US, 2016, S. 3 ff.; Zetter, Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid, 3.3.2016, abrufbar unter: https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/; Tanriverdi, Bundesamt geht von Hackerangriff auf ukrainisches Stromnetz aus v. 22.1.2016, abrufbar unter: https://www.sueddeutsche.de/digital/ukraine-bundesamt-geht-von-hackerangriff-auf-ukrainisches-stromnetz-aus-1.2830197; Park/Walstrom, Cyberattack on Critical Infrastructure: Russia and the Ukrainian Power Grid Attacks v. 11.10.2017, abrufbar unter: https://jsis.washington.edu/news/cyberattack-critical-infrastructure-russia-ukrainian-power-grid-attacks/.

**26** Howell O'Neill, Russian hackers tried to bring down Ukraine's power grid to help the invasion v. 12.4.2022, abrufbar unter: https://www.technologyreview.com/2022/04/12/1049586/russian-hackers-tried-to-bring-down-ukraines-power-grid-to-help-the-invasion/.

**27** Lyngaas, Russian hackers allegedly target Ukraine's biggest private energy firm v. 5.7.2022, abrufbar unter: https://edition.cnn.com/2022/07/01/politics/russia-ukraine-dtek-hack/index.html.

**28** Higgins, Lithuania blames Russia for cyberattacks, citing threats over cargo restrictions v. 27.6.2022, abrufbar unter: https://www.nytimes.com/2022/06/27/world/europe/lithuania-russia-cyberattacks.html; Lyngaas, Pro-Russia hackers claim responsibility for 'intense, ongoing' cyberattack against Lithuanian websites v. 27.6.2022, abrufbar unter: https://edition.cnn.com/2022/06/27/politics/lithuania-cyberattack-pro-russian-group/index.html; Sytas, Russian group claims hack of Lithuanian sites in retaliation for transit ban v. 27.6.2022, abrufbar unter: https://www.reuters.com/technology/lithuania-hit-by-cyber-attack-government-agency-2022-06-27/; Roussi/Cerulus, Russian hackers attack Lithuania over Kaliningrad sanctions v. 27.6.2022, abrufbar unter: https://www.politico.eu/article/russia-hackers-killnet-attack-lithuania-over-kaliningrad-sanction/.

**29** Dazu näher Reeder/Hall The Cyber Defense Review 2021 (Vol. 6 No. 3), 15 ff.; Bogage, Colonial Pipeline CEO says paying $4.4 million ransom was the right thing to do for the country v. 19.5.2021, abrufbar unter: https://www.washingtonpost.com/business/2021/05/19/colonial-pipeline-ransom-joseph-blunt/; Englund/Telford/Nakashima, Colonial Pipeline 'ransomware' attack shows cyber vulnerabilities of U.S. energy grid v. 10.5.2021, abrufbar unter: https://www.washingtonpost.com/business/2021/05/10/colonial-pipeline-gas-oil-markets/; tagesschau, Colonial Pipeline zahlte Lösegeld v. 20.5.2021, abrufbar unter: https://www.tagesschau.de/wirtschaft/unternehmen/colonial-pipeline-loesegeld-hacker-angriff-ransomware-101.html.

**30** Turton/Mehrotra, Hackers Breached Colonial Pipeline Using Compromised Password v. 4.6.2021, abrufbar unter: https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password?leadSource=uverify%20wall.

**31** RL (EU) 2016/1148 des europäischen Parlaments und des Rates v. 6.7.2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union, ABl. 2016 L 194, 1.

Rahmen für die Aktivitäten der Bundesregierung im Bereich Cybersicherheit für – der Intention nach – die nächsten fünf Jahre bildet.[32] Diese Strategie erwähnt konkret den Energiemarkt bzw. Smart Grids an verschiedenen Stellen, wodurch deutlich wird, dass die Bundesregierung den Bedarf nach Anwendungen der Cybersicherheit in diesen Bereichen bereits vor den kriegerischen Entwicklungen des Jahres 2022 erkannt hatte.[33] Darüber hinaus wurde durch die RL eine Kooperationsgruppe zur Unterstützung und Erleichterung der strategischen Zusammenarbeit und des Informationsaustauschs zwischen den Mitgliedstaaten sowie ein Netzwerk von Computer-Notfallteams (CSIRTs-Netzwerk – Computer Security Incident Response Teams Network) zur Förderung einer raschen und wirksamen operativen Zusammenarbeit und zum Vertrauensaufbau zwischen den Mitgliedstaaten geschaffen (vgl. Art. 9 NIS-RL). Zu den Aufgaben der durch die Mitgliedstaaten neu einzurichtenden Computer-Notfallteams gehören u.a. die Überwachung von Sicherheitsvorfällen ebenso wie die Reaktion auf selbige; zudem sollen sie frühzeitig vor Risiken warnen (vgl. Anhang I Nr. 2 NIS-RL). Ferner wurden Sicherheitsanforderungen und Meldepflichten für die Betreiber wesentlicher Dienste und für Anbieter digitaler Dienste festgelegt und für die Mitgliedstaaten die Pflicht begründet, nationale zuständige Behörden und zentrale Anlaufstellen mit Aufgaben im Zusammenhang mit der Sicherheit von Netz- und Informationssystemen zu benennen (Art. 1 Abs. 2 NIS-RL).[34]

## 2. NIS-2-RL

Da ein hohes gemeinsames Cybersicherheitsniveau in der gesamten Union geschaffen werden und zudem auf die aktuelle Situation reagiert werden sollte, haben sich der Rat und das Europäische Parlament im Mai 2022 auf eine Ersetzung der NIS-RL durch die NIS-2-RL geeinigt.[35] Es sollen mit der überarbeiteten RL Unterschiede hinsichtlich der Anforderungen an die Cybersicherheit und bei der Umsetzung von Cybersicherheitsmaßnahmen in den Mitgliedstaaten beseitigt werden. Im Richtlinienentwurf werden daher weitergehende Mindestvorschriften für einen Rechtsrahmen und Mechanismen für eine wirksame Zusammenarbeit zwischen den Mitgliedstaaten festgelegt, wobei den Mitgliedstaaten wie bereits in der NIS-RL freigestellt wird, strengere Vorschriften zu erlassen (Art. 3 NIS-2-RL-E). Auch werden Abhilfemaßnahmen (vgl. Art. 18 NIS-2-RL-E) und Sanktionen festgelegt, um die Durchsetzung der Sicherheitsstandards zu gewährleisten (Art. 31 ff. NIS-2-RL-E). Außerdem soll das Netzwerk der Verbindungsorganisationen für Cyberkrisen, EU-CyCLONe, eingerichtet werden, welches bei dem Management von Cybersicherheitsvorfällen unterstützen soll (Art. 14 NIS-2-RL-E). Eine der wichtigsten geplanten Änderungen ist die Erweiterung des Anwendungsbereichs der RL um weitere Sektoren. Der NIS-2-Richtlinienentwurf umfasst u.a. den Energiesektor, konkret Elektrizität, Fernwärme und -kälte, Erdöl, Erdgas und Wasserstoff (Anhang I NIS-2-RL-E). Es werden durch die RL EU-weit einheitliche Schwellenwerte für die Definition von Unternehmen als Betreiber wesentlicher Dienste eingeführt, die sich vornehmlich an der Größe der Unternehmen orientieren (vgl. Art. 2 NIS-2-RL-E).[36] Die Festlegung dieser Schwellenwerte war zuvor den Mitgliedstaaten überlassen. Gem. Art. 2 Abs. 2 NIS-2-RL-E entfaltet die RL unabhängig vom Erreichen der Schwellenwerte auch in anderen Fällen Wirkung. Dies gilt etwa, wenn sich eine mögliche Störung des von der Einrichtung erbrachten Dienstes wesentlich auf die öffentliche Ordnung, die öffentliche Sicherheit oder die öffentliche Gesundheit auswirken könnte (Art. 2 Abs. 2 lit. d NIS-2-RL-E) oder wenn eine mögliche Störung des von der Einrichtung erbrachten Dienstes zu wesentlichen Systemrisiken führen könnte, insbesondere in Sektoren, in denen eine solche Störung grenzübergreifende Auswirkungen haben könnte (Art. 2 Abs. 2 lit. e NIS-2-RL-E).

Während der NIS-2-Richtlinienentwurf grundsätzlich ein sinnvoller Schritt auf dem Weg zu einer wirksamen EU-Cybersicherheit ist, gilt es den Entwurfstext in seiner extensiv-generalisierenden Art in entscheidenden Punkten noch konkreter zu fassen. Auch die zukünftigen Bedrohungen Kritischer Infrastrukturen durch den Klimawandel sollten verstärkt in den Richtlinienentwurf einbezogen werden.[37] Art. 2 NIS-2-RL-E etwa erweitert den Anwendungsbereich der RL um zahlreiche Adressaten. Nach Art. 2 Abs. 1 S. 2 NIS-2-RL-E fallen lediglich Kleinst- und Kleinunternehmen (dh Unternehmen, die weniger als 50 Mitarbeiter beschäftigen und deren Umsatz 10 Mio. EUR nicht übersteigt) nicht in den Anwendungsbereich der RL. Dabei ist es jedoch zweifelhaft – gerade im Energiesektor –, ob die Anzahl der Mitarbeiter eines Unternehmens und dessen Umsatz die adäquaten Faktoren sind, um die Wichtigkeit des Unternehmens für die Versorgung der EU zu bestimmen. Es wäre grundsätzlich sinnvoller, sich mehr an der Kritikalität einer einzelnen Anlage als an deren Größe oder Sektorzugehörigkeit zu orientieren.[38] Denn nur wenigen Unternehmen allein kommt eine kritische Rolle zu. Den mittelgroßen und kleineren Unternehmen, die in den Richtlinienanwendungsbereich fallen, wird man eine solche Rolle durchweg absprechen können, denn der Ausfall eines einzelnen dieser Unternehmen kann keinen fatalen Effekt auf die Gesamtversorgung haben, da die entsprechende Leistung immer auch von anderen Unternehmen erbracht werden kann.[39] Für eine wirkliche Störung der Versorgungssicherheit müsste eine Vielzahl solcher Unternehmen betroffen sein. Der kumulative Effekt hingegen kann tatsächlich ein ernstes Risiko für die Versorgungssicherheit bedeuten. Dass genau ein solcher kumulativer Effekt im Energiesektor auftreten kann, wurde bereits erläutert.

Insofern lässt sich genauso argumentieren, dass der Anwendungsbereich der RL möglichst groß sein muss, um ein Mindestmaß an Cybersicherheit möglichst weitreichend zu gewährleisten, vor allem auch mit Blick auf die wichtige Rolle vieler kleinerer Unternehmen in Produktlieferketten.[40] Es ist von entscheidender Bedeutung, dass der Gesetzgeber berücksichtigt, dass bei Energieerzeugern und -versorgern – anders als in vielen anderen Sektoren – die Notwendigkeit von IT-Sicherheit sehr wenig mit der Größe ihrer Eigentümer- oder Betreibergesellschaft

---

**32** BMI, Cybersicherheitsstrategie für Deutschland 2021, 2021; zum nationalen Rechtsrahmen demnächst Rath/Ekardt/Schiela in MMR 3/2023.

**33** Etwa BMI, Cybersicherheitsstrategie für Deutschland 2021, 2021, S. 63.

**34** Hierzu Krzykowski Energies 2021, 14 (18 f.); Knoll/Held, Rechtsrahmen der Digitalisierung, 2020, S. 14 f.

**35** Die allgemeine Ausrichtung des Rates zum Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union und zur Aufhebung der RL (EU) 2016/1148 (NIS-2-RL) ist abrufbar unter: https://data.consilium.europa.eu/doc/document/ST-14337-2021-INIT/de/pdf; vergleichend zu beiden Richtlinien Dragomir SEA – Practical Application of Science Volume IX, Issue 27, 155 ff.

**36** Vgl. zu den Änderungen im Vergleich zur NIS-RL Rat der EU, Stärkung der EU-weiten Cybersicherheit und Resilienz – vorläufige Einigung zwischen Rat und Europäischem Parlament, PM v. 13.5.2022, abrufbar unter: 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/; Krzykowski Energies 2021, 14 (20); Sievers Int. Cybersecur. Law Rev. 2021, 223 (225 ff.).

**37** Fekete, Kritische Infrastruktur und Versorgung der Bevölkerung/Begerow/Fekete/Lechleuthner, 2022, S. 18 f.

**38** BDEW, Stellungnahme zum Kommissionsvorschlag für die Überarbeitung der „NIS-Richtlinie" (EU) 2016/1148 (Gewährleistung einer EU-weit hohen Netz- und Informationssicherheit), 2021, S. 6; ebenfalls zur Einbeziehung kleinerer Unternehmen Sievers Int. Cybersecur. Law Rev. 2021, 223 (226).

**39** CLECAT, Position Paper on the threshold for Essential Entities in the Proposal for the Revision of Directive 2016/1148 on the security of Network and Information Systems (NIS-2), 2021, S. 2.

**40** SBS, Proposal for a revised Directive on Security of Network and Information Systems (NIS-2 Directive), 2022, S. 3 f.

zu tun hat.[41] In Bezug auf den Energiesektor bedeutet die Ausnahme für Kleinst- und Kleinunternehmen, dass eine beträchtliche Anzahl von Akteuren keinerlei Anforderungen an die Cybersicherheit unterliegen wird. Ein koordinierter Cyberangriff (entweder gleichzeitig oder durch einen Dominoeffekt) auf mehrere Einheiten des Elektrizitätssystems könnte jedoch das gesamte europäische Stromsystem ernstlich gefährden.[42]

Dennoch besteht hier Konkretisierungsbedarf. So muss ein ausgewogenes Verhältnis bei den Anforderungen an Kleinst- und Kleinunternehmen im Energiesektor gefunden werden. Da die Zahl der kleinen Akteure im Elektrizitätssektor in den kommenden Jahren erheblich zunehmen wird,[43] muss sichergestellt werden, dass für sie Mindestanforderungen an das Risikomanagement und die Berichterstattung im Bereich der Cybersicherheit gelten.[44] Diese Anforderungen müssen in einer angemessenen Relation zu den tatsächlichen Risiken und den Kosten der Umsetzung stehen.[45] Durch die hohen Anforderungen entstünden hohe Compliance-Kosten, die gerade für kleinere Unternehmen nur schwer tragbar wären: Gehaltskosten für Compliance- und IT-Spezialisten, für die aufsichtsrechtliche Berichterstattung und die Umsetzung interner Cybersicherheitsmaßnahmen auf Unternehmensebene.[46] Dies könnte womöglich zu einer Gefährdung des Ausbaus der erneuerbaren Energien führen.

Die Gesetzgebung könnte daher zB verschiedene Arten von Einrichtungen des Energiesektors in erster Linie in Abhängigkeit von den von ihnen betriebenen Anlagen – insbesondere den Auswirkungen eines Ausfalls dieser Anlagen auf das Energiesystem – und in zweiter Linie in Abhängigkeit von ihrer Größe als Unternehmen definieren.[47] Die Größe der Unternehmen sollte nur berücksichtigt werden, um einem erhöhten IT-Risiko entgegenzuwirken, aber nicht der Hauptfaktor sein. Die Verpflichtungen zu Risikomanagementmaßnahmen könnten auf der Ebene der Anlagen festgelegt und jeder Art von Einrichtung auf der Grundlage von Kriterien zugewiesen werden, die sich in erster Linie an der Höhe des Risikos und den Auswirkungen möglicher Ereignisse je nach Art von Anlage und Anlagenbestand orientieren.[48] Es sollten also Risikobewertungsstrategien erstellt werden, die Anforderungen an die Eigentümer von Anlagen in Abhängigkeit von den potenziellen Auswirkungen festlegen, die eine Kompromittierung der einzelnen Anlagentypen auf das übrige Energiesystem und auf den Eigentümer der Anlage selbst haben würde.[49] Jedoch ist bei einem solchen Vorgehen stets auch der Umsetzungsaufwand zu bedenken. Eine Einzelfallprüfung für jede Anlage scheidet faktisch aus. Möglich wäre jedoch eine generalisierte Aufstellung von Anforderungen, die sich nach Typ und Größe bzw. Leistungsmenge der jeweiligen Anlage richtet.

Diese Strategien wären zudem einheitlich im gesamten EU-Gebiet anzuwenden. Die in Art. 18 NIS-2-RL-E von den Einrichtungen verlangten Cybersicherheits-Maßnahmen lassen eine ausreichende Differenzierung zwischen den „wichtigen" und den „essenziellen" Einrichtungen vermissen.[50] In der Folge gelten etwa für ein mittelgroßes Unternehmen die gleichen Anforderungen wie für ein Atomkraftwerk. Die in Abs. 2 lit. d NIS-2-RL-E begründete Verantwortung einer Einrichtung für die gesamte Lieferkette ist ebenfalls teilweise schwer umsetzbar, gerade für kleinere Unternehmen, die global agierenden Lieferanten gegenüberstehen.[51] Die ausführlichen Reporting-Pflichten, die in Art. 20 NIS-2-RL-E auferlegt werden, bedeuten in ihrer Extensivität einen hohen bürokratischen Aufwand,[52] sowohl für die verpflichteten Einheiten als auch für die bearbeitenden Behörden. Vor allem die Berichtspflicht für die „near misses" in Art. 20 Abs. 3 lit. a NIS-2-RL-E erscheint außer Verhältnis zum sicherheitstechnischen Nutzen.[53] Zudem wäre es sinnvoll, eine zentrale Stelle als Adressat der Reports einzurichten, zumindest pro Mitgliedstaat, um Rechtsunsicherheit darüber, welche die „zuständigen Stellen" iSd Art. 20 NIS-2-RL-E sind, zu vermeiden und den Aufwand gering zu halten.[54]

## 3. CRA

Hand in Hand mit der Neuauflage der NIS-RL geht der geplante Erlass der EU-RL über die Resilienz kritischer Einrichtungen (Cyber Resilience Act – CRA). Der Rat der Europäischen Union hat mit Datum v. 20.12.2021 eine allgemeine Ausrichtung zum Entwurf dieser RL gebilligt.[55] Zwischenzeitlich wurde außerdem eine politische Einigung zwischen dem Vorsitz des Rates und dem europäischen Parlament über die RL erzielt.[56] Der CRA wird die RL 2008/114/EG zur Ermittlung und Ausweisung europäischer kritischer Infrastrukturen und Bewertung der Notwendigkeit, ihren Schutz zu verbessern,[57] aus dem Jahr 2008 ersetzen. Gem. Art. 2 Abs. 2 lit. g NIS-2-RL-E gelten die Vorschriften der NIS-2 unabhängig vom Erreichen des Schwellenwerts durch eine Einrichtung auch dann, wenn die Einrichtung als Kritische Einrichtung iSd CRA oder als einer Kritischen Einrichtung gleichgestellte Einrichtung gem. Art. 7 CRA-Richtlinienentwurf (CRA-

---

**41** So auch WindEurope, A cybersecurity framework fit for wind energy, 2021, S. 8.

**42** UFE, UFE's position on the European Commission's proposal for a Directive on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148, 2021, S. 2.

**43** Etezadzadeh, Smart City Made in Germany/Volk/Konermann, 2020, S. 292 f.; TU Berlin, Digitalisierung in der Energiewirtschaft/Ritschel/Sprengel/Walther, 2021, S. 52 f.

**44** UFE, UFE's position on the European Commission's proposal for a Directive on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148, 2021, S. 2.

**45** CCIA, NIS-2 Directive CCIA Europe Comments, 2021, S. 4.

**46** BusinessEurope, Draft Position Paper NIS-2.0 Directive, 2021, S. 4; EuroCommerce, Position Paper Revised Network and Information Security (NIS-2) Directive, 2021, S. 2; CECIMO, Directive on Security of Network and Information Systems across the EU, 2021, S. 1; VDMA, NIS-2 – Evaluation and recommendations on the legislative proposal for a directive on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148 – COM (2020) 823 final, 2021, S. 2.

**47** WindEurope, A cybersecurity framework fit for wind energy, 2021, S. 8.

**48** CLECAT, Position Paper on the threshold for Essential Entities in the Proposal for the Revision of Directive 2016/1148 on the security of Network and Information Systems (NIS-2), 2021, S. 1.

**49** WindEurope, A cybersecurity framework fit for wind energy, 2021, S. 8.

**50** Orgalim, Position Paper on the European Commission's proposal for a Directive on measures for a high common level of cybersecurity across the European Union (NIS-2), 2021, S. 5; CECIMO, Directive on Security of Network and Information Systems across the EU, 2021, S. 1.

**51** EuroCommerce, Position Paper Revised Network and Information Security (NIS-2) Directive, 2021, S. 3.

**52** MedTech Europe, NIS-2 Directive Adoption – Proposal for a Directive on measures for a high common level of Cybersecurity across the Union 2020/0359 (COD), 2021, S. 3; CLECAT, Position Paper on the threshold for Essential Entities in the Proposal for the Revision of Directive 2016/1148 on the security of Network and Information Systems (NIS-2), 2021, S. 3.

**53** BSA, The Software Alliance's Feedback on the revised Directive on Security of Network and Information Systems (NIS-2.0), 2021, S. 6; ETNO, Position Paper Revised Directive on Security of Network and Information Systems (NIS-2), 2021, S. 4; AmCham EU, Our Position – Towards a strong European cybersecurity environment, 2021, S. 5.

**54** Bitkom, Bitkom position on the proposal for a renewed Directive on security of network and information systems, 2021, S. 15 f.; ETNO, Position Paper Revised Directive on Security of Network and Information Systems (NIS-2), 2021, S. 5.

**55** Die allgemeine Ausrichtung des Rates zum Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über die Resilienz kritischer Einrichtungen ist abrufbar unter: https://data.consilium.europa.eu/doc/document/ST-14594-2021-INIT/de/pdf; vgl. hierzu ausf. Voigt/Falk MMR 2023, ●●● – in diesem Heft.

**56** Vgl. Rat der EU, Widerstandsfähigkeit der EU: politische Einigung zwischen Ratsvorsitz und Europäischem Parlament über die Stärkung der Resilienz kritischer Einrichtungen, PM v. 28.6.2022, abrufbar unter: https://www.consilium.europa.eu/de/press/press-releases/2022/06/28/eu-resilience-council-presidency-and-european-parliament-reach-political-agreement-to-strengthen-the-resilience-of-critical-entities/.

**57** RL 2008/114/EG des Rates v. 8.12.2008 zur Ermittlung und Ausweisung europäischer kritischer Infrastrukturen und Bewertung der Notwendigkeit, ihren Schutz zu verbessern, ABl. 2008 L 345/75.

E) gilt. Durch den zu verabschiedenden CRA sollen zahlreiche neue Sektoren in den Anwendungsbereich aufgenommen werden, u.a. der Energiesektor. Während die NIS-2-RL den Schutz Kritischer Einrichtungen vor Cybergefahren bezweckt, bezieht sich der CRA auf den Schutz selbiger vor sonstigen Gefahren.

### 4. Cybersecurity Act

Am 27.6.2019 ist die VO (EU) 2019/881 des europäischen Parlaments und des Rates über die ENISA (Agentur der Europäischen Union für Cybersicherheit) und über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik (Rechtsakt zur Cybersicherheit)[58] – kurz Cybersecurity Act – in Kraft getreten.[59] Die ENISA, deren Mandat durch die Verordnung weiter gestärkt wurde, ist eine 2004 gegründete EU-Agentur, die Organen, Einrichtungen und sonstigen Stellen der Union als Bezugspunkt für Beratung und Sachkenntnis im Bereich Cybersicherheit dienen und so für ein hohes Niveau in diesem Bereich sorgen soll. Außerdem wurde durch den Cybersecurity Act ein Rahmen für die Festlegung europäischer Schemata für die Cybersicherheitszertifizierung geschaffen mit dem Ziel, für Produkte, Dienste und Prozesse der Informations- und Kommunikationstechnik (IKT) in der Union ein angemessenes Maß an Cybersicherheit zu gewährleisten (vgl. Art. 1 Cybersecurity Act).

## IV. Fazit und Ausblick

Es wurde deutlich: Das Recht der Cybersicherheit, gerade auch in Bezug zur Energiewende, befindet sich aktuell europäisch in einem komplexen Prozess des Wandels.[60] An einigen Stellen haben sich Konkretisierungsbedarfe gezeigt, ebenso wie gleichzeitig deutlich wurde, dass – letztlich auch (EU-)grundrechtlich – die Verhältnismäßigkeit gewahrt werden muss, wenn detaillierte Pflichten gegenüber Normadressaten auferlegt werden, die diese kaum erfüllen können bzw. auch nur mit sehr begrenztem Mehrwert für die Cybersicherheit erfüllen können.

Dass die Digitalisierung der Energieversorgung – ähnlich wie wohl in anderen Sektoren, etwa in der Mobilität – zwar bestimmte Sicherheitsanforderungen stärken kann, gleichzeitig aber auch eine kaum vollständig zu kontrollierende neue Angriffsfläche bietet, dürfte bei alledem als zwiespältiger Befund bleiben. Soll Energiesicherheit erreicht werden, wird deshalb auch die Dezentralisierung der Energieversorgung stärker vorangetrieben werden müssen; aktuelle Entwicklungen hin zu neuen LNG-Terminals und einem Weiterbetrieb von Atomkraftwerken laufen dem eher zuwider.[61] Ferner wird auch die Suffizienz- respektive Einsparungsoption wieder stärker in den Blick kommen müssen, die ohnehin wegen der Ambivalenzen und begrenzten Verfügbarkeiten erneuerbarer Energien auch ökologisch relevant ist.[62] Einer alten Erkenntnis – ursprünglich aus der monastischen Tradition – folgend, verschafft ein reduzierter Konsum Freiheitsgrade, anders als es die gängige Diskussion über „Verzicht" insinuiert: Er macht eben auch unabhängiger von drohenden Interventionen Dritter.

## Schnell gelesen ...

- Für eine erfolgreiche Energiewende wird eine zunehmende Digitalisierung insbesondere der Stromnetze notwendig sein, welche die Energieversorgung einem größeren Risiko durch Cyberattacken aussetzt.
- Es gab bereits in der Vergangenheit relevante Cyberangriffe auf die Energieversorgung; aktuell wird das Risiko durch den Russland-Ukraine-Krieg verschärft.
- Auf EU-Ebene befinden sich derzeit zwei wichtige Richtlinien im Gesetzgebungsprozess, die EU-weit für ein höheres Cybersicherheitsniveau sorgen sollen und u.a. eine Neudefinierung des Begriffs der „wesentlichen Dienste" vornimmt.
- Ein besonderes Augenmerk ist bei neuen Regelungen zur Cybersicherheit auf die Verhältnismäßigkeit zu legen, um der Energiewende keine zusätzlichen Steine in den Weg zu legen.

Ass. iur. Theresa Rath,
ist Doktorandin an der Forschungsstelle Nachhaltigkeit und Klimapolitik (FNK) in Leipzig und Berlin, in Verbindung mit der Universität Rostock, Juristische Fakultät.

Prof. Dr. Dr. Felix Ekardt, LL.M.,
ist Leiter der Forschungsstelle Nachhaltigkeit und Klimapolitik (FNK) in Leipzig und Berlin, in Verbindung mit der Universität Rostock, Juristische Fakultät.

RA Alexander Schiela
ist bei Flick Gocke Schaumburg in Berlin tätig und Doktorand an der Forschungsstelle Nachhaltigkeit und Klimapolitik (FNK) in Leipzig und Berlin.

Dieser Beitrag referiert einige Ergebnisse des dreijährigen Konsortial-Forschungsprojekts „Wärmewende in der kommunalen Energieversorgung (KoWa)".

**58** VO (EU) 2019/881 des europäischen Parlaments und des Rates v. 17.4.2019 über die ENISA (Agentur der Europäischen Union für Cybersicherheit) und über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik (Rechtsakt zur Cybersicherheit), ABl. 2019 L 151, 15.
**59** Knoll/Held, Rechtsrahmen der Digitalisierung, 2020, S. 15 f.
**60** Zur nationalen Situation demnächst Rath/Ekardt/Schiela in MMR 3/2023.
**61** Hennig/Ekardt/Antonow u.a. ZNER 2022, 195 ff.; Rath/Ekardt KlimR 2022, 171 ff.
**62** Vgl. Ekardt ZUR 2022, 473 ff.; Ekardt, Sustainability: Transformation, Governance, Ethics, Law, 2019, Ch. 1.3.