Exposé für das Dissertationsvorhaben

Cybersicherheit im Spannungsfeld von Binnenmarktregulierung und nationaler Sicherheit

Verfasser

Mag. Vinzenz Heußler, LL.M.

vinzenz.klaus.heussler@univie.ac.at

Matr.-Nr.: 00849293

Angestrebter akademischer Grad

Doctor iuris (Dr. iur.)

Betreuer

ao. Univ.-Prof. Mag. DDr. Erich Schweighofer

Inhalt

1 Einleitung

Eines der Ziele der Europäischen Union (EU) ist die Errichtung eines Binnenmarktes.[1] Es handelt sich um eine Daueraufgabe der Union, den Binnenmarkt zu verwirklichen beziehungsweise dessen Funktionieren zu gewährleisten.[2] Hierbei stellt der Aufbau des digitalen Binnenmarkts derzeit eine der größten Herausforderungen bei der Weiterentwicklung des Binnenmarkts dar.[3] In Fortführung der Lissabon-Strategie, mit welcher das Ziel formuliert wurde, die Union zum wettbewerbsfähigsten und dynamischsten wissensbasierten Wirtschaftsraum in der Welt zu machen,[4] wurde im Jahr 2010 mit der Strategie Europa 2020[5] die Digitale Agenda für Europa[6] als eine Leitinitiative eingeführt.[7] Damit wurde der wichtige Beitrag anerkannt, den Informations- und Kommunikationstechnologie (IKT) leisten muss, damit die Union ihre für 2020 gesteckten Ziele erreicht.[8] In der Strategie für einen digitalen

[1] Art 3 Abs 3 EUV.
[2] Vgl. *Lengauer* in *Mayer*/*Stöger* (Hrsg), EUV/AEUV Art 3 EUV Rz 9 (Stand 01.12.2012, rdb.at).
[3] *Maciejewski*/*Ratcliff*/*Næss*, Binnenmarkt: Allgemeine Grundsätze, 4 <https://www.europarl.europa.eu/ftu/pdf/de/FTU_2.1.1.pdf> (Stand April 2020).
[4] Schlussfolgerungen des Europäischen Rates vom 23. und 24. März 2000.
[5] Mitteilung der Kommission, Europa 2020 – Eine Strategie für intelligentes, nachhaltiges und integratives Wachstum, COM(2010) 2020 final vom 03.03.2010.
[6] Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen, Eine Digitale Agenda für Europa, COM(2010) 245 final vom 19.05.2010.
[7] COM(2010) 245 final, 16 f.
[8] *Maciejewski*/*Ratcliff*/*Næss*, Der allgegenwärtige digitale Binnenmarkt, 1 <https://www.europarl.europa.eu/ftu/pdf/de/FTU_2.1.7.pdf> (Stand April 2020).

Binnenmarkt[9] räumt die Europäische Kommission (EK) diesem Vorhaben eine vorrangige Stellung ein und bestätigte dies im Jahr 2020 in der Agenda für Europa[10] sowie in der Mitteilung über die Gestaltung der digitalen Zukunft Europas.[11]

Der Trend des immer umfangreicheren Einsatzes von Informations- und Kommunikationstechnologien (IKT) und allen voran der Siegeszug des Internets haben alle Teile der Gesellschaft in den vergangenen Jahrzehnten enorm beeinflusst.[12] Die voranschreitende Digitalisierung hat dazu geführt, dass ganze Lebensbereiche, wirtschaftliche und politische Prozesse in das Internet verlagert wurden. Den damit verbundenen Chancen stehen jedoch erhebliche Risiken gegenüber, welche sich u.a. aus zunehmend und verstärkt professionell gestalteten politischen wie auch kriminellen Aktivitäten im Cyberraum ergeben.[13] Es verwundert daher kaum, dass die Sicherung der digitalen Zukunft Europas von wesentlicher Bedeutung für den Wohlstand in der Union ist und Cybersicherheit daher eine bedeutende Rolle bei der Erschließung des Potenzials des digitalen Binnenmarkts spielt,[14] welche sich in einer zunehmenden Regulierung von Cybersicherheit durch die Union bemerkbar macht. Zeitgleich verbleibt kompetenzrechtlich die nationale Sicherheit in der alleinigen Verantwortung der einzelnen Mitgliedstaaten der Union,[15] wobei sich die nationale Sicherheit auch auf den Cyberraum und damit auf die Sicherheit von Netz- und Informationssystem bzw. die Cybersicherheit erstreckt.

Vor diesem Hintergrund soll der Inhalt dieser Dissertation eine umfassende Abhandlung über die Regulierung von Cybersicherheit durch die Union aufgrund binnenmarktrechtlicher Kompetenzgrundlagen und dem sich daraus ergebende Spannungsfeld zum Bereich der nationalen Sicherheit sein.

---

[9] Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen, Strategie für einen digitalen Binnenmarkt für Europa, COM(2015) 192 final vom 06.05.2015.

[10] *Von der Leyen*, Eine Union, die mehr erreichen will: Meine Agenda für Europa <https://ec.europa.eu/commission/sites/beta-political/files/political-guidelines-next-commission_de.pdf> (26.07.2020).

[11] Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen, Gestaltung der digitalen Zukunft Europas, KOM(2020) 67 endg vom 19.02.2020.

[12] Vgl. Gemeinsame Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen, Cybersicherheitsstrategie der Europäischen Union – ein offener, sicherer und geschützter Cyberraum, JOIN(2013) 1 final vom 07.02.2013, 2.

[13] Cyber Sicherheit Steuerungsgruppe, Bericht Cyber Sicherheit (2017) 42.

[14] *Consilium*, Cybersicherheit in Europa: strengere Regeln und besserer Schutz <https://www.consilium.europa.eu/de/policies/cybersecurity> (25.07.2020).

[15] Art 4 Abs 2 EUV.

2 Motivation und Forschungsgegenstand

In einem ersten Schritt wird die Dissertation der Frage nachgehen, wo im Unionsrecht Cybersicherheit als Regulierungsgegenstand vorkommt. Hierbei wird der Begriff Cyber Security von den Begriffen Cyber Crime, Cyber Justice, Cyber Diplomacy, Cyber Defence und Cyber Terrorismus abzugrenzen sein. Ferner wird eine Unterscheidung zwischen horizontaler sowie vertikaler (bzw. sektorieller) Regulierung von Cybersicherheit vorgenommen werden. Eine bedeutende Rolle wird hierbei die Richtlinie 2002/21/EG vom 7. März 2002 über einen gemeinsamen Rechtsrahmen für elektronische Kommunikationsnetze und -dienste (Rahmen-RL) idgF vom 19.12.2009 zukommen, die bereits IKT-Sicherheitsanforderungen festlegte, noch bevor der Begriff der Cybersicherheit im Jahr 2013 in politischen Dokumenten breiten Gebrauch fand. Denn im Jahr 2013 war die EK der Auffassung, dass es an der Zeit war, dass die Union ihre Maßnahmen im Bereich der Cybersicherheit verstärkt. In diesem Sinne legte sie erstmals eine Cybersicherheitsstrategie vor. Diese Cybersicherheitsstrategie der Union mit dem Untertitel „ein offener, sicherer und geschützter Cyberraum" verfolgte fünf Prioritäten, nämlich 1.) die Erreichung einer höheren Cyber Resilienz, 2.) eine drastische Reduktion von Cyber Crime, 3.) die Entwicklung einer Cyber Defence Policy und von Fähigkeiten iZm der GSVP, 4.) die Entwicklung industrieller und technologischer Ressourcen für Cybersicherheit sowie 5.) die Errichtung einer kohärenten internationalen Cyberspace Policy für die EU und Förderung von europäischen Kennwerten.

Die wichtigste Maßnahme der Cybersicherheitsstrategie 2013 war der Vorschlag für die NIS-RL.[16] Vor dem Hintergrund, dass die Sicherheit von Netz- und Informationssystemen mit den zugehörigen Diensten eine zentrale Rolle für wirtschaftliche und gesellschaftliche Tätigkeiten spielt und ihre Verlässlichkeit und Sicherheit entscheidend für wirtschaftliche und gesellschaftliche Tätigkeiten und das Funktionieren des Binnenmarkts sind,[17] wurde auf europäischer Ebene mit der Richtlinie (EU) 2016/1148 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union (im Folgenden: NIS-RL) die erste unionsweite Rechtssetzung zur Cybersicherheit verabschiedet. Die NIS-RL trat am 08.08.2016 in Kraft und war bis zum 09.05.2018

[16] Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über Maßnahmen zur Gewährleistung einer hohen gemeinsamen Netz- und Informationssicherheit in der Union, COM(2013) 48 final vom 07.02.2013.
[17] ErwGr 1 der Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union, ABl L 2016/194, 1.

umzusetzen. [18] Sie legt Maßnahmen fest, mit denen ein hohes gemeinsames Sicherheitsniveau von Netz- und Informationssystemen in der Union erreicht werden soll. Insbesondere verpflichtet sie die Mitgliedstaaten dazu, eine nationale Strategie für die Sicherheit von Netz- und Informationssystemen zu erlassen, schafft Grundlagen für die strategische und operative Zusammenarbeit auf Unionsebene durch die Einrichtung der NIS-Kooperationsgruppe und des CSIRTs-Netzwerks, enthält die Pflicht zur Benennung national zuständiger Behörden, zentraler Anlaufstellen und von Computer-Notfallteams (Computer Security Incident Response Teams – CSIRTs) und sieht Sicherheitsanforderungen und Meldepflichten für Betreiber wesentlicher Dienste sowie für Anbieter digitaler Dienste vor. Während Anbieter digitaler Dienste der Vollharmonisierung unterliegen und bestimmte Arten von Diensten der Informationsgesellschaft (Online-Marktplatz, Online-Suchmaschine und Cloud-Computing-Dienste) bereitstellen, sieht die NIS-RL für Betreiber wesentlicher Dienste eine Mindestharmonisierung vor. Die NIS-RL schreibt vor, dass die Mitgliedstaaten Betreiber wesentlicher Dienste anhand bestimmter Kriterien ermitteln müssen. Nach diesen Kriterien stellt eine Einrichtung, die als Betreiber wesentlicher Dienste in Frage kommt, einen Dienst bereit, der für die Aufrechterhaltung kritischer gesellschaftlicher und/oder wirtschaftlicher Tätigkeiten unerlässlich ist, wobei die Bereitstellung dieses Dienstes abhängig von Netz- und Informationssystemen ist und ein Sicherheitsvorfall eine erhebliche Störung bei der Bereitstellung dieses Dienstes bewirken würde. Der Anhang II gibt ferner in sieben Sektoren bestimmte Arten von Einrichtungen vor, die die Mitgliedstaaten bei der Ermittlung berücksichtigen müssen.

Im September 2017 veröffentlichte die EK ein Cybersicherheitspaket, welches viele weitere Maßnahmen zur Erhöhung der Cybersicherheit in der Union enthielt.[19] Hervorzuheben ist hierbei der Vorschlag für den Cybersecurity Act.[20] Der Cybersecurity Act, welcher am 27.06.2019 in Kraft trat,[21] verfolgt u.a. das Ziel, die Zusammenarbeit und Koordinierung zwischen den Mitgliedstaaten und den EU-Einrichtungen zu verbessern, die Kapazitäten auf

[18] In Österreich wurde die NIS-RL durch das Bundesgesetz zur Gewährleistung eines hohen Sicherheitsniveaus von Netz- und Informationssystemen (Netz- und Informationssystemsicherheitsgesetz – NISG), BGBl I 111/2018, umgesetzt.

[19] Vgl. *DG CONNECT*, Cybersecurity package 'Resilience, Deterrence and Defence: Building strong cybersecurity for the EU' <https://ec.europa.eu/digital-single-market/en/news/cybersecurity-package-resilience-deterrence-and-defence-building-strong-cybersecurity-eu> (Stand 19.09.2017).

[20] Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die „EU-Cybersicherheitsagentur“ (ENISA) und zur Aufhebung der Verordnung (EU) Nr. 526/2013 sowie über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik („Rechtsakt zur Cybersicherheit“), COM(2017) 477 final vom 13.09.2017.

[21] Verordnung (EU) 2019/881 des Europäischen Parlaments und des Rates vom 17. April 2019 über die ENISA (Agentur der Europäischen Union für Cybersicherheit) und über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik und zur Aufhebung der Verordnung (EU) Nr. 526/2013 (Rechtsakt zur Cybersicherheit, ABl L 2019/151, 15.

Unionsebene auszubauen, um die Maßnahmen der Mitgliedstaaten zu ergänzen, insbesondere im Fall von grenzüberschreitenden Cyberkrisen, und die Transparenz bei den Angaben zur Vertrauenswürdigkeit der bescheinigten Cybersicherheit von IKT-Produkten und -Diensten zu verbessern, um das Vertrauen in den digitalen Binnenmarkt und in digitale Innovationen zu stärken, und das Nebeneinander unterschiedlicher Zertifizierungssysteme in der Union zu vermeiden. Im Wesentlichen sollte dies durch zwei Maßnahmen erreicht werden, und zwar durch die Reformierung des Mandats der Agentur der Europäischen Union für Netz- und Informationssicherheit (ENISA), indem diese ein permanentes Mandat mit erweiterten Aufgaben und Befugnissen erhält,[22] sowie durch die Einführung eines Rahmens für die Festlegung europäischer Schemata für die Cybersicherheitszertifizierung.[23]

Die jüngste EU-Initiative im Bereich der Cybersicherheit, die für diese Dissertation von Relevanz ist und daher im Exposé Erwähnung finden soll, erging im Bereich der Sicherheit der fünften Generation des Mobilfunknetzes. Am 26. März 2019 gab die EK eine Empfehlung über die Cybersicherheit von 5G-Netzen[24] heraus, welche insbesondere die Durchführung einer nationalen Risikoanalyse mit Fokus auf 5G-Netzwerke, die Überprüfung der gesetzten nationalen Maßnahmen, eine verstärkte Zusammenarbeit auf EU-Ebene und die Durchführung einer EU-weit koordinierten Risikoanalyse sowie die Schaffung eines gemeinsamen Instrumentariums von Maßnahmen zur Risikominimierung vorsieht. Dieses gemeinsame Instrumentarium[25] beinhaltet folgende Aussage: "*All Member States should ensure that they have measures in place (including powers for national authorities) to respond appropriately and proportionately to the presently identified and future risks […] They should in particular […] [a]ssess the risk profile of suppliers; as a consequence, apply relevant restrictions for suppliers considered to be high risk - including necessary exclusions to effectively mitigate risks - for key assets defined as critical and sensitive in the EU coordinated risk assessment (e.g. core network functions, network management and orchestration functions, and access network functions)*".[26] Das gemeinsame Instrumentarium sieht als Empfehlung folglich als drastischste Form der Risikominimierung den Ausschluss von bestimmten Vermögenswerten von Hochrisiko-Lieferanten durch die Mitgliedstaaten auf nationaler Ebene vor, knüpft dies jedoch an die Ergebnisse der unionsweit koordinierten Risikoanalyse an.

[22] Art 3 ff VO (EU) 2019/881.
[23] Art 1 lit b VO (EU) 2019/881.
[24] Empfehlung (EU) 2019/534 der Kommission vom 26. März 2019 Cybersicherheit der 5G-Netze, ABl L 2019/88, 42.
[25] *NIS Cooperation Group*, Cybersecurity of 5G networks: EU Toolbox of risk mitigating measures (CG Publication 01/2020) <https://ec.europa.eu/digital-single-market/en/nis-cooperation-group> (21.07.2020).
[26] CG Publication 01/2020, 18.

Mag. Vinzenz Heußler, LL.M.
vinzenz.klaus.heussler@univie.ac.at

3 Stand der Forschung

Seit mit der NIS-RL der erste (horizontale) Rechtsakt zur Cybersicherheit in der Union verabschiedet wurde, nahm Cybersicherheit als Regulierungsgegenstand eine fortlaufende Entwicklung. Neben dem Cybersicherheitspaket 2017 sieht auch das Arbeitsprogramm der EK weitere Initiativen in diesem Bereich vor. Obgleich sich der Hinweis in den Rechtsakten, wonach die nationalen Zuständigkeiten von diesen auf Unionsebene unberührt bleiben, mantraartig wiederholt, wurde die sich daraus ergebende rechtswissenschaftliche Fragestellung der Abgrenzung bisher nicht aufgearbeitet. Generell ist, soweit ersichtlich, das Themengebiet der Regulierung von Cybersicherheit durch die Union in Österreich rechtswissenschaftlich bisher nicht systematisch behandelt worden. Gegenstand bisheriger wissenschaftlicher Arbeiten war in erster Linie die NIS-RL bzw. deren Umsetzung durch die Mitgliedstaaten (siehe „Ausgewählte Literatur“). Für den Bereich der Cybersicherheit fehlt eine umfassende Abhandlung zur Abgrenzung der Kompetenzen der Union von der nationalen Sicherheit. Sehr wohl besteht jedoch umfassende Literatur und Judikatur zur Frage des Anwendungsvorrangs des Unionsrechts und zu den zu untersuchenden Art 4 EUV und Art 114 AEUV sowie zu den verwandten bzw. für die systematische Interpretation relevanten Artikel, wie z.B. Art 2 Abs 2, Art 23, 36 AEUV (siehe „Ausgewählte Literatur“). Es findet sich jedoch keine wissenschaftliche Abhandlung, die sich umfassend und systematisch dem Thema nähern würde.

4 Wissenschaftliche Problemstellung und Forschungsfragen

Die oben genannten Rechtsakte wurden im Kontext der Digitalen Agenda für Europa bzw. im Rahmen der Verwirklichung des digitalen Binnenmarktes vorgeschlagen. Sie haben ihre Basis in Art 114 AEUV. Dieser Artikel bildet die Rechtsgrundlage für die Beseitigung von Hemmnissen im zwischenstaatlichen Verkehr mit Waren und Dienstleistungen im Binnenmarkt durch die Angleichung nationaler Rechts- und Verwaltungsvorschriften mit Hilfe von Sekundärrecht. Die Ratio der Norm liegt in der Herstellung und Erhaltung des Binnenmarktes,[27] dessen Errichtung nach Art 3 Abs 3 erster Satz EUV ein wesentliches Ziel der Union darstellt.[28] Die Union erlässt die erforderlichen Maßnahmen, um den Binnenmarkt

[27] Vgl. Art 26 AEUV.
[28] *Leidenmühler* in *Jaeger*/*Stöger* (Hrsg), EUV/AEUV Art 114 AEUV Rz 2 (Stand 1.10.2018, rdb.at).

zu verwirklichen beziehungsweise dessen Funktionieren zu gewährleisten,[29] wobei es sich zugleich um ein Ziel als auch eine Daueraufgabe der Union handelt.[30] Bei der Regulierung des Binnenmarktes liegt eine geteilte Zuständigkeit der Union mit den Mitgliedstaaten vor.[31]

Nach Art 4 Abs 1 EUV verbleiben alle der Union nicht in den Verträgen übertragenen Zuständigkeiten gemäß Art 5 EUV bei den Mitgliedstaaten. Art 4 Abs 2 zweiter Satz EUV besagt sodann, dass die Union die grundlegenden Funktionen des Staates, insbesondere die Wahrung der territorialen Unversehrtheit, die Aufrechterhaltung der öffentlichen Ordnung und den Schutz der nationalen Sicherheit achtet. Von essentieller Bedeutung für das Dissertationsvorhaben ist der dritte Satz von Art 4 Abs 2 EUV, wonach insbesondere die nationale Sicherheit weiterhin in die alleinige Verantwortung der einzelnen Mitgliedstaaten fällt.

Die wissenschaftliche Problemstellung ergibt sich nunmehr aus dem Spannungsfeld, welches dadurch entsteht, dass die Union Cybersicherheit unter dem Gesichtspunkt der Verwirklichung des Binnenmarktes durch die Angleichung nationaler Rechts- und Verwaltungsvorschriften reguliert, währenddessen Cybersicherheit, verstanden als Teilgebiet der nationalen Sicherheit, in die alleinige Verantwortung der einzelnen Mitgliedstaaten fällt. Dabei ergibt sich die Fragestellung, wie weit die Union bei der Regulierung gehen kann, gerade wenn es um die Cybersicherheit im Bereich der öffentlichen Verwaltung und von Einrichtungen und Diensten geht, die für die Daseinsvorsoge eines Mitgliedstaates von Bedeutung sind. Diesbezüglich soll der Anwendungsbereich der NIS-RL näher beleuchtet werden. In diesem Zusammenhang soll im Vorhaben auch das Verhältnis zur RL 2008/114/EG zur Ermittlung und Ausweisung europäischer kritischer Infrastrukturen (EKI) und Bewertung der Notwendigkeit, ihren Schutz zu verbessern, [32] untersucht werden. Dabei soll die Ähnlichkeit zwischen den Formulierungen des ursprünglichen Vorschlags zur NIS-RL mit denen der EKI-RL zum Vorschein gebracht werden und vor dem Hintergrund erörtert werden, dass die EKI-RL auf Art 308 EGV (jetzt Art 352 AEUV) gestützt ist.

Im Hinblick auf die Frage, inwieweit die Union die Cybersicherheit regulieren kann, soll des Weiteren untersucht werden, ob sich in vertikalen Regulierungsansätzen ähnliche Spannungsfelder auftun oder sich dort die Frage der nationalen Sicherheit nicht in der Form stellt. So sind vertikalen Regulierungsansätze teils spezifischer als die Vorgaben der NIS-RL,

[29] Art 26 Abs 1 AEUV.
[30] Vgl. *Lengauer* in EUV/AEUV Art 3 EUV Rz 9.
[31] Art 4 Abs 2 lit a AEUV.
[32] Richtlinie 2008/114/EG des Rates vom 8. Dezember 2008 über die Ermittlung und Ausweisung europäischer kritischer Infrastrukturen und die Bewertung der Notwendigkeit, ihren Schutz zu verbessern, ABl L 2008/345, 75.

stellen anders als die NIS-RL nicht auf „kritische Infrastruktur“ ab und weisen sich teils als Safety-Bestimmungen aus (wohingegen die NIS-RL von Security spricht). Aus diesem Grund soll untersucht werden, ob die im Deutschen sprachlich nicht hervortretende Unterscheidung zwischen Security, die oft mit als Angriffssicherheit verstanden wird, und Safety, welche oft als Betriebssicherheit verstanden wird, Erkenntnisgewinne verspricht.[33]

Nachdem das Mandat der ENISA, welches durch den CSA erneuert wurde, auf Art 114 AEUV (bzw. das ursprüngliche Mandat auf der Vorgängerbestimmung ex-Art 95 EGV) beruht, stellt sich auch hier die Frage, inwieweit eine EU-Agentur Aufgaben im Bereich der Cybersicherheit wahrnehmen kann, um der Verwirklichung des Binnenmarktes zu dienen. Dies ist besonders spannend aufgrund der Tatsache, dass die ENISA nun erstmals enthält operative Zuständigkeiten wahrnimmt.[34] Das zum ursprünglichen Mandat[35] ergangene Erkenntnis des EuGH in der der Rechtssache C-217/04[36] soll vor diesem Hintergrund beleuchtet werden.

Abschließend soll die Empfehlung der EK über die Cybersicherheit von 5G-Netzen behandelt werden. Diese besagt in ErwGr 26, dass die Zuständigkeiten der Mitgliedstaaten für Tätigkeiten in Bezug auf die öffentliche Sicherheit, die Landesverteidigung, die nationale Sicherheit und das staatliche Handeln im strafrechtlichen Bereich, einschließlich des Rechts der Mitgliedstaaten, Anbieter oder Lieferanten aus Gründen der nationalen Sicherheit von ihren Märkten auszuschließen, von dieser Empfehlung unberührt bleiben. Der Regulierungsansatz zur Cybersicherheit von 5G-Netzen wirft die Frage auf, ob darin nicht ein Beispiel für einen neuen Lösungsweg der Regulierung von Cybersicherheit unter Auflösung der oben genannten Spannungsfelder, oder aber gerade ein Beispiel für einen Lösungsweg mit erhöhtem Fragmentierungsrisiko, erblickt werden kann.

5 Methodik

Im Hinblick auf die methodische Vorgehensweise soll die Abhandlung des Themas in Anwendung der traditionellen juristischen Methodik erfolgen, wonach zunächst eine umfassende Recherche der entsprechenden Bestimmungen, Judikatur und rechtswissenschaftlichen Literatur stattfinden wird. Dabei sollen die einschlägigen

[33] Vgl. *Saurugg*, Smart Metering und mögliche Auswirkungen auf die nationale Sicherheit, 19 <https://www.cybersecurityaustria.at/images/pdf/smart_metering_und_moegliche_auswirkungen_auf_die_nationale_sicherheit.pdf> (Stand Juli 2011).
[34] Art 7 VO (EU) 2019/881.
[35] Verordnung (EG) 460/2004 des Europäischen Parlaments und des Rates vom 10. März 2004 zur Errichtung der Europäischen Agentur für Netz- und Informationssicherheit, ABl L 2004/77, 1.
[36] EuGH 02.05.2006, C-217/04 (Vereinigtes Königreich/Parlament und Rat).

primärrechtlichen Bestimmungen des EUV und AEUV anhand der vorhanden Literatur und Judikatur dargestellt werden, gefolgt von einer Betrachtung der relevanten Bestimmungen in den Sekundärrechtsakten und weiteren Maßnahmen wie z.B. Empfehlungen und Mitteilungen. Des Weiteren kann der Versuch unternommen werden, insbesondere die Judikatur zu Fällen, welche die Rechtsfrage zum Anwendungsbereich des Art 4 Abs 2 EUV zum Gegenstand hatten, auf die Möglichkeit hin zu untersuchen, ob sie fruchtbar gemacht werden können.[37] Das Dissertationsvorhaben muss die parallel zum Erfassen stattfindenden Evaluierungen auf Unionsebene, insbesondere der NIS-RL und der Empfehlung (EU) 2019/553 berücksichtigen.

6 Vorläufiges Inhaltsverzeichnis

1. Einführung
2. Binnenmarkt und Cybersicherheit
   2.1. Der digitale Binnenmarkt
   2.2. EU Cybersicherheitsstrategie 2013
   2.3. EU Cybersicherheitspaket 2017
3. Unionsrechtliche Kompetenzen und nationale Sicherheit
   3.1. Art 4 EUV
   3.2. Art 114 AEUV
4. EU-Rechtsakte und –Maßnahmen zu Cybersicherheit und ihre binnenmarktrechtlichen Grundlagen
   4.1. Rahmenrichtlinie
   4.2. NIS-RL
   4.3. Cybersecurity Act
5. Empfehlung über Cybersicherheit von 5G-Netzen als neuer Regulierungsansatz?
6. Schlusswort

[37] Z.B. EuGH C-623/17 (Privacy International).

7 Ausgewählte Literatur

Nachfolgend wird ein Auszug aus der bisher recherchierten einschlägigen Literatur wie auch zur allgemeinen Literatur über die dazugehörigen einschlägigen Rechtsgebiete wiedergegeben.

Appl, Netz- und Informationssicherheit im Lichte der NIS-Richtlinie (Master-Thesis an der Universität Wien 2017)

Anderl/*Heußler*/*Mayer*/*Müller* (Hrsg), NISG Netz- und Informationssystemsicherheitsgesetz (Manz 2019)

Calliess in *Calliess*/*Ruffert* (Hrsg), EUV/AEUV[5] (2016)

Federal Ministry of Defence/*Rehrl*, Handbook on Cybersecurity <https://www.bundesheer.at/pdf_pool/publikationen/hb_on-cyber-defence-2-auflage_web.pdf> (Stand 2019).

Haslinger, Rechtliche und organisatorische Aspekte neuer Meldepflichten im Bereich der Netz- und Informationssicherheit, jusIT 2017, 218

Jaeger/*Stöger* (Hrsg), Kommentar zu EUV und AEUV (Manz 2020)

Schneider, Meldepflichten im IT-Sicherheitsrecht, Datenschutz, Kritische Infrastrukturen und besondere IT-Dienste (Nomos Verlag 2017)

Öhlinger, Autonome Geltung und Vorrang des Unionsrechts in den Mitgliedstaaten aus der Sicht der österreichischen Verfassung, juridikum 2019, 146 (146)

Kristoferitsch/*Lachmayer*, Die NIS-Richtlinie und ihre österreichische Umsetzung im NIS-Gesetz , ecolex 2020, 74

Lengauer in *Mayer*/*Stöger* (Hrsg), EUV/AEUV Art 3 EUV Rz 9 (Stand 01.12.2012, rdb.at)

Leidenmühler in *Jaeger*/*Stöger* (Hrsg), EUV/AEUV Art 114 AEUV (Stand 1.10.2018, rdb.at)

Leisterer, Internetsicherheit in Europa, Internet und Gesellschaft 12 (2018)

Maciejewski/Ratcliff/Næss, Binnenmarkt: Allgemeine Grundsätze, <https://www.europarl.europa.eu/ftu/pdf/de/FTU_2.1.1.pdf> (Stand April 2020)

Maciejewski/Ratcliff/Næss, Der allgegenwärtige digitale Binnenmarkt, <https://www.europarl.europa.eu/ftu/pdf/de/FTU_2.1.7.pdf> (Stand April 2020)

Muri/*Unteregger*/*Griessner*, IT-Risiko in Banken – aufsichtsrechtliche Entwicklungen, ÖBA 2019, 719

Öhlinger, Autonome Geltung und Vorrang des Unionsrechts in den Mitgliedstaaten aus der Sicht der österreichischen Verfassung, juridikum 2019, 146 (146)

OV, Wo steht der digitale Binnenmarkt heute?, VIL 2018, 15

Saurugg, Smart Metering und mögliche Auswirkungen auf die nationale Sicherheit <https://www.cybersecurityaustria.at/images/pdf/smart_metering_und_moegliche_auswirkungen_auf_die_nationale_sicherheit.pdf> (Stand Juli 2011).

Tschohl/*Hötzendorfer*/*Quirchmayr*/*Huber*/*Hellwig*, Die NIS-Richtlinie und der rechtliche Rahmen von CERTs, in *Schweighofer*/*Kummer*/*Hötzendorfer*/*Sorge* (Hrsg), Trend und Communities der Rechtsinformatik: Tagungsband des 20. Internationalen Rechtsinformatik Symposions IRIS 2017 (OCG 2017) 543

Wetsch, Basiselemente zur Cybersicherheit im Finanzsektor - "G7 fundamental elements of cybersecurity for the financial sector", ZFR 2017/30

8 Zeitplan

Im Laufe des Jahres 2020 wurden bereits umfangreiche Vorarbeiten und Erhebungen durchgeführt. Die für das Doktorat erforderlichen Lehrveranstaltungen und Seminare wurden bereits zur Gänze absolviert. Da der Doktorand in seinem beruflichen Leben Österreich in EU-weiten und internationalen Gremien für die Sicherheit von Netz- und Informationssystemen, denen strategische Aufgaben zugewiesen sind, vertritt, konnte er in Ausübung seines Berufen bereits ein vertieftes und praktisches Verständnis zum Dissertationsthema erwerben. Aufgrund der infolgedessen erfolgten Befassung mit den für das Dissertationsthema maßgeblichen Rechtsdokumenten und des solcherart erworbenen umfangreichen Vorwissens verfolgt der Dissertant das Ziel, die Arbeit innerhalb von eineinhalb Jahren zu verfassen. Dabei sollen die einführenden Kapitel mitsamt der Darstellung der Regulierung von Cybersicherheit auf Unionsebene sowie der einzelnen relevanten Rechtsakte und Maßnahmen bis Ende des Jahre 2020 entstehen. Im ersten Halbjahr 2021 sollen die kompetenzrechtlichen Grundlagen des Unionsrecht und die Abgrenzungsfrage zur nationalen Sicherheit allgemein behandelt werden. Über den Sommer und im zweiten Halbjahr 2021 sollen sodann die jeweiligen Rechtsakte und Maßnahmen im Hinblick auf das oben beschriebene Spannungsfeld beleuchtet werden.