Leonie Sterz/Christoph Werner/Prof. Dr. Oliver Raabe

Intelligente Verkehrssysteme – IT-Sicherheit in offenen Infrastrukturen Teil 1

Der Straßenverkehr wird zunehmend digitalisiert. Dies betrifft sowohl die Fahrzeuge selbst, in denen vermehrt digitale Funktionen wie Assistenzsysteme implementiert werden, als auch die Verkehrsinfrastruktur, in der analoge Verkehrssteuerungsfunktionen wie Straßenschilder und Ampeln durch digitale Systeme ersetzt oder zumindest ergänzt werden. Zu diesen Systemen zählen insbesondere intelligente Verkehrssysteme (IVS), bei denen Informations- und Kommunikationstechnologien im Straßenverkehr, d.h. in den Fahrzeugen, der Verkehrsinfrastruktur und ggf. auch in Wearables von Verkehrsteilnehmer/innen (z.B. Smartphones) eingesetzt werden.[1]

I. Einleitung

Nach dem gesetzlichen Vorstellungsbild verfolgen IVS eine Vielfalt von Zielsetzungen. Neben der effizienteren Verkehrssteuerung sollen auch die Nutzersicherheit und der Komfort erhöht werden.[2] Ein denkbares Szenario ist z.B. das Blaulicht von Einsatzfahrzeugen der Polizei, Feuerwehr und anderen Rettungsdiensten[3] auch digital umzusetzen („virtuelles Blaulicht").[4]

Im Recht wird die Einführung von IVS auf europäischer Ebene durch die RL von 2010[5] (IVS-RL) angestrebt und gefördert. Aus Gründen der dafür notwendigen Kompatibilität und Interoperabilität der an einem IVS beteiligten Systeme wurden delegierte Verordnungen zur Spezifikation erlassen.[6]

Dieser Rechtsrahmen wird durch einen neuen Entwurf zur Änderung der IVS-RL (IVS2-RL-E)[7] fortentwickelt. Mit diesem soll dem Fortschritt in der Digitalisierung der Mobilität in den letzten Jahren Rechnung getragen werden, der durch zunehmende Automatisierung von Kfz bis hin zu einer erstrebten autonomen Fahrfunktion und digital gestütztem Verkehrsmanagement gekennzeichnet ist.[8] Während in den delegierten Verordnungen zur bisherigen IVS-RL vorgesehen war, dass die Daten für die jeweiligen IVS zentral über einen nationalen Zugangspunkt kommuniziert werden,[9] werden die Daten zukünftig vermehrt durch Fahrzeug-Fahrzeug- (V2V), Fahrzeug-Infrastruktur- (V2I) und Infrastruktur-Infrastruktur-Kommunikation (I2I) sowie die Verkehrsvernetzung (V2X)[10] zwischen den Akteuren direkt kommuniziert.[11] Entsprechend werden auch die Regelungen für IVS im IVS2-RL-E um Normen zu kooperativen IVS (C-ITS), die sich durch ebendiesen Austausch von Nachrichten der Nutzer untereinander auszeichnen, ergänzt.[12]

Im Hinblick auf die wachsende Echtzeitkritikalität von Daten und die Vernetzung der Akteure scheint die durchgängige Realisierung von Maßnahmen der IT-Sicherheit zunächst eine Selbstverständlichkeit zu sein. Gleichwohl werden normative Ende-zu-Ende Vorgaben zur Gewähr von IT-Sicherheit z.B. durch Rahmensetzungen für IT-Sicherheitsanalysen und Bestimmung von Kriterien für die Wahl angemessener Schutzmaßnahmen bislang in der geltenden IVS-RL nicht berücksichtigt. Durch den neuen Entwurf der IVS-RL und andere Gesetzesvorhaben[13] wird die IT-Sicherheit aber zumindest teilweise adressiert.[14]

Der zuvor beschriebene Übergang von einer zentralisierten, geschlossenen IVS-Infrastruktur zu offenen IVS mit einem dynamischen Teilnehmerkreis führt zu einem neuen Kommunikationsparadigma mit einem gesteigerten Bedarf einer normativen IT-Sicherheitsregulierung, die gerade und trotz der Rollenvielfalt im IVS eine Ende-zu-Ende Gesamtbetrachtung integriert.

Das IT-Sicherheitsrecht muss dabei insbesondere neben der genannten Echtzeitfähigkeit auch die wachsende Kritikalität der Systeme für vitale Fahrfunktionen und Verkehrssi-

* Diese Untersuchung wurde unterstützt durch Mittel des Topic Engineering Secure Systems (46.23.03) der Helmholtz-Gemeinschaft (HGF) sowie der KASTEL Security Research Labs. Wir bedanken uns bei Frau Julia Straburzynski für ihre Unterstützung bei Recherche und Korrektur.

1 Vgl. Art. 4 Nr. 1 IVS-RL (siehe hierzu unten Fn. 4), § 2 Nr. 1 IVSG.

2 Vgl. Art. 4 Nr. 4 IVS-RL.

3 Vgl. § 38 Abs. 1, 2 StVO.

4 Vgl. Bieker-Walz, Verkehrsmanagement für Einsatzfahrzeuge, S. 15 f.; Spehr, FAZ 23.04.2008, abrufbar unter: https://www.faz.net/-gyg-x1ua, Stand 08.11.2022.

5 Richtlinie 2010/40/EU des Europäischen Parlaments und des Rates vom 7. Juli 2010 zum Rahmen für die Einführung intelligenter Verkehrssysteme im Straßenverkehr und für deren Schnittstellen zu anderen Verkehrsträgern.

6 Die sich auf die vorrangigen Bereiche (Art. 2 IVS-RL) und die daraus abgeleiteten vorrangigen Maßnahmen (Art. 3 IVS-RL) beziehen.

7 COM(2021) 813 final, 2021/0419 (COD), Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates zur Änderung der Richtlinie 2010/40/EU zum Rahmen für die Einführung intelligenter Verkehrssysteme im Straßenverkehr und für deren Schnittstellen zu anderen Verkehrsträgern.

8 Dies spiegelt sich datenschutzrechtlich auch in der Einführung des § 63e StVG wider.

9 Vgl. Art. 5 Abs. 2, 3 del. VO (EU) Nr. 885/2013; Art. 7 Abs. 1, 2 del. VO (EU) Nr. 886/2013.

10 Umfasst auch die Vernetzung mit „persönlichen tragbaren Geräten" wie z.B. Smartphones: Art. 2 Abs. 4 del. VO 2019/1789.

11 Hierfür wird auch der Begriff Mobile Ad-Hoc-Network (MANET) und als Unterbegriff hierzu Vehicle Ad-Hoc-Network (VANET) verwendet, vgl. Plößl, Mehrseitige sichere Ad-hoc Vernetzung von Fahrzeugen, S. 7 f.

12 Vgl. Art. 1 Nr. 3 lit. b IVS2-RL-E.

cherheit sowie die erhöhte Unsicherheit der IT-Verantwortlichen im Hinblick auf Angriffsvektoren und Schutzmaßnahmen reflektieren. Ebenso muss der Rechtsrahmen Herausforderungen aus dem neuen Rollenmodell bewältigen. Einzelne Fahrzeuge unterschiedlicher Hersteller sind konstruktive Bestandteile eines IVS als Datenlieferanten oder -empfänger, treten dem System aber nur temporär bei und verlassen es im nächsten Moment wieder. Über Smartphone-Apps können auch Fußgänger und Radfahrer temporär einbezogen werden.

Eine IT-Sicherheitsregulierung von IVS besteht außerhalb des IVS-Rechts, jedenfalls dem Grunde nach, im Recht kritischer Infrastrukturen (KRITIS-Recht), welches auf europäischer Ebene aus der NIS-RL und auf nationaler Ebene aus dem BSIG und der BSI-KritisV besteht. Dabei sind IVS als kritische Infrastruktur adressiert, wenn das konkrete IVS den Schwellenwert in Ziff. 1.4.3. Anhang 7 der BSI-Kritis-V von 500.000 angeschlossenen oder durchschnittlich im Versorgungsgebiet versorgter Nutzer erreicht oder überschreitet. Dann greifen für die jeweiligen Betreiber die IT-Sicherheitspflichten aus § 8a BSIG, mithin die Pflicht, angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit der informationstechnischen Systeme, Komponenten oder Prozesse zu treffen, die für die Funktionsfähigkeit des IVS maßgeblich sind. Aus der Perspektive der erfassten Systemgrenzen und des weiten Fokus auf Dienstangebote scheint das KRITIS-Recht zunächst im Gegensatz zu eher produktbezogenen Regulierungsregimen (s. Typengenehmigungsrecht, del. VO 2019/1789) grundsätzlich geeignet, den geforderten Ende-zu-Ende Schutz leisten zu können.

Es stellt sich jedoch schon hier die Frage, ob die materiellen Regelungsprinzipien des KRITIS-Rechts, welche auf „klassische" zentrale, geschlossene Infrastrukturen wie die Strom- und Wasserversorgung zugeschnitten sind, für IVS überhaupt geeignet sein können. Allein für die Informationsbasis bei der Wahl von angemessenen Schutzmaßnahmen der IT-Sicherheit nach § 8a BSIG deutet sich bereits an, dass ein Schutzregime, welches für die Herausforderungen in regelmäßig kommunikativ geschlossenen Systemen der klassischen kritischen Infrastrukturen konzipiert ist, diesen Herausforderungen derartig offener Systeme schwerlich gewachsen sein kann.

Weiterhin besteht, allerdings eher produktbezogen, eine IT-Sicherheitsregulierung für Fahrzeuge. Diese ist in Form der UN-R 155[15] im Rahmen von Typengenehmigungs- und Marktüberwachungsverfahren europäisch integriert und stellt so einen Rahmen normativer IT-Sicherheitsregulierung für Kraftfahrzeuge zur Verfügung. Fraglich ist allerdings, ob wegen des produktbezogenen Fokus der UN-R diese wiederum auch die spezifischen Anforderungen der IVS zur Gewähr von Ende-zu-Ende IT-Sicherheit hinreichend in den Fokus nehmen kann.

Vor diesem Hintergrund lohnt sich in diesem ersten Teil des Aufsatzes eine Detailschau der Einzelregelungen und des gesamten Regelungsgefüges bei IVS (II.) auch im Hinblick auf das Zusammenspiel und Lücken bei der Gewähr von Ende-zu-Ende IT-Sicherheit im Rahmen von nationaler, europäischer und internationaler Normsetzung. Ein zentrales Defizit ist das Fehlen einer normativen Risikomethodik bzw. eine nicht hinreichend angepasste Verweisung auf private Normung.[16] Diese Herausforderungen und Regelungslücken werden abschließend unter III. in einem Fazit zusammengefasst. Ein entsprechender Lösungsansatz für die Begründung der Verantwortlichkeit sowie die Gewährleistung der Ende-Zu-Ende IT-Sicherheit werden im zweiten Teil des Beitrags im nächsten Heft vorgestellt.

II. Regelungsgefüge

Im folgenden Abschnitt wird das KRITIS-Recht (1.), die IVS-RL (2.) sowie das fahrzeugbezogene Typengenehmigungsrecht (3.) betrachtet.

1. KRITIS-Recht

a) Anwendbarkeit auf IVS

Wie zuvor beschrieben können IVS als kritische Infrastrukturen erfasst sein, wenn sie den entsprechenden Schwellenwert erreichen. Der Schwellenwert bezieht sich auf die Anzahl von 500.000 angeschlossenen oder durchschnittlich im Versorgungsgebiet versorgten Nutzern. Ist dieser erreicht, unterliegen die Betreiber von IVS den IT-Sicherheitspflichten nach § 8a BSIG.

Allerdings ist diese Anzahl schwerlich zu erreichen: Es besteht ein Wandel von großflächigen, zentral vernetzten IVS-Dienstangeboten zu verteilten, fahrzeugfokussierten und auf multilateraler Echtzeitkommunikation basierenden Diensten. Dies führt dazu, dass pro Dienstangebot die Anzahl der Nutzer/innen deutlich geringer ausfallen wird. Daher soll im zweiten Teil des Beitrags der Frage nachgegangen werden, ob diese Anwendungsvoraussetzung in Form von nutzer3zahlbezogenen Schwellenwerten sachgerecht ist.

b) Wahl von Schutzmaßnahmen

Sofern ein konkretes IVS als kritische Infrastruktur zu werten ist, richten sich gegenwärtig die Anforderungen im Bereich des IT-Sicherheitsrechts nach § 8a BSIG. Die Betreiber des IVS hätten mithin „angemessene" Schutzmaßnahmen zu ergreifen. Fraglich erscheint jedoch, ob der Maßstab der „Angemessenheit" hier hinreichend bestimmt ist. Denn es wird grundsätzlich kein Rahmen für Inhalte, Maßstäbe und Methodik bei der Ermittlung der Angemessenheit von tech-

13 Eine von der Kommission verabschiedete delegierte Verordnung (C(2019)1789 final), die insbesondere auch IT-Sicherheitsanforderungen an C-ITS-Stationen/-Dienste und ein Informationssicherheitsmanagementsystem gemäß ISO/IEC 27001 vorsieht, fand allerdings keine Zustimmung des Rats und konnte daher nicht in Kraft treten. Hierzu näher unter Abschnitt II. 2. c).

14 Ausführlich unter 2. b) und c).

15 UN-Regelung Nr. 155 – Einheitliche Bedingungen für die Genehmigung von Fahrzeugen hinsichtlich der Cybersicherheit und des Cybersicherheitsmanagementsystems [2021/387]

16 Vgl. Ullmann/Strubbe/Wieschebrink, Vernetzter Straßenverkehr: Herausforderungen für die IT-Sicherheit in: Roßnagel/Hornung, Grundrechtsschutz im Smart Car, S. 309.

nisch-organisatorischen Maßnahmen zur IT-Sicherheit bereitgestellt.[17]

aa) Notwendigkeit einer methodischen Konkretisierung

Ein solcher konkretisierter Rahmen könnte jedoch aus mehreren Gründen notwendig sein: Einerseits dürfte im Hinblick auf den Eingriffscharakter der gesetzlich geforderten Investitionen in Sicherheitstechnik und Unternehmensorganisation schon aus Art. 12 und 14 GG eine Konkretisierung der Methodik geboten sein, um ein hinreichendes Maß an Normenbestimmtheit zu erreichen.

Andererseits könnte eine Konkretisierung auch erforderlich sein, um den Betreibern die Einhaltung der Vorgaben und damit der Gewährleistung eines angemessenen IT-Sicherheitsniveaus zu ermöglichen. Hierzu enthalten andere bereichsspezifische Regelungen zu KRITIS regelmäßig schon eine verfahrensrechtliche Konkretisierung dieser Maßstäbe für die Wahl von Schutzmaßnahmen.

So verlangt der IT-Sicherheitskatalog nach § 11 Abs. 1a EnWG der BNetzA, dass die Netzbetreiber im Rahmen der Wahl von Schutzmaßnahmen ein Informationssicherheitsmanagementsystem (ISMS) implementieren, das den Anforderungen der ISO/IEC 27001 in der jeweils geltenden Fassung genügt.[18] Für den dem IVS artverwandten Bereich der Verkehrssteuerungs- und Leitsysteme im kommunalen Straßenverkehr ist nach § 8a Abs. 2 BSIG ein branchenspezifischer Sicherheitsstandard (B3S) eingeführt worden, welcher explizit ein ISMS entsprechend ISO/IEC 27001 fordert.[19] Ebenso wird in Annex IV der o.g. gescheiterten del. VO 2019/1789 verlangt, dass Betreiber einer C-ITS-Station ein ISMS im Einklang mit ISO/IEC 27001 betreiben.[20] Ohne einen Verweis auf die ISO/IEC 27001 wartet hingegen in den Art. 5-14 der Vorschlag für eine Verordnung über die Betriebsstabilität digitaler Systeme des Finanzsektors (DORA) mit einem vollständig konturierten IKT-Risikomanagementrahmen auf.[21] Schließlich tendiert auch die kommende NIS-RL 2.0 in Art. 17 f. zu einem Weg für ein granulares, methodisches Grundkonzept risikobasierter Maßnahmenwahl für die IT-Sicherheit.[22]

Insgesamt kann man konstatieren, dass das Fehlen einer normativen Risikomethodik für die Betreiber kritischer Infrastrukturen problematisch ist. Dies gilt bei IVS im Besonderen, da es sich hier regelmäßig nicht um statische Client-Server-Architekturen handelt, wie sie klassischen KRITIS-Infrastrukturen zu eigen sind.

Die risikoprägenden Unsicherheiten sind hier zum einen deshalb erhöht, da durch verteilte und offene Kommunikationsarchitekturen die vernetzten Teilnehmer wie Fahrzeuge dem System temporär beitreten und ebenso dynamisch wieder austreten können. Zum anderen besteht auch durch die Ermöglichung neuer Angriffsvektoren in Bezug auf die multidirektionalen Nachrichtenübermittlungen eine erhöhte Unsicherheit. Für einen besonderen Bedarf an normativer Formalisierung des Verfahrens zur Risikobestimmung und Maßnahmenwahl spricht zudem, dass im Verhältnis zu den Kfz-Herstellern und dem Regulierungsregime der UN-R 155[23] die Systemgrenzen und damit die Verantwortlichkeit für die IT-Sicherheit explizit bestimmt werden müssen, um Kollisionen der Schutzregime zu vermeiden.

Deshalb ist für IVS eine normative inhaltliche und methodische Konkretisierung zur risikobasierten Ermittlung der Angemessenheit einer Maßnahmenwahl im Vergleich zu „klassischen" kritischen Infrastrukturen erst recht geboten.

bb) Ausgestaltung der Konkretisierung

Hierfür wird bislang wie beschrieben häufig auf die private Normung der ISO/IEC 27000-Normfamilie verwiesen. In Betracht kommen neben einen solchen einfachen Verweis sowohl eine bereichsspezifisch angepasste Verweisung als auch eine unmittelbare gesetzliche Verankerung der Grundzüge einer Risikomethodik.

aaa) Einfache Verweisung

Einerseits könnte nach dem Vorbild des IT-Sicherheitskataloges zu § 11 Abs. 1b EnWG eine dynamische Verweisung auf Methoden und Maßstäbe der ISO/IEC 27000-Normfamilie in Betracht gezogen werden. Es besteht aber die Frage, ob der Inkorporation privater Normwerke durch eine Verweisung nicht die geforderte Normenklarheit gesetzlicher Regelungen entgegensteht. Das Gebot der Normenklarheit besagt, dass Rechtsnormen so formuliert sein müssen, dass der/die Betroffene die Rechtslage erkennen und somit sein/ihr Verhalten daran anpassen kann.[24] Es wird aus dem Rechtsstaatsprinzip nach Art. 20 Abs. 3 GG abgeleitet.[25] Die Verweisungen sollen dem Gebot jedenfalls dann genügen, wenn sie hinreichend klar erkennen lassen, welche – ihrerseits hinreichend klaren und bestimmten Normen – im Einzelnen gelten sollen und wenn dem/der Bürger:in die Rechtslage insgesamt hinreichend klar sein kann.[26] Dies ist bei Verweisen auf die ISO/IEC 27000 besonders problematisch, da diese in der Regel dynamisch auf die jeweils aktuelle Fassung der privaten Normung abstellen.

17 Allerdings besteht die Möglichkeit der Verwendung Branchenspezifischer Sicherheitsstandards (B3S) nach § 8a Abs. 2 BSIG sowie von Audits, Prüfungen und Zertifizierungen, die durch das BSI festgelegt werden (§§ 8a Abs. 3, 5 BSIG).

18 Vgl. BNetzA, IT-Sicherheitskatalog nach § 11 Abs.1a EnWG, S. 10; https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/Energie/Unternehmen_Institutionen/Versorgungssicherheit/IT_Sicherheit/IT_Sicherheitskatalog_08-2015.pdf?__blob=publicationFile&v=1, abgerufen am 08.11.2022.

19 Vgl. DIN VDE V 0832-700 VDE V 0832-700:2019-03, Straßenverkehrs-Signalanlagen, Teil 700: Branchenspezifischer Sicherheitsstandard (B3S) für Verkehrssteuerungs- und Leitsysteme im kommunalen Straßenverkehr, Ziff. 4.3.1., hierzu auch unter Abschnitt 2. c).

20 Vgl. Annex 4 del. VO 2019/1789, S. 3.

21 Vgl. Vorschlag für eine VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES über die Betriebsstabilität digitaler Systeme des Finanzsektors und zur Änderung der Verordnungen (EG) Nr. 1060/2009, (EU) Nr. 648/2012, (EU) Nr. 600/2014 und (EU) Nr. 909/2014 COM(2020) 595 final 2020/0266 (COD).

22 Vgl. Vorschlag für eine RICHTLINIE DES EUROPÄISCHEN PARLAMENTS UND DES RATES über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union und zur Aufhebung der Richtlinie (EU) 2016/1148, COM(2020) 823 final.

23 Bei dem für die Anwendung ebenfalls auf die ISO/IEC 27001 verwiesen wird; vgl. United Nations, ECE/TRANS/WP.29/2021/59, Proposals for Interpretation Documents for UN Regulation No. 155 (Cyber security and cyber security management system), S. 3.

24 Ständige Rechtsprechung des BVerfG, vgl. anstelle vieler BVerfGE 45, 400, 420 = BVerfG NJW 1977, 1723, 1724; BVerfGE 156, 11 = NVwZ 2021, 226 Rn. 87.

25 BVerfGE 45, 400, 420 = BVerfG NJW 1977, 1723, 1724; BVerfGE 156, 11 = NVwZ 2021, 226 Rn. 87.

26 Dürig/Herzog/Scholz/Grzeszick, 98. EL März 2022, GG Art. 20 VII. Rn. 55.

Insofern müssen Verweisungen jedenfalls „begrenzt bleiben und dürfen nicht durch die Inbezugnahme von Normen, die andersartige Spannungslagen bewältigen, ihre Klarheit verlieren und in der Praxis nicht zu übermäßigen Schwierigkeiten bei der Anwendung führen".[27] Gemessen an diesen Maßstäben könnte ein dynamischer gesetzlicher Verweis auf die jeweils gültige Methodik der Risikobewertung und Maßnahmenwahl aus der ISO/IEC 27000-Reihe aus der Perspektive des Rechtsstaatsprinzips allerdings fraglich sein. Ganz grundsätzlich ist diese Normreihe zur Konkretisierung von Methoden, Kriterien und Verfahren zum Risikomanagement der Informationssicherheit bei *privater Geschäftstätigkeit* in Unternehmen bestimmt.

Damit sind aber weitestgehend *andere Spannungslagen*, insbesondere hinsichtlich der Schutzgüter und Risikokriterien, adressiert, als sie der Risikobewertung als Gegenstand von Angemessenheitserwägungen im Rahmen der IT-Sicherheit in IVS zugrunde liegen.

Die für einen Geschäftsbetrieb maßgeblichen Risikokriterien/Schutzgüter wie „Verlust von Finanzmitteln, Beeinträchtigung von Geschäftsplänen und Deadlines" sind im Hinblick auf die IVS-relevanten Schutzgüter/Schadereignisse regelmäßig unerheblich. Allenfalls in diese Richtung weisend, jedoch unklar im Bedeutungsgehalt, können die genannten Risikokriterien der „Verletzung von rechtlichen oder regulatorischen Anforderungen" gelten,[28] wobei sich letzteres als zirkelschlüssig erweisen könnte, als die private Normung gerade die gesetzlichen Anforderungen konkretisieren sollte.

Zudem implementiert die ISO-Normreihe auch das Kriterium der Risikoakzeptanz.[29] Dies ist im Rahmen privatautonomer Entscheidungen, deren Auswirkungen in der Regel auf finanzielle Binnenaspekte gerichtet sind, ein nachvollziehbarer Umstand. Eine gänzlich andere Spannungslage zeigt sich bei den IVS: Hier sind die normativen Schutzgüter der Daseinsvorsorge, des Lebensschutzes und der Verkehrssicherheit maßgeblich. Diesbezüglich existiert kein Spielraum für private Akzeptanzkriterien von Betreibern kritischer Infrastrukturen.

Vor diesem Hintergrund bewältigt die fragliche ISO-Normfamilie offensichtlich andere Spannungslagen zum Risikomanagement als das KRITIS-Recht. Insofern wäre eine nicht angepasste Verweisung auf die jeweils aktuellen Normen der ISO/IEC 27000-Reihe in einer bereichsspezifischen Regelung zu IVS nach dem Rechtsstaatsprinzip aus Art. 20 Abs. 3 GG nicht geeignet, den unbestimmten Rechtsbegriff der Angemessenheit auszufüllen.

aaaa) Angepasste Verweisung oder gesetzliche Ausgestaltung

Eine gesetzliche Ausgestaltung einer Risikomethodik für IVS könnte aber durch einen modifizierenden Verweis auf die ISO/IEC 27001 erfolgen. Die gesetzliche Modifikation müsste dann im Hinblick auf die abwägungsrelevanten Schutzgüter der Verkehrssicherheit und das Kriterium der Risikoakzeptanz erfolgen. Dies würde dem Weg entsprechen, der auf europäischer Ebene durch Anhang IV der del. VO 2019/1789 vorgezeichnet ist. Ebenso könnte aber auch bereichsspezifisch eine vollständige Verfahrungsregelung zu einem ISMS für IVS als kritische Infrastruktur beispielsweise im IVSG implementiert werden.[30]

Die normative Ausgestaltung der Risikomethodik könnte dem Grundgedanken der rechtlichen Privatisierung von ehemaligen Staatsaufgaben folgend zur Gewähr von Straßenverkehrssicherheit durch IVS erforderlich sein. Im KRITIS-Recht entspricht es grundsätzlich dem „Gebot der funktionalen Äquivalenz", dass die Rücknahme der staatlichen Erfüllungsverantwortung wiederum durch verfahrensrechtliche Instrumente des öffentlichen Rechts auszugleichen sein kann.[31] Der diesbezügliche Anknüpfungspunkt ist die objektiv-rechtliche Schutzpflichtdimension der Grundrechte. Als grober Maßstab soll gelten: Je stärker sich der Staat bei der Leistungserbringung auf Private verlässt, desto größer deren Gewähr für die ordnungsgemäße Funktionserfüllung im Schutzpflichtenmodell sein muss.[32] Im Rahmen der Einführung von IVS findet eine Verlagerung von Verantwortlichkeiten für die Straßenverkehrssicherheit auf private Dienstbetreiber statt. Dies gilt insoweit auch für die hierfür notwendige IT-Sicherheit. Angesichts der hier verwendeten hochkomplexen IKT wiese der Staat ohnehin erhebliche Informationsdefizite und Wissensprobleme auf.[33]

Allerdings gilt es bei wissensbasierten Entscheidungsprogrammen, wie bei der Wahl von Schutzmaßnahmen der IT-Sicherheit, zwischen dem Sach-, Erfahrungs- und Regelwissen des Entscheiders zu differenzieren. Das notwendige Sachwissen wird auch schon in klassischen ordnungsrechtlichen Verfahren naturgemäß für die Behörden als instabil angesehen.[34] Gerade im Bereich der Regulierung komplexer Technologien und der Dynamisierung von Rechtsgebieten wird beim staatlichen Entscheider zudem grundsätzlich ein Mangel der stabilen Verfügbarkeit des Erfahrungswissens bei Prognoseentscheidungen unter Unsicherheit, wie es dem Konditionalprogramm von Risikoentscheidungen über IT-Schutzbedarfe eigen ist, angenommen.[35] Auf der Ebene des notwendigen „Regelwissens" könnte allerdings im Hinblick

27 BVerfG NJW 2020, 2235, 2256 Rn. 215.

28 ISO/IEC 27005:2008, S. 8.

29 ISO/IEC 27005:2008, S. 21.

30 Es ist zu beachten, dass die IT-Sicherheitsregelungen der del. VO 2019/1789 produktbezogen auf die einzelnen C-ITS-Stationen ausgelegt sind, wohingegen eine KRITIS-Regelung den Zusammenhang des vollständigen Teilsystems bzw. Dienstangebotes in den Fokus der Risikobetrachtung und Maßnahmenwahl nehmen müsste.

31 Burgi, Die Funktion des Verfahrensrechts in privatisierten Bereichen – Verfahren als Gegenstand der Regulierung nach Verantwortungsteilung in: Hoffmann-Riem/Schmidt-Aßmann, Verwaltungsverfahren und Verwaltungsverfahrensgesetz, S. 155, 174 f.

32 Schoch, Gewährleistungsverwaltung: Stärkung der Privatrechtsgesellschaft?, NVwZ 2008, 241, 244.

33 Schoch, Gewährleistungsverwaltung: Stärkung der Privatrechtsgesellschaft?, NVwZ 2008, 241, 242.

34 Vgl. Röhl, in: Hoffmann-Riem/Schmidt-Aßmann/Voßkuhle, Grundlagen des Verwaltungsrechts Bd. I 2012, S. 748 ff.

35 Vgl. Wollenschläger, Wissensgenerierung im Verfahren, S. 31.

auf eine effektive Gestaltung des Verfahrens des Risikomanagements nach wie vor eine deutliche Überlegenheit staatlicher Kompetenzen angelegt sein.

Hinsichtlich der Methoden der Risikobewertung, könnte sich deshalb die gesetzliche Gestaltung des Verfahrensrahmens für IT-Sicherheit in kritischen Infrastrukturen deutlich sachgerechter darstellen als der einfache oder angepasste Verweis auf die internationale Standardisierung der privaten ISO/IEC 27000-Normfamilie.

Vor diesem Hintergrund erscheint eine gesetzliche Konkretisierung des Verfahrensprogramms und die Konturierung der leitenden inhaltlichen und methodischen Vorgaben für die Wahl von Schutzmaßnahmen bei IVS geboten.

c) Zwischenfazit

Das auf IVS anwendbare KRITIS-Recht weist zumindest ein wesentliches Defizit auf: Das KRITIS-Recht lässt eine für IVS passende Risikomethodik zur Gewährleistung der IT-Sicherheit vermissen. Im zweiten Teil des Beitrags wird sich zeigen, ob mit dem die Anwendbarkeit begründenden Schwellenwertkonzept ein weiteres im Hinblick auf IVS bestehendes Defizit hinzukommt.

2. IVS-RL

Anders als im KRITIS-Recht gibt es in der aktuell geltenden IVS-RL keine Regelungen, die dem IT-Sicherheitsrecht zuzuordnen sind (a). Allerdings finden sich in dem Entwurf der neuen IVS-RL vereinzelt Vorgaben zur IT-Sicherheit (b), die durch delegierte Verordnungen konkretisiert werden können. Hierfür könnte sich der EU-Gesetzgeber an der gescheiterten del. VO 2019/1789 orientieren (c).

a) Bisherige IVS-RL

So verweist Art. 10 IVS-RL lediglich deklaratorisch auf das Datenschutzrecht. In den Grundsätzen für die Spezifikationen und die Einführung von IVS in Anhang II findet sich ebenfalls keine Vorschrift dahingehend, dass IVS angemessen gegen Angriffe auf die IT-Sicherheit geschützt werden müssen. Die dort in Buchstabe i geforderte Belegung der technischen Reife[36] bezieht sich lediglich auf die Betriebssicherheit.

Das Fehlen von Anforderungen im Rahmen des IT-Sicherheitsrechts ist dem vorrangigen Ziel der IVS-Richtlinie, die Einführung von IVS in der Union zu fördern, geschuldet (vgl. Art. 1 Abs. 1, Erwg. 23 IVS-RL). Dies spiegelt sich auch in den vier delegierten Verordnungen wider, die die EU-Kommission zur Ergänzung der IVS-RL erlassen hat. Diese regeln jeweils Einzelheiten zu bestimmten Arten von IVS-Diensten, wie dem eCall,[37] Echtzeitinformationsdiensten,[38] Informationsdiensten für LKW-Parklätze[39] und der Bereitstellung eines Mindestniveaus allgemeiner für die Straßenverkehrssicherheit relevanter Verkehrsinformationen.[40] Anforderungen an die IT-Sicherheit dieser Dienste fehlen auch hier.

b) IVS-2-RL-E

Am 15.12.2021 verabschiedete die EU-Kommission den IVS2-RL-E.[41] Derzeit (Stand 16.11.2022) wird der Entwurf im Rat diskutiert. Der Entwurf behält im Wesentlichen die bisherige Ausrichtung der IVS-RL auf Verbreitung und Verstärkung der Interoperabilität von IVS durch erhöhte Verfügbarkeit der hierfür relevanten Daten und verstärkte Zusammenarbeit der Beteiligten bei.[42] Neu ist, dass der Gesetzgeber auf den oben unter I. erläuterten Wechsel des Kommunikationsparadigmas von einem zentralen und geschlossenen hin zu einem multidirektionalen, offenen und verteilten System reagiert hat. So werden mit dem Entwurf die bereits erwähnten C-ITS aufgenommen. Auf die in C-ITS erhöhte Unsicherheit hat der Gesetzgeber durch die Aufnahme von IT-Sicherheitsvorschriften reagiert. Neben den IT-Sicherheitsvorschriften zu C-ITS enthält der IVS2-RL-E auch einige wenige allgemeine IT-sicherheitsrechtlichen Regelungen für IVS.

Die IT-sicherheitsrechtlichen Regelungen werden im Folgenden zusammengefasst.

aa) Allgemeine IT-Sicherheitsregelungen für IVS

Für IVS existieren im IVS2-RL-E zwar keine materiellen IT-Sicherheitsvorgaben, aber solche, die die EU-Kommission zu bestimmten behördlichen Maßnahmen ermächtigen.

Nach Art. 7a IVS2-RL-E kann die EU-Kommission in Notfällen, die einen schwerwiegenden Einfluss auf die Straßenverkehrssicherheit, die IT-Sicherheit und die Verfügbarkeit sowie Integrität von IVS-Diensten haben, vorläufige Maßnahmen erlassen. Der Anwendungsbereich beschränkt sich auf die vorrangigen Bereiche gem. Art. 2 IVS-RL. Außerdem müsste der Notfall geeignet sein, das sichere und ordnungsgemäße Funktionieren des Verkehrssystems der EU zu beeinträchtigen. Unklar ist, was unter einem schwerwiegenden Einfluss zu verstehen ist. Die Vorschrift bezieht sich nur auf überregional wirkende Ereignisse, wodurch der Anwendungsbereich erheblich eingeschränkt ist.

36 Art. 5 Abs. 1 i.V.m. Anhang II lit. i IVS-RL „Belegung der technischen Reife: d. h. nach einer angemessenen Risikobewertung die Zuverlässigkeit innovativer IVS anhand ausreichender technischer Entwicklung und betrieblicher Nutzung nachweisen".

37 Delegierte Verordnung (EU) Nr. 305/2013 der Kommission vom 26. November 2012 zur Ergänzung der Richtlinie 2010/40/EU des Europäischen Parlaments und des Rates in Bezug auf die harmonisierte Bereitstellung eines interoperablen EU-weiten eCall-Dienstes.

38 Delegierte VO 2015/962 der Kommission vom 18. Dezember 2014 zur Ergänzung der Richtlinie 2010/40/EU des Europäischen Parlaments und des Rates hinsichtlich der Bereitstellung EU-weiter Echtzeit-Verkehrsinformationsdienste.

39 Delegierte VO (EU) Nr. 885/2013 der Kommission vom 15. Mai 2013 zur Ergänzung der Richtlinie 2010/40/EU des Europäischen Parlaments und des Rates in Bezug auf die Bereitstellung von Informationsdiensten für sichere Parkplätze für Lastkraftwagen und andere gewerbliche Fahrzeuge.

40 Delegierte VO (EU) 2022/670 der Kommission vom 2. Februar 2022 zur Ergänzung der Richtlinie 2010/40/EU des Europäischen Parlaments und des Rates hinsichtlich der Bereitstellung EU-weiter Echtzeit-Verkehrsinformationsdienste.

41 COM(2021) 813 final.

42 Vgl. S. 6 des Entwurfs COM(2021) 813 final.

Daneben ist die EU-Kommission nach Art. 6 Abs. 1 i.V.m. Art. 7 Abs. 1 IVS-RL und Anhang I Ziff. 3.4.1 IVS2-RL-E befähigt, Spezifikationen zur Unterstützung der Sicherheit in Bezug auf das Human-Machine-Interface, zur Verwendung mobiler Geräte wie beispielsweise Smartphones und zur Sicherheit der fahrzeuginternen Kommunikation zu erlassen. Da sich insbesondere erstere und letztere Regelungen mit dem fahrzeugspezifischen Recht überschneiden könnten (siehe Abschnitt 3.), gilt die Befugnis zum Erlass der Spezifikationen nur, soweit sie nicht in den Geltungsbereich der einschlägigen fahrzeugspezifischen Verordnungen[43] fallen. Inwieweit hierfür neben der umfassenden UN-R 155 überhaupt Raum ist (hierzu unter Abschnitt 3. a), ist unklar.

bb) Besondere IT-Sicherheitsregelungen für C-ITS

Für C-ITS enthält der Entwurf Ermächtigungen zum Erlass von Anforderungen an die Public Key Infrastructure (PKI) und Sicherheitskonzepte für das Risikomanagement bei C-ITS-Diensten.

aaa) Anforderungen an die PKI

Die für C-ITS ausgetauschten V2X-Nachrichten werden unverschlüsselt gebroadcastet, d.h. jede Person mit einem Empfangsgerät kann diese lesen. Die Gefahr der Erstellung von Bewegungsprofilen wird durch die pseudonymisierte Versendung und regelmäßige Änderung des Pseudonyms verringert. Um Vertrauen in die Authentizität und Integrität der Nachrichten herzustellen, werden sie zudem signiert übertragen. Hierfür wird eine PKI verwendet. Da es mehrere PKI geben kann, ist zur Sicherstellung der Interoperabilität und des Vertrauens der PKI untereinander eine übergeordnete Instanz erforderlich. Diesbezüglich kann die EU-Kommission nach Art. 10a IVS2-RL-E und Anhang I Ziff. 4.3 Spezifikationen für ein EU-System für das Management von Sicherheitsberechtigungsnachweisen von C-ITS-Diensten erlassen (EU C-ITS Security Credential Management System – EU CCMS). Hierzu gehört die Festlegung bestimmter Rollen (Anhang I Ziff. 4.3.2. IVS2-RL-E) sowie der Erlass von Regeln für die Verwaltung von Public Key Zertifikaten für C-ITS-Dienste (Anhang I Ziff. 4.3.1. IVS2-RL-E).

Im Rahmen der o.g. del. VO 2019/1789 wurde bereits eine Zertifikatsrichtlinie erarbeitet, die gemeinsame Regeln für den Betrieb einer PKI festlegt.[44] Auch wenn die del. VO nicht in Kraft getreten ist, wird die Zertifikatsrichtlinie bis heute verwendet und ist verpflichtend, wenn man als Organisation am EU CCMS teilnehmen möchte.[45] Das BSI hat kürzlich zwei Technische Richtlinien erlassen, die die Anforderungen aus der Zertifikatsrichtlinie zusammenfassen und ergänzen.[46] Da sich die unverbindliche Zertifikatsrichtlinie in der Praxis bereits durchgesetzt hat, darf angenommen werden, dass sich die EU-Kommission für eine neu erlassene, verbindliche Zertifikatsrichtlinie auf Basis des IVS2-RL-E an der bisherigen Zertifikatsrichtlinie orientieren wird.

Auch die Rollen sollten bereits in der del. VO 2019/1789 festgelegt werden. Danach sollte die EU-Kommission die erforderlichen Rollen übernehmen, bis eine gesonderte Instanz dafür geschaffen wurde (Art. 24-26 del. VO 2019/1789). Auch hieran könnte sich der EU-Gesetzgeber bei Erlass neuer Spezifikationen auf Basis des IVS2-RL-E orientieren.

aaaa) Sicherheitskonzept für C-ITS-Dienste

Weiterhin ist bei den Spezifikationen im Rahmen des EU CCMS der Erlass eines Sicherheitskonzepts für das Informationssicherheitsmanagement in C-ITS-Diensten vorgesehen (Anhang I Ziff. 4.3.3. IVS2-RL-E). Regelungstechnisch ist dies nicht ganz geglückt, da der Umfang dieses Sicherheitskonzepts nicht klar wird. Weil das Sicherheitskonzept als Unterpunkt zum EU CCMS aufgeführt ist, könnte man wegen der Systematik den Umfang allein auf solches Informationssicherheitsmanagement beziehen, das auf Zertifikaten basiert. Dies würde aber verkennen, dass sich ein umfassendes Informationssicherheitsmanagement nicht in der Verwendung und Verwaltung von Zertifikaten erschöpfen kann. So sind Angriffe denkbar, die sich durch Signaturzertifikate nicht verhindern lassen, wie DoS-Angriffe oder die Verfälschung von Daten durch Manipulation von Sensoren, bevor diese per V2X-Nachricht versendet werden. Auch die Sicherheitsrichtlinie aus der del. VO 2019/1789 (dazu sogleich unter Abschnitt 2.c), die hier wieder als Anhaltspunkt für eine neue delegierte Verordnung herangezogen werden könnte, bezieht sich nicht nur auf Zertifikate, sondern auf ein allgemeines Management der Informationssicherheit in C-ITS. Dies alles spricht dafür, auch das im IVS2-RL-E aufgeführte Sicherheitskonzept allgemein und nicht lediglich in Bezug auf Zertifikate auszulegen. Um dies klarzustellen, hätte die Ziff. 4.3.3. Anhang 1 IVS2-RL-E neben und nicht unter dem EU CCMS aufgeführt werden sollen (beispielsweise als Ziff. 4.4.).

cc) Zwischenfazit

Insgesamt geht der IVS2-RL-E aus Sicht der IT-Sicherheit in die richtige Richtung, indem der EU-Gesetzgeber auf den Wechsel des Kommunikationsparadigmas reagiert hat und insbesondere die IT-Sicherheit von C-ITS behandelt. Es bleibt aber abzuwarten, wie die EU-Kommission die genannten Regelungsbereiche durch den Erlass delegierter Rechtsakte nach In-Kraft-Treten des IVS2-RL-E ausfüllen wird und inwiefern sich diese mit dem fahrzeugspezifischen Recht überschneiden werden.

43 Genauer sind dies VO (EU) 2018/858 („TypengenehmigungsVO"), VO (EU) Nr. 167/2013 (TypengenehmigungsVO bezüglich land- und forstwirtschaftlicher Fahrzeuge), VO (EU) Nr. 168/2013 (TypengenehmigungsVO bezüglich zwei- oder dreirädriger Kraftfahrzeuge und vierrädiger Kraftfahrzeuge).

44 Del. VO 2019/1789 Annex 3.

45 Bräunlich/Matzerath, Vorgaben für den sicheren und interoperablen Betrieb von kooperativen intelligenten Transportsystemen im europäischen Anwendungskontext, in: Cyber-Sicherheit ist Chefinnen- und Chefsache! Tagungsband zum 18. Deutschen IT-Sicherheitskongress 2022, S. 157, 159 f.; BSI TR 03164-1 (11); https://cpoc.jrc.ec.europa.eu/Documentation.html, abgerufen am 09.11.2022; https://its-norway.no/wp-content/uploads/2021/02/6-Geert-van-der-Linden-C-ITS-21-03-11.pdf, abgerufen am 09.11.2022.

46 BSI TR 03164-1 und 03164-2.

Da in der gescheiterten del. VO 2019/1789 vor allem hinsichtlich des EU CCMS nahezu dasselbe geregelt werden sollte und da diese trotz ihrer Unverbindlichkeit bereits eine hohe Praxisrelevanz erreicht hat, spricht vieles dafür, dass sich der EU-Gesetzgeber für die zu erlassenden delegierten Rechtsakte an dieser orientieren wird. Angesichts dessen soll die del. VO 2019/1789 in Bezug auf die C-ITS-Sicherheitsrichtlinie im Folgenden kritisch beleuchtet werden.

aaa) Entwurf der del. VO 2019/1789

Die del. VO 2019/1789 sieht in Art. 27 vor, dass jeder Betreiber einer C-ITS-Station ein ISMS nach ISO/IEC 27001 implementiert und dabei die im Anhang IV Abschnitt 1.3.1. enthaltenen Einschränkungen und zusätzlichen Anforderungen berücksichtigt.

Das ISMS umfasst sämtliche C-ITS-Stationen eines Betreibers sowie alle anderen durch ihn betriebenen Informationsverarbeitungssysteme, die die genormten C-ITS Nachrichten verarbeiten (Ziff. 1.3.1. Abs. 1 Annex 4 del. VO 2019/1789). C-ITS-Stationen sind nach Art. 2 Abs. 3 del. VO 2019/1789 alle Software- und Hardwarekomponenten, die die für den C-ITS-Dienst erforderlichen Nachrichten empfangen, senden und verarbeiten. Die del. VO verweist hier auf die EN 302 665 v 1.1.1, die verschiedene Arten von C-ITS-Stationen definiert, namentlich persönliche (z.B. Smartphones), zentrale, straßen- (z.B. RSU) und fahrzeugseitige Stationen.

Mit der Adressierung der C-ITS-Stationen weist die del. VO 2019/1789 weniger eine Dienstperspektive auf, als dies in der übrigen IVS2-RL-E und im KRITIS-Recht üblich ist. Bei beiden Rechtsregimen stehen insoweit der IVS-Dienst bzw. die kritische Dienstleistung (§ 1 Abs. 1 Nr. 3 KritisV) im Vordergrund. Dagegen blickt die del. VO 2019/1789 auf ein C-ITS als Summe einzelner C-ITS-Stationen und nimmt folglich die C-ITS-Station als Produkt in den Fokus. Bei Überschreitung der entsprechenden Schwellenwerte kann die del. VO 2019/1789 daher komplementär zum KRITIS-Recht sein.[47]

Der Betreiber der C-ITS-Stationen in Art. 2 Abs. 16 del. VO 2019/1789 wird nur knapp definiert als jede natürliche oder juristische Person, die für die Inbetriebnahme und den Betrieb von C-ITS-Stationen verantwortlich ist. Wie die Verantwortlichkeit bei mehreren relevanten Personen bestimmt werden soll, wird nicht erläutert. Der Betreiber von C-ITS-Stationen muss im Rahmen des ISMS lediglich andere hierfür relevante Personen und Interessenträger bestimmen. Konkrete Maßnahmen knüpfen hieran jedoch nicht an.

Neben einer erforderlichen Zertifizierung nach der ISO/IEC 27001 hinsichtlich des ISMS (Art. 28 del. VO 2019/1789) bedürfen C-ITS-Stationen einer Zertifizierung nach ISO/IEC 15408, die Evaluationskriterien für die IT-Sicherheit von Produkten und Systemen enthält (Ziff. 1.6.2.2 Abs. 30-32 del. VO 2019/1789). Auch dies zeigt die produktorientierte Sicht der del. VO 2019/1789. Zusätzlich muss eine Konformitätserklärung über die C-ITS-Station abgegeben werden, die besagt, dass die in Art. 5 del. VO 2019/1789 festgesetzten Anforderungen eingehalten wurden (Art. 13 Nr. 1 del. VO 2019/1789 und Annex 5 del. VO 2019/1789). Diese enthalten jedoch keine Anforderungen hinsichtlich der IT-Sicherheit, sondern vorrangig hinsichtlich ihrer Interoperabilität.

Als Zwischenfazit lässt sich zunächst positiv festhalten, dass die del. VO 2019/1789 nicht nur einen einfachen Verweis auf die ISO/IEC 27001, sondern an IVS angepasste Einschränkungen und zusätzliche Anforderungen enthält. So werden besonders die Systemgrenzen, bzw. in der Terminologie der del. VO der Anwendungsbereich, in Ziff. 1.3.1. Abs. 3 Annex 4 del. VO 2019/1789 festgelegt. Zudem werden die möglichen Auswirkungen auf Schutzziele im Fall von IT-Sicherheitsvorfällen bezüglich verschiedener Nachrichtentypen aufgelistet und bewertet (Ziff. 1.4. Annex 4 del. VO 2019/1789). Negativ ist hingegen, dass weder der Katalog an Schutzgütern eindeutig auf das normativ relevante Maß beschränkt wurde[48] noch insoweit die individuelle Risikoakzeptanz ausgeschlossen wurde.

Tendenziell war die del. VO 2019/1789 aus Sicht des IT-Sicherheitsrechts begrüßenswert, weil sie zeigte, dass der europäische Gesetzgeber im Zuge der zunehmenden Vernetzung des Straßenverkehrs das Erfordernis einer IT-sicherheitsrechtlichen Regelung in diesem Bereich erkannt hat. Insofern hat das Scheitern der del. VO 2019/1789 die Entwicklung dieser Rechtsmaterie behindert.

3. Typengenehmigungsrecht

Nach § 2 Nr. 1 IVSG umfassen IVS den Einsatz von IKT im Straßenverkehr, wozu auch die Fahrzeuge gehören.[49] Die Fahrzeuge sind als Informationsquellen und -senken faktisch vernetzter Bestandteil von IVS. Gleichwohl unterfallen Fahrzeuge daneben auch einer eigenen Regulierung, insbesondere dem Typengenehmigungsrecht.

Das Typengenehmigungsrecht regelt die Berechtigung eines Herstellers, für eine unbestimmte Anzahl von ihm gefertigter, baugleicher Fahrzeuge Übereinstimmungsbescheinigungen auszustellen, die dann wiederum für die Zulassung der Fahrzeuge erforderlich sind.[50] Das Typengenehmigungsrecht ist mithin durch eine fahrzeugzentrierte Sicht gekennzeichnet, wobei die Anforderungen an das Fahrzeug durch den Hersteller nachzuweisen sind.

Zentrales Gesetz des Typengenehmigungsrechts ist die Typengenehmigungsverordnung (VO 2018/858), die auf die neuere General Safety Regulation II (VO 2019/2144) verweist. In den Anhängen der letztgenannten werden wiederum diverse UN-Regelungen aufgelistet, die ebenfalls Teil der Anforderungen an die Typengenehmigung sind. Hierzu gehört insbesondere die für die vorliegende Untersuchung relevante UN-R 155, welche die Cybersicherheit der Fahrzeuge betrifft und durch die del. VO (EU) 2022/1389 in die VO 2019/2144 eingefügt wurde.

47 Erwägungsgrund 6 del. VO 2019/1789.

48 Del. VO 2019/1789, Anhang IV, Ziff. 1.4, Abs. 15.

49 Vgl. Art. 4 Nr. 1 IVS-RL.

50 Siebert, in: Siebert, Die Genehmigungsverfahren für Kraftfahrzeuge, 2. Aufl. 2021, S. 23; daneben besteht die Möglichkeit der Einzelgenehmigung von Fahrzeugen, der in der Praxis aber nur eine untergeordnete Bedeutung zukommt.

a) UN-R 155

Die UN-R 155 schreibt zur Gewährleistung der Cybersicherheit die Durchführung eines Cybersecurity-Managementsystems (CSMS) vor. Hierbei handelt es sich im Kern um ein Risikomanagement, d.h. eine Methodik für den Umgang mit Risiken.

Ein Risiko ist nach UN-R 155, „die Möglichkeit, dass durch eine bestimmte Bedrohung Schwachstellen eines Fahrzeugs ausgenutzt werden und dadurch eine Organisation oder einer Person Schaden zugefügt wird." Ergänzend kann die in ISO/SAE 21434 (Road vehicles – Cybersecurity engineering) genannte Definition herangezogen werden,[51] welche Risiko als „die Auswirkung von Ungewissheit auf die Cybersicherheit von Straßenfahrzeugen, ausgedrückt durch die Durchführbarkeit von Angriffen und deren Auswirkungen", beschreibt.[52]

Zusammenfassend kann man damit festhalten, dass mit der Möglichkeit der Ausnutzung bzw. der Durchführbarkeit eines Angriffs die Wahrscheinlichkeit eines Ereignisses beschrieben wird und dieses Ereignis bestimmte Auswirkungen haben kann. Bei den Auswirkungen wird nach ISO/SAE 21434 der Schaden oder die physische Beeinträchtigung eines Schadszenarios betrachtet, welches wiederum als nachteilige Folge oder unerwünschtes Ergebnis aufgrund der Beeinträchtigung einer (oder mehrerer) Cybersicherheitseigenschaft(en) (Schutzziele) eines Assets oder einer Gruppe von Assets definiert ist.

Als Beispiele für Schadensszenarien werden in Ziff. 8.3.2. der ISO/SAE 21434 die Offenlegung von Verbraucherinformationen durch einen Vertraulichkeitsverlust im Infotainmentsystem sowie das ungewollte Auslösen einer Vollbremsung bei Höchstgeschwindigkeit durch einen Integritätsverlust im Bremssystem genannt. Ein Schadensszenario, bei dem das Fahrzeug dritte Verkehrsteilnehmende durch Falschinformationen (ggf. über ein IVS) schädigt, wird hingegen nicht genannt.

Die Risikomethodik wird fachspezifisch weiter ausgestaltet. Als Hilfestellung für die Risikoidentifikation werden in Anhang 5 etwa die Grundzüge der fachspezifischen Bedrohungen, Schwachstellen und Angriffsmethoden benannt. Im Rahmen der Risikobehandlung mindestens zu treffende Maßnahmen sind abstrakt in Anhang 5 Teil B und C niedergelegt, wobei ein Abweichen durch alternativ-gleichwertige bzw. neuere Maßnahmen zugelassen wird. Im Ergebnis müssen die Maßnahmen nach Ziff. 7.3.4, 7.3.5. „angemessen" sein, was bedeutet, dass das verbleibende Risiko auf Basis der Risikokriterien für den Hersteller als tolerierbar angesehen werden muss.[53]

b) Überschneidender Anwendungsbereich

Wie bei der Definition von IVS begründet auch die UN-R 155 einen überschneidenden Anwendungsbereich zwischen IVS und Fahrzeugen: Die Gewährleistung der Cybersicherheit erfordert nach Ziff. 7.3.3 in der Risikobewertung auch die „Wechselwirkungen mit sämtlichen externen Systemen [wie etwa IVS] zu berücksichtigen." Die „Risikobewertung" bildet nach der Definition in Ziff. 2.1 den Oberbegriff für Risikoermittlung, Risikoanalyse und Risikoeinschätzung und damit den Kern des CSMS. Mithin sind diese Wechselwirkungen mit externen Systemen in nahezu der gesamte Risikomethodik zu berücksichtigen.[54]

Mit Blick auf den Lebenszyklus der Fahrzeuge kommt diesem Aspekt auch deshalb besonderes Gewicht zu, da das CSMS nicht nur für die Entwicklungs- und Produktionsphase, sondern auch für die Postproduktionsphase gilt, die nach Ziff. 2.7 bis zum Ende der Lebensdauer aller Fahrzeuge des Fahrzeugtyps andauert, also die vollständige Betriebsphase umfasst. Folglich muss der Hersteller alle Risiken (auch durch Wechselwirkungen mit externen Systemen) berücksichtigen, die in diesem Zeitraum erst noch entstehen, etwa durch das Aufkommen neuer IVS. Durch diese Ausdehnung auf die Betriebsphase der Fahrzeuge wird der Hersteller ähnlich wie der Betreiber eines Systems zur kontinuierlich aktualisierten Risikobewertung (Ziff. 7.2.2.2.) und damit verbundener Risikobehandlung der Fahrzeuge verpflichtet.

c) Unsicherheit

Bezüglich der Bewältigung der Risiken aus Wechselwirkungen mit externen Systemen gilt es jedoch weiterhin zu beachten, dass der Fahrzeughersteller nur Sach- und Erfahrungswissen darüber hat, welche Daten das Fahrzeug von externen Systemen für seine Fahrfunktionen benötigt und wie sich somit auch Manipulationen der Daten auf die Fahrfunktionen auswirken.[55] Erhebliche Unsicherheit besteht beim Fahrzeughersteller hingegen darüber, welche entfernten Auswirkungen von ihm ausgesendete und ggf. durch Dritte manipulierte Daten haben. Die Risikoabschätzung bzgl. des Datenoutputs an externe Systeme bleibt aus der Perspektive des Herstellers somit zwangsläufig unvollständig; es ist insoweit aus Anhang 5 auch nicht ersichtlich, dass diese entfernten Auswirkungen mitberücksichtigt wurden. Insofern besteht ein Wissensdefizit bei der Betrachtung der Risiken im Überschneidungsbereich. Hierauf wird im zweiten Aufsatzteil vertiefend eingegangen.

d) Zwischenfazit

Die UN-R 155 als Bestandteil des Typengenehmigungsrechts fordert vom Fahrzeughersteller die Einhaltung eines Cybersicherheitsmanagements, mithilfe dessen die Cybersicherheitsrisiken über den gesamten Lebenszyklus der Fahrzeuge betrachtet werden. Diese Methodik entspricht auch den bereits dargestellten Anforderungen, mit Ausnahme der auch hier bestehenden Möglichkeit der individuellen Risikoakzeptanz.[56]

51 Siehe: UN-R 155 Interpretation Document, Ziff. 2.1 und zu Ziff. 5.3.1., part (a) hinsichtlich der Kompetenz des Personals.

52 ISO/SAE 21434, Ziff. 3.1.25.

53 UN R 155 Interpretation Document zu Ziff. 7.2.2.2., part (d).

54 In ISO/SAE 21434, Ziff. 9.3.2. wird insoweit auch darauf hingewiesen, dass die Systemgrenzen (hier: item boundaries) anhand der Schnittstellen zu anderen Objekten und Komponenten innerhalb und/oder außerhalb des Fahrzeugs zu beschreiben sind.

55 Z.B. Daten aus der Cloud, vgl. UN-R 155 Interpretation Document, zu Ziff. 7.3.5., part (b).

Gleichzeitig schließt das CSMS auch Risiken aus Wechselwirkungen mit externen Systemen mit ein, wobei der Fahrzeughersteller insofern nur die Risiken für das Fahrzeug und keine entfernten Risiken für IVS durch manipulierte Daten aus dem Fahrzeug betrachten muss. Diese könnte er auch nur unzureichend behandeln, da für ihn mangels Sach- und Erfahrungswissen hohe Unsicherheit darüber besteht, welche Auswirkungen diese Risiken im Rahmen des IVS auslösen könnten.

III. Fazit

Der untersuchte Rechtsrahmen weist diverse Schwierigkeiten und Defizite auf. Im Rahmen des KRITIS-Rechts wurde auf die Problematik des vollständigen Fehlens einer gesetzlichen Risikomethodik sowie auf die alternative Möglichkeit des angepassten Verweises auf private Normung (ISO/SAE 27000) hingewiesen. Außerdem wurde die Frage aufgeworfen, ob das Schwellenwertkonzept im Hinblick auf IVS sachgerecht ist. Dem soll im zweiten Teil des Beitrags weiter nachgegangen werden.

Bezüglich des IVS-Rechts konnte gezeigt werden, dass dieses insbesondere mit dem neuen Entwurf und der gescheiterten delegierten Verordnung sinnvolle Regelungsansätze für die IT-Sicherheit bietet. Kritisch wurde insofern attestiert, dass bei der modifizierenden Verwendung der ISO/SAE 27000-Risikomethodik nicht alle rechtlich relevanten Aspekte auch hinreichend angepasst wurden; dies gilt insbesondere für die fehlende Beschränkung auf normative Schutzgüter sowie die fortbestehende Möglichkeit individueller Risikoakzeptanz.

Schließlich wurde das für die IT-Sicherheit relevante Typengenehmigungsrecht in Form der UN-R 155 untersucht und dabei dieselbe Problematik bezüglich der individuellen Risikoakzeptanz festgestellt.

Noch entscheidender als die bereits genannten methodischen Defizite ist aber, dass sowohl das IVS-Recht als auch die UN-R 155 in ihrem Anwendungsbereich wechselseitige Überschneidungen aufweisen. Es wurde herausgearbeitet, dass diese Überschneidungen sich sachlich immanent aus dem Charakter der IVS als offene Systeme mit den Fahrzeugen als informationsempfangende und -bereitstellende Teilnehmer ergeben. Für die Normadressaten beider Systeme (IVS, Fahrzeuge) besteht somit hohe Unsicherheit über die jeweils anderen Systeme. Hierfür fehlt es bislang an einer gesetzlichen Methodik, mit der diese Unsicherheit bewältigt werden kann. Eine Vertiefung dieses Problems sowie entsprechende Lösungsvorschläge werden im zweiten Teil des Aufsatzes geboten.