Hackerangriff auf ein autonom fahrendes Fahrzeug

13

Welche Rechtsfragen ergeben sich?

Karl Maier, Nicole Antonczyk, Robin Biskup und Leyla Dalir

Zusammenfassung

Der stetige Fortschritt der Technologie führte im letzten Jahrzehnt zu einem verstärkten Fokus auf automatisierte Prozesse. Insbesondere die Automobilindustrie möchte die visionären Vorstellungen von selbstfahrenden Kraftfahrzeugen in den kommenden Jahren zur Realität werden lassen. Mit dem Wegfall der Fahrzeugführer versprechen die Autohersteller ihren Kundinnen und Kunden eine innovative und effiziente neue Mobilität. Hieraus entwickelt sich allerdings eine erhöhte Gefahr eines Cyberangriffes auf die Fahrzeugsoftware. Daraus resultiert eine Vielzahl an Rechtsfragen, falls beispielsweise externe Hacker die vollständige Kontrolle über die Fahrzeugsteuerung eines selbstfahrenden Kraftfahrzeuges erlangen konnten.

13.1 Hintergrundinformationen

Für die heutige deutsche Gesellschaft scheint die Vorstellung von selbstfahrenden Kraftfahrzeugen, die sich in dem öffentlichen Straßenverkehr etablieren konnten, noch weit in der Zukunft zu liegen. In rechtlicher Hinsicht konnte sich Deutschland allerdings als weltweiter Vorreiter des autonomen Fahrens durchsetzen. Allein durch die Anpassung des Straßenverkehrsrechtes verspricht sich Deutschland, die Vision von den ersten selbstfahrenden Kraftfahrzeugen bereits im Jahr 2022 verwirklichen zu können (vgl. Bundesministerium für Verkehr und digitale Infrastruktur 2021).

K. Maier (✉) · N. Antonczyk · R. Biskup · L. Dalir
TH Köln, Institut für Versicherungswesen, Köln, Deutschland
E-Mail: karl.maier@th-koeln.de

R. Arnold et al. (Hrsg.), *Risiko im Wandel*,
https://doi.org/10.1007/978-3-658-37071-8_13

Hierzu wurde am 29.07.2021 das Straßenverkehrsgesetz reformiert, welches den Rechtsrahmen schafft, automatisierte Fahrzeuge der vierten Stufe in festgelegten Betriebsbereichen im öffentlichen Straßenverkehr im Regelbetrieb zuzulassen (vgl. Bundesministerium für Verkehr und digitale Infrastruktur 2021). Das Inkrafttreten des Gesetzes für autonome Fahrzeuge ermöglicht insbesondere wirtschaftliche Erfolge von innovativen Geschäftsmodellen, in denen Fahrer eingespart werden können. Beispielsweise könnten im öffentlichen Personenverkehr Beförderungsbedarfe oder in der Logistik die Verteilung von Post oder Dokumenten zwischen verschiedenen Standorten durch Fahrzeuge mit autonomer Funktion abgedeckt werden (vgl. Gesetzesentwurf der Bundesregierung 2021, S. 20). Zwar wird der Einsatz dieser Fahrzeuge noch örtlich begrenzt sein und speziellen Zulassungsanforderungen unterliegen, allerdings können Forschung und Technik damit jahrelang geplante Pilotprojekte finalisieren und erstmals umsetzen (vgl. Science Media Center 2021).

Dieser technische, wissenschaftliche sowie rechtliche Fortschritt wirft unter versicherungstechnischen Gesichtspunkten noch einige Fragen auf. Insbesondere Cyberangriffe auf Kraftfahrzeuge, die sich ohne Fahrer selbst steuern können, rücken immer mehr in den Fokus. Vor allem durch unerkannte Sicherheitslücken im Fahrzeugsystem können Hacker bereits heute teilautomatisierte Kraftfahrzeuge angreifen. Auf dem Weg zum autonomen Fahren können dabei weitere Sicherheitsrisiken entstehen, die das Gefahrenpotenzial für Cyberangriffe erhöhen. Daher stellt sich die Frage, inwiefern die einzelnen Beteiligten bei einem Cyberangriff auf ein automatisiertes oder autonomes Kraftfahrzeug haften können.

Das vorliegende Kapitel beschäftigt sich zunächst mit den Grundlagen von automatisierten und autonomen Kraftfahrzeugen. Mit der Aufteilung nach den fünf Stufen der Automatisierung soll zunächst ein Einblick in die aktuelle und zukünftige technische Entwicklung gegeben werden. Im Anschluss werden dann die Folgen des automatisierten Fahrens näher betrachtet, wobei insbesondere die Modalitäten von Cyberangriffen und deren Auswirkungen auf automatisierte Kraftfahrzeuge dargestellt werden. Schließlich wird auf die sich hieraus ergebende Anschlussfrage nach der Haftung des Fahrzeughalters bzw. der Fahrzeughalterin, aber auch des Fahrers bzw. der Fahrerin dargestellt. Auf Basis der Haftung werden zum Schluss bestimmte, bereits am Markt etablierte Versicherungslösungen untersucht.

13.1.1 Vom assistierten zum autonomen Fahren

Im Jahr 2014 wurden durch die Society of Automotive Engineers International (SAE International)[1] *sechs Automatisierungsklassen* für automatisierte Fahrsysteme definiert, die im SAE-Standard J3016 erläutert werden (vgl. SAE International 2021). Die Norm **SAE**

[1] Die SAE International ist führend in der Vernetzung sowie Ausbildung von Mobilitätsexperten, um sichere Mobilitätslösungen zu ermöglichen; zu den Gründungsmitgliedern gehörten unter anderem Andrew L. Riker und Henry Ford (vgl. SAE International 2021).

J3016 beschreibt dabei die Klassifizierung und definiert die Begrifflichkeiten für straßengebundene Kraftfahrzeuge mit Systemen zum automatisierten Fahren. Die Stufen gelten für die Fahrautomatisierungsfunktionen, die in einem bestimmten Fall des Straßenbetriebs eines ausgerüsteten Fahrzeugs eingesetzt werden. Obwohl ein bestimmtes Fahrzeug mit einem Fahrautomatisierungssystem ausgestattet sein kann, welches mehrere Fahrautomatisierungsfunktionen auf verschiedenen Ebenen bereitstellen kann, wird der Grad der Fahrautomatisierung durch die aktivierten Merkmale bestimmt (vgl. SAE International 2021).

- In der ersten Stufe, dem **Level Null**, findet *keine Automatisierung* statt (vgl. Bardt 2016, S. 41). Die Steuerung der Kraftfahrzeuge erfolgt manuell durch die Fahrer während der gesamten Fahrt (vgl. DATACOM Buchverlag GmbH 2020). Die Fahrer übernehmen sowohl die Längsführung als auch die Querführung (vgl. Bundesanstalt für Straßenwesen 2018). Es erfolgt keine Aktivierung eines eingreifenden Fahrzeugsystems. Aus diesem Grund wird das Level 0 auch „*Driver only*“ genannt.
- Das **erste Level** beschreibt das assistierte Fahren eines Kraftfahrzeugs mit *Fahrassistenzsystemen* (vgl. Bardt 2016, S. 41). Dabei entlasten diese Systeme die Fahrer bei bestimmten Fahraufgaben. Zu diesen unterstützenden Maßnahmen gehören unter anderem der Tempomat, der automatische Abstandsregeltempomat sowie der automatische Spurhalteassistent (vgl. ADAC 2021). Der Abstandsregeltempomat unterstützt die Fahrer dabei, den Sicherheitsabstand zum vorausfahrenden Fahrzeug durch Bremsen oder Beschleunigen einzuhalten. Die aktuell verbreiteten Abstandsregeltempomaten sind außerdem dazu in der Lage, selbsttätig abzubremsen, bis die Fahrzeuge stehen, und nach Freigabe durch die jeweiligen Fahrer automatisch wieder anzufahren. Im Jahr 2018 waren in Deutschland 71 Prozent der erworbenen Neuwagen mit einem Tempomat ausgestattet (vgl. Statista 2021). Nichtdestotrotz müssen die Fahrer die Kraftfahrzeuge ununterbrochen unter Kontrolle haben und den Verkehr ständig im Blick behalten. Durch den automatischen Spurhalteassistent erhalten die Fahrer zusätzliche Unterstützung bei der Einhaltung der Fahrspur (vgl. ADAC 2021).
- Im **zweiten Level** geht es um das *teilautomatisierte Fahren* (vgl. Bardt 2016, S. 41). Dabei haben die Fahrer weiterhin die Kontrolle über die Kraftfahrzeuge und müssen das System nach wie vor dauerhaft überwachen (vgl. Delhaes 2017). Beim teilautomatisierten Fahren können Kraftfahrzeuge einige Aufgaben zeitweilig selbst ausführen. Dies geschieht ohne Eingriff der Fahrer (vgl. ADAC 2021). Es ist möglich, dass die Kraftfahrzeuge auf der Autobahn die Spur halten und gleichzeitig bremsen oder beschleunigen. Zusätzlich können die Kraftfahrzeuge automatisch einparken, sodass die Fahrer nicht mehr zum Lenkrad greifen müssen. Allerdings müssen die Fahrer die Assistenzsysteme ständig überwachen und eingriffsbereit sein (vgl. ADAC 2021).
- Das **dritte Level** beschreibt das *bedingt automatisierte Fahren*, bei dem sich die Fahrer vorübergehend von der Fahraufgabe und dem Verkehr abwenden dürfen (vgl. Bardt 2016, S. 41). Lediglich auf Anforderung des Systems müssen die Fahrer eingreifen (vgl. ADAC 2021). Für einen begrenzten Zeitraum und unter geeigneten, vom Herstel-

ler vorgegebenen Bedingungen, werden bestimmte Fahraufgaben vom Kraftfahrzeug selbst übernommen. Die Fahrer werden dementsprechend entlastet. Je nach Verkehrssituation sind die Kraftfahrzeuge in der Lage zu überholen, zu bremsen oder zu beschleunigen. Sollte das System ein Problem erkennen und eine Fehlermeldung anzeigen, müssen die Fahrer umgehend eingreifen und das Steuer übernehmen (vgl. ADAC 2021).

- In **Level vier** wird das *hochautomatisierte Fahren* beschrieben (vgl. Bardt 2016, S. 41). Das hochautomatisierte Fahren stellt die Vorstufe des autonomen Fahrens dar, in der das Fahrzeug den überwiegenden Teil der Fahrt eigenständig absolviert. In dieser Stufe werden Fahrer verlangt, die jedoch zu Passagieren werden und nur im Bedarfsfall handeln müssen. Dies hat zur Folge, dass die komplette Fahrzeugführung auf die Kraftfahrzeuge übertragen werden. Diese sind in der Lage, bestimmte Anwendungsfälle wie zum Beispiel Autobahnfahrten oder das Fahren im Parkhaus selbstständig durchzuführen (vgl. ADAC 2021). Durch entwickelte Systeme werden Gefahrensituationen frühzeitig erkannt. Somit ist es möglich, dass ein Kraftahrzeug auch bei hoher Geschwindigkeit ohne Eingriff der jeweiligen Fahrer fährt. Die Fahrzeuge sind in der Lage, Systemgrenzen zu erkennen, um die Fahrer zur Übernahme mit ausreichender Zeitreserve zu informieren. Bestimmte Handlungen wie zum Beispiel das Blinken oder das Überholen werden selbstständig vom Kraftfahrzeug vollzogen. Bei Beendigung einer Fahrt parkt sich das Kraftfahrzeug eigenständig ein (vgl. ADAC 2021).
- Das vollautomatisierte Fahren, auch *autonomes Fahren* genannt, wird im **fünften** und **letzten Level** definiert (vgl. Bardt 2016, S. 41). Beim autonomen Fahren sind Fahrten ohne Insassen möglich und es gibt nur noch Passagiere ohne Fahraufgabe. Das Fahrzeugsystem ist in der Lage, sämtliche Anwendungsfälle eigenständig durchzuführen. Dabei werden sämtliche Geschwindigkeitsbereiche und Umfeldbedingungen berücksichtigt (vgl. Delhaes 2017). Das Fahrzeug wird komplett vom System geführt und erledigt alle erforderlichen Handlungen selbstständig. In diesem Szenario werden weder eine Fahrtüchtigkeit noch eine Fahrerlaubnis benötigt, lediglich eine Zieleingabe muss durch die Passagiere getätigt werden (vgl. Roshan 2021, Rn. 137; vgl. ADAC 2021).

13.1.2 Cyberrisiken und Car Hacking

Ein **Cyberangriff** beschreibt eine gezielte Einwirkung von außen auf Informations- und Sicherheitsinfrastrukturen von Computersystemen im Cyberraum (vgl. Grützner und Jakob 2015). Diese Eingriffe werden von Hackern ausgeübt. Dabei nutzen die Hacker fortlaufend neue Methoden, um sich Zugänge zu verschiedenen Computersystemen oder Netzwerken schaffen zu können (vgl. Mehrbrey und Schreibauer 2016, Rn. 75).

Im Bereich der Informatik wird der Begriff des Hackers zunächst nicht mit kriminellen Aktivitäten in Verbindung gebracht (vgl. Siller 2018). Sobald Hacker allerdings unerkannte Lücken in fremden Systemen nutzen, um sich beispielsweise selbst zu bereichern, sensible Daten zu entwenden oder andere Schäden anzurichten, wird der unerlaubte Eingriff als Straftat gewertet (vgl. Siller 2018; vgl. § 202c StGB). Mithilfe der umfassenden

Anonymität des Internets erhalten solche Hacker die Möglichkeit, ihre kriminellen Aktivitäten unentdeckt durchführen zu können (vgl. Mehrbrey und Schreibauer 2016, Rn. 75).

In Bezug auf die zunehmende Automatisierung von Kraftfahrzeugen entsteht dadurch auch eine Gefahr von Cyberangriffen auf solche Kraftfahrzeuge, das sogenannte **Car Hacking**. Externe Hacker könnten sich einen Zugang zu den Fahrzeugsystemen eines automatisierten oder autonomen Kraftfahrzeuges verschaffen. Die technischen Assistenzsysteme können dann nicht mehr ordnungsgemäß funktionieren, sodass einzelne Fahrprozesse beim automatisierten Fahren verändert ablaufen. Falls Hacker in das Fahrzeugsystem eines autonom fahrenden Kraftfahrzeuges eingreifen, kann die vollständige Kontrolle des Kraftfahrzeuges übernommen werden.

Die ersten Cyberangriffe auf automatisierte Kraftfahrzeuge fanden im Jahr 2015 statt, bei denen Forscher durch Car Hacking auf einen US-amerikanischen Geländewagen zugreifen konnten (vgl. Stender-Vorwachs und Oppermann 2020, S. 217, Rn. 47). Im Rahmen von wissenschaftlichen Versuchen konnten die Forscher eine Schwachstelle im Infotainment-System des Jeep Cherokee identifizieren und erfolgreich die Kontrolle des Fahrzeugsystems übernehmen, während das Kraftfahrzeug selbstständig gefahren ist (vgl. AXA o. J.). Dadurch hatten die Hacker unter anderem die Möglichkeit, die Bremsen, die Türverriegelung und die Scheibenwischer zu bedienen. Außerdem konnten sie die Lenkung steuern, sobald sich das Kraftfahrzeug im Rückwärtsgang befand (vgl. Stender-Vorwachs und Oppermann 2020, S. 217, Rn. 47).

Daneben wurden ebenfalls im Jahr 2015 Sicherheitslücken innerhalb des Connected Drive-Systems des Automobilherstellers BMW gefunden. Diese Sicherheitslücken konnten das Fahrzeugsystem von BMW über das Mobilfunknetz angreifbar machen. Zur Behebung des Fehlers wurde ein Software-Update an über zwei Millionen Fahrzeugen durchgeführt (vgl. Maier 2015).

Auch das Smartphone bietet ein potenzielles Risiko für Cyberangriffe auf vernetzte Kraftfahrzeuge an. Durch Fahrzeugsysteme, die Öffnen und Schließen des Fahrzeugs per Smartphone ermöglichen, konnte ein externer Hacker die Kommunikation zwischen einem Smartphone und dem Kraftfahrzeug abfangen, sodass er die Standortdaten des Kraftfahrzeuges empfangen und das System aus der Ferne bedienen konnte. Solche Szenarien beschränken sich nicht nur auf ein bestimmtes Kraftfahrzeug, sondern können ganze Modellreihen und Automarken übergreifend treffen (vgl. Maier 2015).

In Hinblick auf mögliche Cyberangriffe sind auch die Telematik-Systeme von Versicherern problematisch, da dort lückenhafte Zugangspunkte für Hacker vorzufinden waren, die relevante Fahrzeugfunktionen angreifbar machen können (vgl. Maier 2015). Grundsätzlich werden solche Sicherheitslücken durch Kontrollen und Systemupdates erkannt und vermieden, aber derzeit noch unentdeckte Sicherheitslücken können eine lebensbedrohliche Gefahr für die Fahrer und Passagiere eines automatisierten Kraftfahrzeuges darstellen.

13.2 Haftungsfragen bei Cyberangriffen

Bei Cyberangriffen können sich Haftungsfragen sowohl beim *Fahrzeughalter* bzw. bei der *Fahrzeughalterin* als auch beim *Fahrer* bzw. bei der *Fahrerin* eines Fahrzeugs ergeben.[2]

13.2.1 Halterhaftung bei Cyberangriffen auf ein Kraftfahrzeug

Gemäß Straßenverkehrsordnung (§ 7 Abs. 1 StVG) ist die Haftung des Halters eines Kraftfahrzeuges wie folgt beschrieben:

> „*Wird bei dem Betrieb eines Kraftfahrzeugs ein Mensch getötet, der Körper oder die Gesundheit eines Menschen verletzt oder eine Sache beschädigt, so ist der Halter verpflichtet, dem Verletzten den daraus entstehenden Schaden zu ersetzen*".

Eine Rechtsgutverletzung nach § 7 Abs. 1 StVG liegt vor, wenn Leib, Leben, Gesundheit oder Eigentum bei dem Betrieb eines Kraftfahrzeugs verletzt werden. Die Rechtsgutverletzung muss beim Betrieb des Kraftfahrzeugs erfolgen. Das Kraftfahrzeug ist im Betrieb, wenn sich das Kraftfahrzeug im öffentlichen Verkehrsbereich fortbewegt. § 7 Abs. 1 findet auch Anwendung, wenn das Kraftfahrzeug in verkehrsbeeinflussender Weise ruht. Zusätzlich muss sich die Betriebsgefahr des Kraftfahrzeugs realisieren. Durch die Nutzung eines Kraftfahrzeugs wird eine Gefahrenquelle eröffnet, die zur Haftung nach § 7 Abs. 1 StVG führt. Ein Schaden ist demgemäß bereits dann bei dem Betrieb eines Kraftfahrzeugs entstanden, wenn sich von einem Kraftfahrzeug ausgehende Gefahren ausgewirkt haben.

Ein **Halter** ist diejenige Person, die das Kraftfahrzeug in eigenem Namen sowie für eigene Rechnung in Gebrauch hat und darüber die Verfügungsgewalt ausübt. Dies hat zur Folge, dass ein Halter nicht zugleich auch Eigentümer des Kraftfahrzeugs sein muss (vgl. Langheid und Wandt 2017, Rn. 90).

Gemäß § 7 Abs. 2 StVG greift die Gefährdungshaftung nicht, wenn höhere Gewalt im Spiel ist; gemäß Abs. 3 greift die Gefährdungshaftung ebenfalls nicht, wenn der Halter des Fahrzeugs nicht in Kenntnis darüber gesetzt ist und auch nicht möchte, dass jemand anderes das Fahrzeug nutzt. Dies sind die einzigen Möglichkeiten für den Halter, nicht für entstandene Schäden resultierend aus dem Betrieb des Fahrzeugs aufkommen zu müssen. Im zweiten Fall ist der tatsächliche Benutzer dann zum Schadensersatz verpflichtet.

Die **höhere Gewalt** wird in der Rechtsprechung als ein betriebsfremdes von außen durch elementare Naturgewalten oder durch Handlungen Dritter herbeigeführtes Ereignis definiert, das nach menschlicher Einsicht und Erfahrung unvorhersehbar ist und mit wirtschaftlich erträglichen Mitteln auch durch eine äußerste Sorgfalt nicht verhütet oder

[2] Zur Vermeidung von Missverständnissen in Bezug auf die üblichen Fachtermini werden in den nachfolgenden Ausführungen relevante Begriffe im generischen Maskulinum Singular verwendet, ohne dass dies die persönliche Meinung der Autorinnen und Autoren zu diesem Thema darstellt.

unschädlich gemacht werden kann und aufgrund seiner niedrigen Eintrittswahrscheinlichkeit auch nicht in Kauf zu nehmen ist (vgl. König 2013, S. 146). Wenn ein Unfall also aufgrund eines Fehlers in der Beschaffenheit des Fahrzeugs oder wegen des Versagens der Technik entstanden ist, greift die Möglichkeit des Halters nicht, sich über die höhere Gewalt zu entlasten (vgl. König 2013, S. 146). Die höhere Gewalt diente der Ablösung des Ausschlussgrunds des unabwendbaren Ereignisses der alten Fassung des StVG. Da bspw. Schadensersatzansprüche bei Unfällen mit Kindern, älteren Menschen und sonstigen hilfsbedürftigen Personen nicht als höhere Gewalt angesehen werden, bleibt in diesen Fällen zugunsten dieser Personen ein Anspruch gegen den Halter des betreffenden Fahrzeugs bestehen (vgl. Burmann, StVG § 7 Haftung des Halters, Schwarzfahrt, Rn. 17–22).

Fraglich bleibt, ob ein Ausschluss der Halterhaftung bei Cyberangriffen nach § 7 Abs. 2 StVG oder § 7 Abs. 3 StVG möglich wäre. Zunächst ist zu prüfen, ob ein Cyberangriff dem Begriff der höheren Gewalt gemäß § 7 Abs. 2 StVG zuzuordnen ist.

Der Begriff höhere Gewalt setzt drei Merkmale voraus, die allesamt erfüllt sein müssen, damit die Entlastung eines Halters möglich ist. Es muss sich um ein

- von *außen einwirkendes*,
- *außergewöhnliches* und
- *nicht abwendbares* Ereignis handeln (vgl. Burmann et al. 2020, Haftung des Halters, Schwarzfahrt, Rn. 17–22).

Ein von *außen einwirkendes* Ereignis liegt vor, wenn das Ereignis in einem nicht mit dem Fahrzeugbetrieb oder seinen Einrichtungen verbundenen Zusammenhang steht (vgl. Burmann et al. 2020, Haftung des Halters, Schwarzfahrt, Rn. 17–22). Dies können Naturereignisse sein, die keine plötzlichen Witterungsänderungen und -einflüsse sind, aber auch Attentate oder Sabotageakte (vgl. Grüneberg 2021, Rn. 39–43).

Außergewöhnlich ist ein Ereignis nur dann, wenn es selten vorkommt bzw. einer Ausnahme entspricht. Dies ist nicht der Fall, wenn man damit rechnen kann wie bspw. mit dem Fehlverhalten anderer Verkehrsteilnehmer (vgl. Burmann et al. 2020, Haftung des Halters, Schwarzfahrt Rn. 17–22).

Als letztes muss das Ereignis für den Betroffenen *unabwendbar* gewesen sein. Unabwendbarkeit ist dann anzuerkennen, wenn nach menschlicher Einsicht und Erfahrung das Ereignis unvorhersehbar und zusätzlich nicht mit einer äußersten Sorgfalt sowie wirtschaftlich erträglichen Mitteln hätte verhindert werden können (vgl. BGH-Urteil Nr. 83, § 22 Abs. 1 und 2 WHG, 30.05.1974). In Abgrenzung zur erforderlichen Sorgfalt nach § 276 Abs. 2 BGB liegt äußerste Sorgfalt dann vor, wenn der Betroffene die äußerste, vernünftigerweise zu erwartende, Sorgfalt anwendet, um das Ereignis abzuwenden und dementsprechend auch die darauffolgenden Schäden zu vermeiden (vgl. Graf von Westphalen 2020, S. 275). Es fordert ein höheres Maß an Anstrengungen zur Abwehr und Vorsorge eines Ereignisses der höheren Gewalt als im Rahmen von einfacher Fahrlässigkeit bei der erforderlichen Sorgfalt geboten ist. In diesen Fällen ist die äußerste Sorgfalt

auf die erforderliche Sorgfalt gemäß vorliegenden Umständen begrenzt (vgl. Graf von Westphalen 2020, S. 275).

Zu prüfen ist, ob diese drei Voraussetzungen bei einem Cyberangriff auf ein Fahrzeug vorliegen.

Ein Cyberangriff kommt von außen, da die Einwirkung eines Hackers in einem nicht mit dem Fahrzeugbetrieb oder den Einrichtungen verbundenen Zusammenhang steht. Das bedeutet, der Hackerangriff ist nicht auf innere Betriebsvorgänge zurückzuführen. Zwar wird bei der Übernahme der Fahrzeugfunktionen ein Teil der Vorgänge tangiert, die dazu schadenbedingte Tätigkeit des Hackers wird aber von außerhalb vorgenommen. Darüber hinaus liegt im Hacker eine betriebsfremde Person vor, die keine berechtigten Beziehungen zu dem Fahrzeug hat und in erster Linie auch ohne Willen und ggf. auch ohne Wissen des Halters das Fahrzeug nutzt (vgl. Lammers 2006, S. 163).

Das Ereignis muss derart ungewöhnlich sein, dass es schon einem elementaren Ereignis gleicht (vgl. Pütz und Maier 2019). Allerdings kann man aus der Definition der höheren Gewalt entnehmen, dass auch durch Handlungen dritter Personen herbeigeführte Ereignisse als außergewöhnlich betrachtet werden können. Die tatsächliche Intention des Hackers lässt sich nur vermuten, aber sie kann dieser eines Attentäters oder Sabotageakteurs nahekommen. Aus diesen Gründen ist auch das zweite Merkmal gegeben.

Als letztes ist zu prüfen, ob das Ereignis und die darauf zurückzuverfolgenden Schäden selbst durch äußerste Sorgfalt nicht hätten verhindert werden können. An diesem Merkmal wird die Entlastungsmöglichkeit der höheren Gewalt dann scheitern, wenn der Fahrer Kenntnis über den Hackerangriff erlangt und die Fahrfunktionen dann wieder übernehmen kann (vgl. Pütz und Maier 2019). Selbst bei Fahrzeugen der vierten Stufe des automatisierten Fahrens ist ein Eingriff durch den Fahrer möglich und könnte ggf. sogar notwendig sein, wenn das Fahrzeug den Fahrer dazu auffordert. Daher ist ein Hackerangriff zumindest bei automatisierten Fahrzeugen der *ersten* bis zur *vierten Stufe* abwendbar, sodass kein Fall höherer Gewalt vorliegt und folglich weiterhin eine Haftung des Halters nach § 7 StVG zu bejahen ist. Für den geschädigten Dritten bleibt dann der Direktanspruch gegen den Kfz-Haftpflichtversicherer gemäß § 115 Abs. 1 S. 1 Nr. 1 VVG i. V. m. § 1 PflVG des versicherten gehackten Fahrzeugs bestehen (vgl. Koch 2018, S. 903).

Allerdings betont der BGH im Zusammenhang mit der Haftung nach §§ 1 und 2 HaftPflG, dass bei dem Vorliegen von höherer Gewalt Risiken nicht betrachtet werden sollten, die nicht mehr der eigentlichen Gefahr, die in Verkehr gebracht worden ist, sondern ausschließlich einem Drittereignis zuzurechnen sind (vgl. Koch 2018, S. 905). Sinngemäß auf Kraftfahrzeuge übertragen handelt es sich dabei um Risiken, die mit dem Betrieb des Fahrzeugs nichts mehr zu tun haben und ausschließlich einem Drittereignis zuzurechnen sind (vgl. Koch 2018, S. 905). Wenn das Fahrzeug nun also gehackt wird und dadurch Fehlfunktionen aufweist, die auf Störungen des Datenaustauschs zurückzuführen sind (welcher in Echtzeit im Regelfall verarbeitet werden muss) dürfte sowohl für Halter als auch Fahrer die höhere Gewalt anzusehen sein und folglich beide von ihrer Haftung entlasten (vgl. Koch 2018, S. 905).

Geht man von dieser Sichtweise aus, bleibt eine Haftung gem. § 7 Abs. 2 StVG aus und der Halter bzw. Kfz-Haftpflichtversicherer gem. § 116 Abs. 1 S. 1 VVG ist dem Geschädigten gegenüber zu keiner Leistung mehr verpflichtet. Dies würde die Position des Geschädigten deutlich verschlechtern, entfiele doch der Direktanspruch gegenüber dem Kfz-Haftpflichtversicherer des Halters. Dennoch hat der Geschädigte dann die Möglichkeit, sich die Daten der Black Box des Fahrzeugs übermitteln und auswerten zu lassen, um seine Schadensersatzansprüche beim Hersteller geltend zu machen (vgl. Koch 2018, S. 906). Für Störungen, die auf einer Netzüberlastung o.Ä. beruhen, käme nur eine Haftung des Netzbetreibers und nicht des Kfz-Herstellers in Betracht (vgl. Koch 2018, S. 906). Kommt bei der Auswertung heraus, dass ein Fehler des Autopiloten vorliegt, muss der Kfz-Hersteller beweisen, keine seiner Pflichten – bei Hackerangriffen womöglich die Produktbeobachtungspflicht – schuldhaft verletzt zu haben (vgl. Koch 2018, S. 906). Folglich entsteht dem Geschädigten nicht nur ein höherer Aufwand, sondern bietet bspw. die freiwillig abgeschlossene Betriebshaftpflichtversicherung des Herstellers dem Geschädigten auch weitaus weniger Schutz als die Kfz-Haftpflichtversicherung des Halters eines Fahrzeugs (vgl. Koch 2018, S. 906). Wenn also bei Cyberangriffen auf ein Kfz das Vorliegen von höherer Gewalt bejaht wird, wird der Geschädigte es schwieriger haben, seine Ansprüche überhaupt geltend zu machen. Darüber hinaus wird er auch bei der Befriedigung dieser Ansprüche – ob durch Hersteller, Netzbetreiber, IT-Dienstleister o.Ä. – deutlich schlechter gestellt als bei Geltendmachung bei einem Kfz-Haftpflichtversicherer. Ob dies nun tatsächlich den Zweck der EU-Richtlinie zum Opferschutz erfüllt, ist fraglich bzw. dürfte zu verneinen sein.

Nur eine engere Auslegung des Begriffs der höheren Gewalt, die Einführung einer reinen Erfolgshaftung beim Gebrauch des Kraftfahrzeugs im Autopilot-Modus oder eine Entkopplung der Haftung des Kfz-Haftpflichtversicherers von der Haftung der anderen im Prozess beteiligten Unternehmen könnten dann dem Geschädigten tatsächlich helfen – vor allem bei gänzlich autonomen Fahrzeugen (vgl. Koch 2018, S. 906). Für eine enge Auslegung des Begriffs der höheren Gewalt spricht, dass nur so der mit § 7 StVG erstrebte Opferschutz gewährleistet ist.

Nach § 7 Abs. 3 StVG entfällt die Ersatzpflicht des Fahrzeughalters bei einer Benutzung des Kraftfahrzeuges ohne Wissen und Willen des Halters. Die Haftung des Fahrzeughalters kann dennoch eintreten, wenn die Benutzung des Kraftfahrzeuges durch sein Verschulden ermöglicht worden ist, wenn der Benutzer vom Fahrzeughalter für den Betrieb des Kraftfahrzeugs angestellt ist oder wenn ihm das Kraftfahrzeug vom Halter überlassen worden ist (vgl. § 7 Abs. 3 StVG, zum Begriff des Verschuldens im Allgemeinen siehe Schmidt 2021).

Im Jahr 1956 wurde der Begriff des Benutzers im Sinn des § 7 Abs. 3 StVG letztmalig durch den BGH konkretisiert (vgl. BGH NJW 1957, 500). Demnach gilt jemand als Benutzer, wenn dieser sich das Kfz unter Verwendung der motorischen Kraft als Fortbewegungsmittel dienstbar macht und dadurch die Verfügungsgewalt über das Fahrzeug ausübt, wie sie sonst dem Halter zusteht (vgl. BGH NJW 1957, 500). Für den Benutzer entsteht somit eine halterähnliche Verfügungsmacht (vgl. Burmann et al. 2020, Rn. 23). Dabei wird klar zwischen dem eigentlichen unbefugten Benutzer des Fahrzeuges und den Fahrgästen

abgegrenzt. Nicht alle Fahrgäste, die das Fahrzeug als Fortbewegungsmittel nutzen, sind Benutzer des Fahrzeuges (vgl. BGH NJW 1957, 500, Rn. 501). Vielmehr kann ein Fahrgast erst als Benutzer bezeichnet werden, wenn eine Beziehung zu dem Fahrzeug besteht, die der des Halters verwandt ist (vgl. BGH NJW 1957, 500, Rn. 501). In dem Sinne kann auch ein Mitfahrender zur Haftung gezogen werden, wenn er den Fahrer durch sein Verhalten auffordert, die Schwarzfahrt durchzuführen (vgl. BGH NJW 1957, 500, Rn. 501).

Fraglich bleibt, ob ein Hacker die genannten Voraussetzungen eines unbefugten Benutzers erfüllt. Falls ein Hacker als unbefugter Benutzer betrachtet werden kann, entfällt grundsätzlich die Gefährdungshaftung des Fahrzeughalters aus § 7 Abs. 1 StVG. Diese Ersatzpflicht wird auf den Hacker übertragen.

Bei einem Cyberangriff kann der Hacker die vollständige Kontrolle der Fahrzeugsystemsteuerung erlangen. Es befähigt ihn, die Schwarzfahrt veranlassen und steuern zu können (vgl. Pütz und Maier 2019, Rn. 446). Die Kontrolle allein ist jedoch nicht aussagekräftig, um den Hacker als unbefugten Benutzer bezeichnen zu können. Entscheidend ist die Frage, mit welchem Zweck der Hacker sich die Verfügungsgewalt aneignet (vgl. Pütz und Maier 2019, Rn. 446).

Grundsätzlich hat der Hacker kein Interesse an dem Kraftfahrzeug. Es ist insbesondere nicht von Bedeutung, inwiefern der Hacker das Fahrzeug als Transportmittel nutzen kann. Die vollständige Steuerung der Schwarzfahrt tritt somit in den Hintergrund. Vorrangig möchte er dem ursprünglichen Nutzer die eigentliche Kontrolle des Fahrzeuges entziehen, indem er die Fahrzeugsystemsteuerung angreift und in ihrer Funktionsweise stört. Die Handlungsabsicht des Hackers kann somit nicht der Absicht eines unbefugten Benutzers des Fahrzeuges zugeordnet werden; der Hacker will das Fahrzeug nicht „benutzen“, er will nicht von A nach B gelangen. Aufgrund der fehlenden Benutzereigenschaft bleibt die Gefährdungshaftung des Halters bestehen und die grundlegende Funktion des Verkehrsopferschutzes aus § 7 StVG erhalten (vgl. Pütz und Maier 2019, Rn. 446).

Falls der Hacker das Fahrzeug tatsächlich als Transportmittel benutzt und folglich als unbefugter Benutzer gilt, dann übernimmt dieser vollumfänglich die Haftung des Halters. Hierbei sind die Verkehrsopfer dazu angehalten, Ansprüche bei einer etwaigen Haftpflichtversicherung des Hackers geltend zu machen. Allerdings besteht zunächst die Schwierigkeit, den Hacker ausfindig zu machen. Eine weitere Problematik bildet der fehlende Versicherungsschutz aufgrund des Vorsatzausschlusses gemäß § 103 VVG. Würde daher die Haftung des Halters nach § 7 Abs. 3 StVG entfallen, würde die grundlegende Verkehrsopferschutzfunktion des § 7 StVG ins Leere laufen. Mit Berücksichtigung der Verkehrsopfer wäre die Betrachtung des Hackers als unbefugter Benutzer somit nicht vorteilhaft (vgl. Pütz und Maier 2019, Rn. 446). Sie ist aber aus Rechtsgründen auch nicht geboten; der Hacker will das Kfz stören und nicht benutzen, sodass § 7 Abs. 3 StVG nicht zu Anwendung kommt.

13.2.2 Fahrerhaftung bei Cyberangriffen auf ein Kraftfahrzeug

Falls der Fahrzeugführer eines Kraftfahrzeuges eine Pflichtverletzung begeht und diese zu vertreten hat, kann er für Schäden dritter Personen gemäß § 18 Abs. 1 StVG und gemäß § 823 Abs. 1 BGB haften. Hierbei gilt § 18 StVG als Sonderregelung, die im Vergleich zum Deliktsrecht weniger strenge Voraussetzungen aufweist (vgl. Universität Greifswald 2018).

In § 18 StVG wird die Ersatzpflicht des Fahrzeugführers erläutert. Nach Abs. 1 ist der Führer des Kraftfahrzeugs in den Fällen des § 7 Abs. 1 StVG zum Ersatz des Schadens nach den Vorschriften der §§ 8 bis 15 StVG verpflichtet. Die Ersatzpflicht ist ausgeschlossen, wenn der Schaden nicht durch ein Verschulden des Führers verursacht ist. Ist in den Fällen des § 17 StVG auch der Kraftfahrzeugführer zum Ersatz des Schadens verpflichtet, so sind auf diese Verpflichtung (in seinem Verhältnis zu den Haltern und Führern der anderen beteiligten Kraftfahrzeuge) die Vorschriften des § 17 StVG entsprechend anzuwenden.

Eine Rechtsgutverletzung liegt analog zu § 7 StVG vor, wenn die Rechtsgüter *Leib*, *Leben*, *Gesundheit* oder *Eigentum* geschädigt werden. Die entstandene Rechtsgutverletzung muss sich aus dem Betrieb des Kraftfahrzeugs ergeben. Da der Betrieb eines Kraftfahrzeugs bei der Haftung nach § 7 StVG untersucht wurde, wird hier auf eine nähere Erläuterung verzichtet. Der Bundesgerichtshof stellt klar, dass der Fahrzeugführer derjenige ist, der selbst alle oder wenigstens einen Teil der wesentlichen Einrichtungen des Fahrzeugs bedient, die für seine Fortbewegung bestimmt sind (vgl. BGH, Urteil vom 27.07.1962 – 4 StR 215/62). Nach § 1a Abs. 4 StVG ist der Fahrzeugführer derjenige, der eine hoch- oder vollautomatisierte Fahrfunktion aktiviert und zur Fahrzeugsteuerung verwendet, auch wenn er im Rahmen der bestimmungsgemäßen Verwendung dieser Funktion das Fahrzeug nicht eigenhändig steuert.

Die Haftung nach StVG stellt eine verschuldensunabhängige Haftung dar. Dies hat zur Folge, dass das Verschulden des Fahrzeugführers vermutet wird. Nach § 18 Abs. 2 StVG findet die Vorschrift des § 16 StVG entsprechende Anwendung. Die Ausschlüsse der Fahrerhaftung nach § 18 StVG werden in §§ 7 und 8 StVG geregelt. Es liegen dieselben Ausschlüsse wie bei der Halterhaftung nach § 7 Abs. 1 StVG vor. Die für die Anwendbarkeit des § 18 StVG ergebenen Rechtsfolgen resultieren genau wie bei der Halterhaftung nach § 7 StVG aus den §§ 249 ff. BGB sowie §§ 9–13 StVG. Die Höchstbeträge, welche sich aus § 12 StVG ergeben, finden bei der Fahrerhaftung ebenfalls Anwendung.

Zur Klärung der Haftung des Fahrers nach § 18 StVG muss untersucht werden, inwieweit die Fahrerhaftung bestehen bleibt, wenn den Fahrer mit steigendem Automatisierungsgrad des Kraftfahrzeugs lediglich reduzierte Sorgfaltspflichten treffen. Trotz des Einsatzes von (teil-)automatisierten Fahrsystemen bleibt der menschliche Fahrer weiterhin Fahrzeugführer im Sinne von § 18 Abs. 2 StVG. Nach § 1b Abs. 1 und Abs. 2 StVG muss der Fahrer wahrnehmungsbereit bleiben, um jederzeit die Steuerung des Kraftfahrzeugs unverzüglich wieder übernehmen zu können. Ein Verschulden des Fahrers kann zunehmend in Frage gestellt werden, wenn der menschliche Fahrer lediglich zu einer

reduzierten Sorgfaltspflicht nach § 1b Abs. 1 StVG verpflichtet ist, die sich in der Tatsache begründet, dass sich das Kraftfahrzeug teils oder sogar vollständig selbst steuert. Die Voraussetzungen für eine verschuldensunabhängige Fahrerhaftung nach § 18 Abs. 1 StVG können daher vor allem bei dem tatsächlichen Einsatz von hoch- oder vollautomatisierter Fahrfunktionen nicht mehr erfüllt sein.

Daneben könnten die Verkehrsopfer einen Schadensersatzanspruch gegen den tatsächlichen Fahrer aus § 823 Abs. 1 BGB geltend machen. Dabei gilt der Fahrer eines automatisierten Kraftfahrzeuges gemäß § 1a Abs. 4 StVG als Fahrzeugführer. Die Haftung setzt voraus, dass der Fahrer die einzelnen Verkehrsopfer schuldhaft und rechtswidrig in einem nach § 823 Abs. 1 BGB geschützten Rechtsgut verletzt hat. Folglich ist es entscheidend, ob der Fahrer für einen durch den Cyberangriff verursachten Schaden verantwortlich gemacht werden kann. Hierzu muss zunächst die Verletzungshandlung berücksichtigt werden.

Für die Verletzungshandlung ist es bedeutsam, ob das Verhalten des Fahrers zu einer Gefahrerhöhung geführt hat. Die Näherung an eine Gefahr entspricht dabei einem aktiven Tun, während eine fehlende Gefahrabwendung einer Unterlassung entspricht. Beruht die Rechtsgutverletzung auf einem Unterlassen, dann muss bereits vorher eine Rechtspflicht zum Handeln bestanden haben (vgl. Stender-Vorwachs und Oppermann 2020, S. 165, Rn. 111).

Als Rechtspflichten werden hierbei die gleichen Sorgfaltsanforderungen an den Fahrer erwartet, die in § 18 Abs. 1 StVG und insbesondere in § 1b StVG berücksichtigt werden. Nach § 1b StVG ist dies somit der Fall, wenn der Fahrer entweder seine Verkehrspflicht der Aufrechterhaltung einer kontinuierlichen Wahrnehmungsbereitschaft verletzt hat oder die Fahrzeugsteuerung nicht unverzüglich übernimmt, sobald der störende Eingriff in das Fahrzeugsteuerungssystem für ihn erkennbar ist oder ihm angezeigt wird.

Bereits bei einer fahrlässigen Verletzung seiner Sorgfaltspflichten hat der Fahrer seine Handlung gemäß § 276 Abs. 2 BGB zu vertreten (vgl. Stender-Vorwachs und Oppermann 2020, S. 166, Rn. 119). Dies trifft auch zu, wenn ein Cyberangriff ursächlich für die erkannten Komplikationen ist und die darauffolgende Verletzungshandlung des Fahrers auf einem Augenblickversagen beruht. Allein durch das Fahren mit einem automatisierten Kraftfahrzeug schafft der Fahrer eine Gefahrenquelle für andere, für die er verantwortlich ist. Allerdings kann ihm kein Verschulden angerechnet werden, falls der Fahrer seine Pflichten gemäß § 1b StVG nicht fahrlässig verletzt hat (vgl. Pütz und Maier 2019, Rn. 446).

Bei Kraftfahrzeugen mit autonomer Fahrfunktion ist eine Haftung des Fahrers als Passagier nach § 823 Abs. 1 BGB demnach ausgeschlossen. Er kann für keine typischen Verletzungshandlungen eines Fahrers verantwortlich gemacht werden, da er während der gesamten Fahrt keine Kontrolle über das Steuerungssystem besitzt und weiterhin keine Möglichkeit für ihn entstehen kann, die Fahrzeugsteuerung manuell zu übernehmen (vgl. Hey 2019, S. 29).

13.3 Etablierte Versicherungslösungen

Wie auch die Nachfrage nach Cyber-Versicherungen für Unternehmen in den nächsten Jahren vermutlich deutlich steigen wird (vgl. Munich Re 2021; vgl. auch Kap. 11 in diesem Band), so wird sie auch wahrscheinlich nach Versicherungsschutz bei Cyberangriffen auf Kraftfahrzeuge zunehmen. Dies steht im engen Zusammenhang mit der steigenden Anzahl an automatisierten Fahrzeugen, die eine potenziell vergrößerte Angriffsfläche für Hacker bietet.

Dem Unternehmen „Upstream Security" aus Israel zufolge, das auf dem Markt als erstes eine Cloud-basierte Cybersicherheitslösung zum Schutz automatisierter Fahrzeuge vor Cyberbedrohungen sowie Cybermissbrauch entwickelte, sind von 2010 bis 2019 bei 367 öffentlich gemeldeten Cyberangriffen auf Kraftfahrzeuge 57 Prozent von kriminellen Hackern durchgeführt worden (vgl. Upstream Security Ltd. 2020, S. 3, 11). Nur 38 Prozent dienten der Warnfunktion für entdeckte Sicherheitslücken durch sogenannte *White-Hat-Hacker*, die im Gegensatz zu den unruhestiftenden *Black-Hat-Hackern* das Ziel verfolgen, Unternehmen und Verbraucher vor kriminellen Hackerangriffen zu warnen (vgl. Upstream Security Ltd. 2020, S. 11).

Im Jahr 2020 sind insgesamt 266 neue öffentlich gemeldete Cyberangriffe auf Kraftfahrzeuge dazugekommen (vgl. Upstream Security Ltd. 2021, S. 3). Anhand dieser Zahlen ist zu erkennen, dass Cyberangriffe auch auf Kraftfahrzeuge deutlich zunehmen und in naher Zukunft auch den privaten Verbraucher treffen könnten.

Zahlreiche Versicherungsunternehmen haben dieses neuartige Risiko erkannt und darauf bereits reagiert. Im Folgenden werden die Versicherungslösungen einiger Versicherer dargestellt.

So hat bspw. die Zurich Versicherungs-Gesellschaft AG als Vorreiter den Baustein „*Cyber-Angriff*" zur Autoversicherung in der Teilkasko für die Schweiz integriert, den man zusätzlich abschließen kann (vgl. Loelf 2019, vgl. Zürich Versicherung AG 2021). Hierbei kann man sich entweder für eine Leistung bis zu 2000 CHF oder bis zu 5000 CHF entscheiden (vgl. Zürich Versicherung AG 2021). Dies sind umgerechnet circa 1800 EUR oder circa 4500 EUR. Von der Deckung von berechtigten Schadensersatzansprüchen Dritter bei Cyberangriffen spricht die Zurich Versicherungs-Gesellschaft AG in diesem Zusammenhang zumindest explizit nicht.

Dieser Baustein ist allerdings keine Allgefahrendeckung, sondern es werden nur Kosten übernommen im Rahmen einer *Beschädigung*, *Zerstörung* oder *Verschlüsselung* der Software, die durch das Hacking verursacht werden können, wenn das Fahrzeug dadurch nicht mehr nutzbar ist oder dessen Funktionen beeinträchtigt werden (vgl. Zürich Versicherung AG 2019, S. 10). Diese werden dann nur bis zur o. g. festgelegten Versicherungssumme übernommen.

Darüber hinaus verpflichtet sich der Versicherte, die Systeme und Programme auf dem aktuellen Stand der Technik zu halten oder den Empfehlungen der offiziellen Software des Herstellers zu entsprechen und diese vor unberechtigten Eindringen Dritter zu schützen

(vgl. Zürich Versicherung AG 2019, S. 10). Dazu gehört auch das Aufspielen von neuer Software oder vorhandener Updates (vgl. Zürich Versicherung AG 2019, S. 10).

Die Allgemeinen Versicherungsbedingungen der Zurich Versicherung sehen außerdem auch einige Ausschlüsse vor. So sind bspw. die Kosten für die Wiederherstellung von Fahrzeug unabhängigen Dateien und gespeicherten Daten im Fahrzeug oder die Kosten durch die unberechtigte Nutzung des Internets nicht erstattungsfähig (vgl. Zürich Versicherung AG 2019, S. 10). Schäden im Zusammenhang mit der Übertragung eines Schadprogrammes durch eine Werkstatt oder durch den Hersteller bzw. den Softwareanbieter auf das Fahrzeug sind ebenfalls nicht versichert (vgl. Zürich Versicherung AG 2019, S. 10).

Die R+V Versicherung AG, die nun auch für Deutschland das Risiko „Cyberangriff" in die Bedingungen mit aufnimmt, schließt sich der Variante des Schweizer Versicherers nicht an, einen separaten Baustein anzubieten. In einer Pressemitteilung vom 09.08.2018 gab der Versicherer bekannt, dass Dritte über die Kfz-Haftpflichtversicherung bei Fernsteuerung des Fahrzeugs durch einen Hacker geschützt sind und der eigene dadurch entstandene Blechschaden über die Vollkaskoversicherung reguliert wird (vgl. R+V 2018). Die Schäden am eigenen Fahrzeug werden bis zum Wiederbeschaffungswert abzüglich des Restwertes ersetzt. Auch eine Neupreisentschädigung bei Erfüllung der Voraussetzungen ist im Rahmen des Cyberrisikos nicht ausgeschlossen (vgl. R+V 2021, S. 22).

Für die R+V handelt der Hacker bei einem Cyberangriff (genauso wie ein Vandale) bös- oder zumindest mutwillig (vgl. R+V 2021, S. 20). Dabei sind Beschädigungen, die Zerstörung oder der Totalschaden des Fahrzeugs wie auch bei Vandalismus in der Vollkaskoversicherung gedeckt. Darüber hinaus werden auch die Kosten für die erforderliche Umprogrammierung der Software ersetzt – vorausgesetzt der Hackerangriff wurde nicht durch einen Programmier- oder Wartungsfehler des Herstellers begünstigt (vgl. R+V 2018; vgl. R+V 2021, S. 20). Der Versicherer weist außerdem darauf hin, regelmäßig auf Software-Updates zu achten, damit Sicherheitslücken geschlossen werden und das Risiko, von einem Cyberangriff betroffen zu sein, minimiert wird (vgl. R+V 2018).

Auch die Allianz SE konkretisiert Schäden durch mut- oder böswillige Handlungen eines Hackers, dessen Angriff unmittelbar auf das betroffene Fahrzeug gerichtet sein muss (vgl. Allianz 2020, S. 6). Wenn Hackerangriffe auf ein mit dem Fahrzeug kommunizierendes Unternehmen gerichtet sind und dadurch Funktionen am Fahrzeug beeinträchtigt werden, entspricht dies nur mittelbaren Handlungen, die im Rahmen der Vollkaskoversicherung bei der Allianz nicht gedeckt sind (vgl. Allianz 2020, S. 6). Darüber hinaus versichert die Allianz auch Schäden am Fahrzeug, die bei einem Unfall entstehen und durch die Manipulation der Fahrzeugsoftware durch einen Hacker verursacht worden sind (vgl. Allianz 2020, S. 6).

Die Unfallschäden, die durch einen eingedrungen Hacker verursacht werden, sind in der Regel von allen Kfz-Versicherern im Rahmen der Vollkaskoversicherung zu ersetzen, da es hier nicht darauf ankommt, ob die Attacke selbst die Tatbestandsvoraussetzungen eines Unfalls erfüllt.

Neben den bereits genannten Versicherern reagierte auch die HUK-COBURG auf dieses Risiko und nahm es in die Versicherungsbedingungen im Rahmen der Kfz-

Haftpflichtversicherung mit auf (vgl. HUK-COBURG 2021, S. 6). Es ist zu erwarten, dass die Mehrheit der Versicherer in naher Zukunft auf die Cyberrisiken bei einem Hackerangriff auf ein Kraftfahrzeug eingehen wird.

Literatur[3]

ADAC (2021): Autonomes Fahren: Die 5 Stufen zum selbstfahrenden Auto, in: ADAC.de, https://www.adac.de/rund-ums-fahrzeug/ausstattung-technik-zubehoer/autonomes-fahren/grundlagen/autonomes-fahren-5-stufen/, zugegriffen am 30.07.2021. (Quelle wurde gewählt wegen der guten Darstellung der technischen Aspekte des autonomen Fahrens).

Allianz (2020): Versicherungsbedingungen für Ihre Allianz Kfz-Versicherung (AKB), https://goaeportale.allianz.de/PKR/B-4/PKRB-4014Z0.pdf.download.pdf, zugegriffen am 12.08.2021.

AXA (o. J.): Gehackt, manipuliert, gestohlen…Cyberangriffe auf Autos, in: axa.de, https://www.axa.de/das-plus-von-axa/auto-kfz-unterwegs/sicher-unterwegs/cybercrime-auto-gehackt, zugegriffen am 25.08.2021.

Bardt, H. (2016): Autonomes Fahren: Eine Herausforderung für die deutsche Autoindustrie, IW-Trends – Vierteljahresschrift zur empirischen Wirtschaftsforschung, ISSN 1864-810X, Institut der deutschen Wirtschaft (IW), Köln, Vol. 43.

BGH (1974): Urteil Nr. 83, 30.05.1974, §22 Abs. 1 und 2 WHG in VerwRspr 1975, S. 385, https://beck-online.beck.de/Dokument?vpath=bibdata%2Fzeits%2Fverwrspr%2F1975%2Fcont%2Fverwrspr.1975.385.1.htm&pos=0, zugegriffen am 06.07.2021.

BGH (1956): † Schwarzfahrt, Begriff des Benutzers (NJW 1957, 500), Rn. 501, https://beck-online.beck.de/Dokument?vpath=bibdata%2Fzeits%2Fnjw%2F1957%2Fcont%2Fnjw.1957.500.1.htm&anchor=Y-300-Z-NJW-B-1957-S-500&readable=2&VorgaengerDokumentStreffer3=Urteil%20vom%2021.12.1956%20-%20VI%20ZR%20294%2F55&VorgaengerDokumentFullname=bibdata%2Fzeits%2Fnjw%2F1957%2Fcont%2Fnjw.1957.499.2.htm, zugegriffen am 16.07.2021.

Bundesanstalt für Straßenwesen (2018): BASt präsentiert Forschungsfahrzeug, in: BASt.de, https://www.bast.de/BASt_2017/DE/Presse/Mitteilungen/2018/presse-09-2018.html, zugegriffen am 30.07.2021.

Bundesministerium für Verkehr und digitale Infrastruktur (2021): Gesetz zum autonomen Fahren tritt in Kraft, in: bmvi.de, https://www.bmvi.de/SharedDocs/DE/Artikel/DG/gesetz-zum-autonomen-fahren.html, zugegriffen am 11.08.2021.

Burmann, M. et al. (2020): Straßenverkehrsrecht, 26. Auflage, § 7 StVG Rn. 18-23, https://beck-online.beck.de/Dokument?vpath=bibdata%2Fkomm%2Fjanjagburkostvr_26%2Fstvg%2Fcont%2Fjanjagburkostvr.stvg.p7.gl3.gla.htm&pos=2&hlwords=on, zugegriffen am 16.07.2021.

DATACOM Buchverlag GmbH (2020): SAE-Level, https://www.itwissen.info/SAE-Level-SAE-level.html, zugegriffen am 30.07.2021.

Delhaes, D. (2017): Warnung vor dem Autopiloten, in: handelsblatt.com, https://www.handelsblatt.com/politik/deutschland/automatisiertes-fahren-warnung-vor-dem-autopiloten/19297056-all.html, zugegriffen am 04.11.2021.

Gesetzesentwurf der Bundesregierung (2021): Entwurf eines Gesetzes zur Änderung des Straßenverkehrsgesetzes und des Pflichtversicherungsgesetzes – Gesetz zum autonomen Fahren, https://www.bmvi.de/SharedDocs/DE/Anlage/Gesetze/Gesetze-19/gesetz-aenderung-strassenverkehrsgesetz-

[3] Allgemeiner Hinweis vorab: Datenbanken für juristische Fachartikel wie Beck-online oder juris sind i. a. nur angemeldeten Nutzern zugängig.

pflichtversicherungsgesetz-autonomes-fahren.pdf?__blob=publicationFile, zugegriffen am 02.11.2021.

Graf von Westphalen (2020): Höhere Gewalt-Klauseln: AGB-rechtliche Pandora-Büchse in der Pandemie, ZVertriebsR 2020, S. 275, https://beck-online.beck.de/Dokument?vpath=bibdata%2Fzeits%2Fzvertriebsr%2F2020%2Fcont%2Fzvertriebsr.2020.275.1.htm&pos=6&hlwords=on, zugegriffen am 13.07.2021.

Grüneberg (2021): Haftungsausschluss gem. §7 Abs. 2 StVG, Berz/Burmann, Handbuch des Straßenverkehrsrechts (43. EL 2021), Rn. 39-43, https://beck-online.beck.de/?vpath=bibdata%2Fkomm%2FBerzBurmannHdbStVR_43%2Fcont%2FBerzBurmannHdbStVR%2EglKap4%2EglA%2EglII%2Egl1%2Eglg%2Ehtm, zugegriffen am 04.07.2021.

Grützner, T./Jakob, A. (2015): Cyberangriff, Compliance von A-Z, 2. Auflage, München, C.H. Beck, https://beck-online.beck.de/?vpath=bibdata/lex/GruetznerJakobLexC_2/cont/GruetznerJakobLexC.Cyberangriff.htm, zugegriffen am 27.07.2021.

Hey, T. (2019): Die außervertragliche Haftung des Herstellers autonomer Fahrzeuge bei Unfällen im Straßenverkehr, Wiesbaden, Springer Gabler, https://link.springer.com/book/10.1007/978-3-658-23957-2, zugegriffen am 02.11.2021.

HUK-COBURG (2021): Allgemeine Bedingungen für die Kfz-Versicherung (AKB) inkl. Kundeninformation, https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwiN-o3mga7yAhX8gf0HHeeoBtIQFnoECAUQAQ&url=https%3A%2F%2Fwww.huk.de%2Fcontent%2Fdam%2Fhukde%2Fdokumente%2Fprodukte%2Fallgemeine_versicherungsbedingungen_kfz.pdf&usg=AOvVaw32FvZegIUzTd6Z0cdq4B%2D%2D, zugegriffen am 13.08.2021.

Koch, R. (2018): Verteilung des Haftpflichtversicherungs-/Regressrisikos bei Kfz-Unfällen während der Fahrzeugführung im Autopilot-Modus gem. §1a Abs. 2 StVG in VersR Aufsätze, 69. Jg., Nr. 15 ab S. 901, https://www.wiso-net.de/dosearch?_searchOnlyInAbstractField=&_searchOnlyInTitleField=&explicitSearch=true&q=0342-2429.IS.+AND+2018.YR.+AND+15.HN.+AND+901.SE.#VRA__02x69x2018x15x0901x0001, zugegriffen am 14.07.2021.

König (2013): Straßenverkehrsrecht – Hentschel/König/Dauer (42. Aufl. 2013), §7 StVG, S.146, https://beckassets.blob.core.windows.net/product/readingsample/11152335/hentschel-strassenverkehrsrecht-9783406643729.pdf, zugegriffen am 04.07.2021.

Lammers, U. (2006): Kraftfahrtversicherung: Produktorientierte Qualifikation (3. Aufl.).

Langheid, T./Wandt, M. (2017): Kraftfahrzeug-Haftpflichtversicherung, in: Münchener Kommentar zum VVG, https://beck-online.beck.de/Dokument?vpath=bibdata%2Fkomm%2Fmuekovvg_2_band3%2Fcont%2Fmuekovvg.glteil2.glkap3.gl410.gld.glii.gl1.htm&pos=11&hlwords=on, zugegriffen am 02.11.2021.

Loelf, F. (2019): Erste Cyberversicherung für Autos, in Total Consulting Versicherungsmakler GmbH, https://www.total-consulting.gmbh/erste-cyberversicherungen-fuer-autos/, zugegriffen am 10.08.2021.

Maier, F. (2015): Hackerangriffe auf vernetzte Autos, Auto-Hacks 2015: Remote Gefahr, in: computerwoche.de, https://www.computerwoche.de/a/auto-hacks-2015-remote-gefahr,3215128, zugegriffen am 09.08.2021.

Mehrbrey, K. L./Schreibauer, M. (2016): Haftungsverhältnisse bei Cyber-Angriffen – Ansprüche und Haftungsrisiken von Unternehmen und Organen (MMR 2016, 75) Rn. 75, https://beck-online.beck.de/Dokument?vpath=bibdata%2Fzeits%2Fmmr%2F2016%2Fcont%2Fmmr.2016.75.1.htm&pos=3&hlwords=on, zugegriffen am 27.07.2021.

Munich Re (2021): Cyber-Versicherung: Risiken und Trends 2021, https://www.munichre.com/topics-online/de/digitalisation/cyber/cyber-insurance-risks-and-trends-2021.html, zugegriffen am 10.08.2021.

Pütz, F./Maier, K. (2019): Haftung und Versicherungsschutz bei Cyberangriffen auf ein Kfz, in: r+s 2019 Heft 8, S. 444, https://beck-online.beck.de/Dokument?vpath=bibdata%2Fzeits%2Frunds%2F2019%2Fcont%2Frunds.2019.444.1.htm&pos=1&hlwords=on, zugegriffen am 07.07.2021.

R+V Kfz-Versicherung (2021): Verbraucherinformation, https://www.ruv.de/dam/jcr:e053f7d8-4e4f-4c58-ac82-4ea750924d7a/ruv-kkr_kfz_verbraucherinfo.pdf, zugegriffen am 12.08.2021.

R+V (2018): R+V deckt Cyberrisiken in der Kfz-Versicherung ab, Information für die Medien, https://www.ruv.de/dam/jcr:5532b6a8-4790-4f77-95eb-fa02e8a8c96f/20180809-cyberrisiken%20kfz-versicherung.pdf, zugegriffen am 12.08.2021.

Roshan, B. (2021): Automatisiertes und autonomes Fahren im Überblick, https://beck-online.beck.de/Dokument?vpath=bibdata%2Fzeits%2Fnjw-spezial%2F2021%2Fcont%2Fnjw-spezial.2021.137.1.htm&pos=2&hlwords=on, zugegriffen am 02.11.2021.

SAE International (2021): https://www.sae.org/standards/content/j3016_201806/, zugegriffen am 28.07.2021.

Schmidt (2021): Verschulden, in Creifelds Rechtswörterbuch (26. Edition 2021, C.H.BECK), https://beck-online.beck.de/Dokument?vpath=bibdata%2Flex%2Fcre_26%2Fcont%2Fcre.verschulden.htm&anchor=Y-500-W-CRE-SW-VERSCHULDEN, zugegriffen am 17.08.2021.

Science Media Center (2021): Wie weit ist die Forschung mit dem autonomen Fahren?, in: sciencemediacenter.de, https://www.sciencemediacenter.de/alle-angebote/science-response/details/news/wie-weit-ist-die-forschung-mit-dem-autonomen-fahren/, zugegriffen am 21.07.2021.

Siller, H. (2018): Hacker, in: wirtschaftslexikon.gabler.de, https://wirtschaftslexikon.gabler.de/definition/hacker-53395, zugegriffen am 28.07.2021.

Statista (2021): Anteil der Autos die mit einem Tempomat ausgestattet sind im Jahr 2018 in Deutschland, in: Statista.com, https://de.statista.com/statistik/daten/studie/255312/umfrage/anteil-der-pkw-mit-tempomat/, zugegriffen am 02.08.2021.

Stender-Vorwachs, J./Oppermann, B. (2020): Autonomes Fahren – Technische Grundlagen, Rechtsprobleme, Rechtsfolgen, 2. Auflage, München, C.H. Beck.

Universität Greifswald (2018): 1. Besprechungsfall, https://rsf.uni-greifswald.de/storages/uni-greifswald/fakultaet/rsf/lehrstuehle/ls-habermeier/1._Besprechungsfall__16.04.2018_-_Loesungsvorschlag.pdf, zugegriffen am 02.11.2021.

Upstream Security Ltd. (2021): Upstream Security global automotive cybersecurity report 2021, research into cyber attack trends in light of cybersecurity standards and regulations, https://info.upstream.auto/hubfs/Security_Report/Security_Report_2021/Upstream_Security-Global_Automotive_Cybersecurity_Report_2021.pdf?_hsmi=101240621&_hsenc=p2ANqtz-_c3eMS5LDY3NDkvLK1-EjNmp-2oJJmysGgjz253_GgDL3ztbPOzuLDPxSad-62TG-w14YAA5CZjD0GGcQhlNz8pBHBtQ, zugegriffen am 10.08.2021.

Upstream Security Ltd. (2020): Upstream Security's global automotive cybersecurity report 2020, research into cyber-attack trends in the smart mobility ecosystem, https://info.upstream.auto/hubfs/Security_Report/Security_Report_2020/Upstream%20Security-Global_Automotive_Cybersecurity_Report_2020.pdf?_hsmi=80788392&_hsenc=p2ANqtz%2D%2DElmeWueiPcm9CY65hv1h_oTq5YMzU3oAiZvBUgGL0gNRggT6Jmq5s4b-kh1S-rHInZ72xqZNTHvMUbs37A_Z6-r8WA, zugegriffen am 10.08.2021.

Zürich Versicherung AG (2021): Auch Autos sind vor Hackern nicht mehr sicher, zurich.ch, https://www.zurich.ch/de/services/wissen/fahrzeuge-und-reisen/cyberangriffe-aufs-auto, zugegriffen am 10.08.2021.

Zürich Versicherung AG (2019): Motorfahrzeugversicherung, Kundeninformation Allgemeine Versicherungsbedingungen (AVB), https://www.zurich.ch/-/media/zurich-site/content/privatkunden/fahrzeuge-reisen/dokumente/avb-motorfahrzeug-versicherung/avb-motorfahrzeuge-automotorrad-versicherung.pdf?la=de, zugegriffen am 10.08.2021.

Prof. Dr. Karl Maier hat in Rechtswissenschaften promoviert und ist als Professor am **ivw**Köln mit den Schwerpunkten Kraftfahrt-, Unfall, Rechtschutzversicherung und Versicherungsrecht tätig. Er ist einer der Leiter der Forschungsstelle Versicherungsrecht am **ivw**Köln.

Nicole Antonczyk absolvierte im Jahr 2021 hr Bachelor-Studium im Studiengang Risk and Insurance mit den Schwerpunkten Rechnungswesen, Riskmanagement und HUKR. Zeitgleich schloss sie ihre Ausbildung zur Kauffrau für Versicherungen und Finanzen im Rahmen eines dualen Studiums bei der Provinzial Holding AG ab. Während der Ausbildung beschäftigte sie sich schwerpunktmäßig mit der Kraftfahrtversicherung. Derzeit studiert sie Wirtschaftsrecht im Master an der Westfälischen Hochschule in Recklinghausen und übt eine Werkstudententätigkeit bei der Provinzial aus.

Robin Biskup absolvierte in 2021 sein Bachelor-Studium im Studiengang Versicherungswesen an der TH Köln. Nach seinem Abitur begann er zunächst in 2015 seine Berufsausbildung als Kaufmann für Versicherungen und Finanzen bei der Debeka Versicherung in Köln. Nach Abschluss der Ausbildung wechselte er zum Industrie-Versicherungsmakler Interassekuranz Sitt & Overlack GmbH. Zum Sommersemester 2018 nahm er das Bachelorstudium an der TH Köln auf und arbeitete parallel als Werkstudent bei der neu gegründeten Versicherungsmakler-Gesellschaft Sitt + Co. GmbH als Kundenbetreuer für Gewerbe- und Industriekunden. Diese Tätigkeit führt er aktuell mit erweiterten Zuständigkeiten in einer Vollzeit-Tätigkeit aus und beabsichtigt darüber hinaus einen berufsbegleitenden Masterstudiengang im Studiengang Versicherungsrecht an der TH Köln.

Leyla Dalir absolvierte im Jahr 2021 ihr Bachelorstudium im Fach Versicherungswesen mit den Schwerpunkten Rückversicherung, Haftpflicht- und Kraftfahrtversicherung sowie Rechnungswesen und Versicherungsmathematik an der Technischen Hochschule in Köln. Im Jahr 2018 begann sie als duale Studentin im Provinzial Konzern. Im Rahmen ihrer Ausbildung war sie in der Vertragsabteilung der Lebensversicherung, der Schadenbearbeitung in der allgemeinen Haftpflicht sowie im zentralen Controlling tätig. Zur Zeit der Erstellung der Publikation befand sie sich im Masterstudium im Fach Betriebswirtschaftslehre an der Heinrich-Heine-Universität Düsseldorf und arbeitete als Werkstudentin im Bereich Kapitalanlagencontrolling und IT-Koordination in der Provinzial Versicherung.