

HANNFRIED LEISTERER

Internetsicherheit in Europa

Internet und Gesellschaft

12

Mohr Siebeck

Internet und Gesellschaft

Schriften des Alexander von Humboldt Institut
für Internet und Gesellschaft

Herausgegeben von
Jeanette Hofmann, Ingolf Pernice,
Thomas Schildhauer und Wolfgang Schulz

12



Hannfried Leisterer

Internetsicherheit in Europa

Zur Gewährleistung der Netz-
und Informationssicherheit durch
Informationsverwaltungsrecht

Mohr Siebeck

Hannfried Ulrich Leisterer, geboren 1986; Studium der Rechtswissenschaften an der Freien Universität sowie Humboldt-Universität zu Berlin; DFG-Forschungsstudent am Graduiertenkolleg „Verfassung jenseits des Staates“; Kollegiat im Kompetenznetzwerk für das Recht der zivilen Sicherheit in Europa (KORSE) des Bundesministeriums für Bildung und Forschung und wiss. Mitarbeiter am Alexander von Humboldt Institut für Internet und Gesellschaft, Berlin; 2017 Promotion; Referendar am Kammergericht Berlin.

ISBN 978-3-16-155976-1 / eISBN 978-3-16-156266-2
DOI 10.1628/978-3-16-156266-2

ISSN 2199-0344 (Internet und Gesellschaft)

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliographie; detaillierte bibliographische Daten sind im Internet über <http://dnb.dnb.de> abrufbar.

© 2018 Mohr Siebeck Tübingen. www.mohrsiebeck.com

Das Werk einschließlich aller seiner Teile ist urheberrechtlich geschützt. Jede Verwertung außerhalb der engen Grenzen des Urheberrechtsgesetzes ist ohne Zustimmung des Verlags unzulässig und strafbar. Das gilt insbesondere für Vervielfältigungen, Übersetzungen, Mikroverfilmungen und die Einspeicherung und Verarbeitung in elektronischen Systemen.

Das Buch wurde von Gulde Druck in Tübingen gesetzt, auf alterungsbeständiges Werkdruckpapier gedruckt und gebunden.

Wenn die ökonomische und soziale Entwicklung nicht als unabänderliches Schicksal hingenommen, sondern als permanente Aufgabe verstanden werden soll, bedarf es einer umfassenden, kontinuierlichen sowie laufend aktualisierten Information über die wirtschaftlichen, ökologischen und sozialen Zusammenhänge. Erst die Kenntnis der relevanten Daten und die Möglichkeit, die durch sie vermittelten Informationen mit Hilfe der Chancen, die eine automatische Datenverarbeitung bietet, für die Statistik zu nutzen, schafft die für eine am Sozialstaatsprinzip orientierte staatliche Politik unentbehrliche Handlungsgrundlage.

– BVerfG 65, 1 (47) – Volkszählungsurteil

Vorwort

Die Juristischen Fakultät der Humboldt-Universität zu Berlin hat die vorliegende Arbeit im Mai 2017 als Dissertation angenommen. Literatur und Rechtsprechung sind bis zu diesem Zeitpunkt berücksichtigt.

Herrn Professor Dr. Dr. h.c. Ingolf Pernice danke ich sehr herzlich dafür, dass er die Arbeit betreut und mich seit der Zeit des Studiums gefördert hat. Nicht zuletzt seine positive Haltung dient mir immer als Vorbild.

Herrn Professor Dr. Matthias Ruffert danke ich für die zügige Erstellung des Zweitgutachtens.

Die Arbeit ist im Rahmen des mit Mitteln des Bundesministeriums für Bildung und Forschung geförderten Kompetenznetzwerks für das Recht der Zivilen Sicherheit in Europa (KORSE) entstanden. Für die großzügige Förderung bedanke ich mich sehr. Das Bundesministerium des Innern hat durch einen Druckkostenzuschuss die Veröffentlichung der Arbeit ermöglicht. Dafür bin ich ebenfalls dankbar.

Eingeflossen in die Arbeit ist der Austausch mit vielen Personen. Ihnen schulde ich Dank für die Begegnungen, Erfahrungen und Erkenntnisse.

Viele Überlegungen verdanke ich meinen Kollegen Emma Peters, Dr. Adrian Haase sowie Dr. Sebastian Leuschner. In verschiedenen Abschnitten der Arbeit waren mir Marie-Luise Weckerling, Maria Rothämel, Hanna Soditt und Theresa Behrendt eine besondere Hilfe.

Für wertvolle Gespräche und die freundschaftliche Begleitung seit meinem Studium danke ich Rainer Ziemann und Kai Schmidt. Für die technische Expertise und Klärung technischer Fragen danke ich Richard Spreng. Steve Ritter vom Bundesamt für Sicherheit in der Informationstechnik danke ich für die freundlichen und geduldigen Gespräche, die mir den praktischen Hintergrund zu den rechtlichen Überlegungen deutlich machten. Für methodische Hinweise danke ich Herrn Professor Dr. Edmundt Brandt.

Nicht zuletzt möchte ich Dr. Karina Preiß sowie allen Kollegen am Alexander von Humboldt Institut für Internet und Gesellschaft (Berlin) für die wunderbare Zeit, die ich am Institut als Wissenschaftlicher Mitarbeiter hatte, danken.

Meinen Eltern, Ingeburg und Hanns-Ulrich Leisterer, und meiner Ehefrau Dorina ist diese Arbeit in Dankbarkeit gewidmet.

Hamburg im Januar 2018

Hannfried Leisterer

Inhaltsverzeichnis

§ 1 Einleitung	1
A. Internetsicherheit als Wissensproblem	1
B. Aufbau der Untersuchung	6
§ 2 Internetsicherheit und Informationsverwaltungsrecht	9
A. Schutzzielbezogene Eingrenzung der Internetsicherheit auf Netz- und Informationssicherheit	9
B. Infrastrukturbedingte Sicherheitsprobleme und Regulierbarkeit des Internets	13
I. Infrastruktur des Internets	13
1. Physikalische Infrastruktur	14
2. Logische Infrastruktur	15
II. Regulierbarkeit des Internets	16
C. Sicherheitsgewährleistung durch Informationsverwaltungsrecht	21
I. Epistemische Funktion des Informationsverwaltungsrechts	22
II. Generierung, Transfer und Distribution von Wissen und sicherheitsrelevanten Informationen	24
III. Daten, Information, Wissen und Kommunikation	26
§ 3 Generierung von Informationen über die Netz- und Informationssicherheit	31
A. Funktion der Informationsgenerierung für die Sicherheitsgewährleistung	31
I. Schutzpflicht zur Informationsgewinnung	32
II. Gewährleistungsverantwortung	34
1. Europäische Dimension	35
2. Grundgesetz	37
a) Internetinfrastruktur als grundrechtliches Schutzgut	37
b) Gewährleistungsverantwortung aus Art. 87f GG	39
B. Informations- und Wissensakteure	42

I.	Europäische Institutionen	44
	3. Europäische Agentur für Netz- und Informationssicherheit	44
	4. EU-Intelligence and Situation Centre	45
II.	Nationale Behörden	45
	1. Nationale Behörden für Netz- und Informationssicherheit	45
	a) Bundesamt für Sicherheit in der Informationstechnik	45
	b) Bundesnetzagentur	47
	c) Datenschutzbehörden	48
	2. Nachrichtendienstliche Einrichtungen	48
	a) Bundesnachrichtendienst	48
	b) Bundesamt für Verfassungsschutz	49
	3. Nationales Cyber-Abwehrzentrum	51
III.	Computer Security Incident Response Teams	52
C.	Rahmen der Informationsgenerierung	53
I.	Internetsicherheit im europäischen Primärrecht	54
	1. Raum der Freiheit, der Sicherheit und des Rechts	54
	2. Schutz personenbezogener Daten	56
	3. Europäisches Infrastrukturrecht	56
	4. Europäisches Katastrophenschutzrecht	57
	5. Europäisches Statistikrecht	58
	6. Gewährleistung der Netz- und Informationssicherheit als Angelegenheit des Binnenmarktes	58
II.	Sekundär- und einfachrechtlich erfasste Internetinfrastrukturen, Dienste, Anbieter und Verantwortliche sowie sonstige Quellen	60
	1. Telekommunikationsnetzbetreiber und -diensteanbieter sowie Over-the-Top-Kommunikationsdienste	60
	a) Europäisches Sekundärrecht und Einordnung im deutschen nationalen Recht	60
	b) Einordnung neuer Internetdienste wie Over-the-Top- Dienste	61
	2. Betreiber wesentlicher Dienste und kritischer Infrastrukturen	65
	3. Anbieter digitaler Dienste und Telemedien	69
	4. Verantwortliche im Sinne des Datenschutzrechts	70
D.	Rechtsgrundlagen zur Generierung von Informationen über die Sicherheit von Netzen und Informationssystemen	70
I.	Pflichten zur Beibringung von Informationen	74
	1. Sicherheitsnachweise	74

a)	Vorlage des Sicherheitskonzeptes von Telekommunikationsunternehmen	74
b)	Nachweis der Sicherheit von Betreibern wesentlicher Dienste bzw. kritischer Infrastrukturen	76
c)	Nachweis der Sicherheit von Anbietern digitaler Dienste	78
2.	Meldepflichten bei Sicherheitsverletzungen	80
a)	Betreiber von Telekommunikationsnetzen und Anbieter von Telekommunikationsdiensten	80
aa)	Anlass der Meldung	80
bb)	Inhalt der Meldung	84
b)	Betreiber wesentlicher Dienste und Kritischer Infrastrukturen	87
aa)	Anlass der Meldung	87
bb)	Inhalt der Meldung	90
c)	Anbieter digitaler Dienste	93
aa)	Anlass der Meldung	94
bb)	Konkretisierung durch Durchführungsakte der Kommission	95
cc)	Inhalt der Meldung	96
d)	Meldung auf freiwilliger Basis	97
3.	Meldepflicht bei Datenschutzverletzungen	99
a)	Meldepflicht im allgemeinen Datenschutzrecht	99
aa)	Anlass der Meldung	100
bb)	Inhalt der Meldung	101
b)	Meldepflicht im Telekommunikationsrecht	104
aa)	Anlass der Meldung	104
bb)	Inhalt der Meldung	106
II.	Befugnisse zur Generierung von Informationen	108
1.	Untersuchung von IT-Produkten und -Systemen	108
a)	Informationspflichten für Hersteller von Soft- und Hardware im öffentlichen Sicherheitsrecht	108
b)	Befugnis zur Untersuchung von IT-Sicherheitsprodukten	110
2.	Informationsbefugnisse im sicherheitsbezogenen Telekommunikationsrecht	111
a)	Sicherheitsbezogene Informationsbefugnis	111
aa)	Sicherstellung materiell-rechtlicher Sicherheitspflichten	112

bb)	Kriterium der Erforderlichkeit aus der Wissensperspektive	114
b)	Informationelle Generalbefugnis	120
3.	Nachrichtendienstliche Instrumente zur Informationsgewinnung	121
a)	Überwachung des Internetdatenverkehrs zur Erkennung von Cybergefahren	121
aa)	Strategische Fernmeldeaufklärung	122
bb)	Überwachung der Ausland-Ausland- Telekommunikation	126
b)	Besondere nachrichtendienstliche Mittel zum Schutz kritischer Infrastrukturen	130
c)	Nachrichtendienstliche Auskunftsverlangen	131
aa)	Auskunft über Bestands- und Nutzungsdaten bei Anbietern von Telemediendiensten	131
bb)	Auskunft über Strukturen der Telekommunikationsdienste und -netze	133
III.	Übernahme verwaltungsexternen Wissens	134
1.	Kooperation mit Privaten	135
a)	Vorschlag von technischen Sicherheitsstandards durch Branchenverbände	135
b)	Ausgestaltung des Verfahrens der Sicherheitsaudits, Prüfungen und Zertifizierungen	136
c)	Einbindung bei der Erstellung von Sicherheitskatalogen	136
d)	Einkauf von Expertise und Informationen über Sicherheitslücken	136
e)	Einsatz wissenschaftlicher Kommissionen	137
2.	Dysfunktion und Zulässigkeit der Informationsgenerierung über Private	137
a)	Wissensübernahme von Privaten im Bereich Sicherheit	138
b)	Zur Zulässigkeit der Inanspruchnahme Privater bei der Informations- und Wissensgenerierung	140
E.	Besondere Grenzen der Informationsgenerierung	142
I.	Meldepflichten und Selbstbelastungsschutz	142
1.	Verbot der Pflicht zur Selbstbelastung	142
2.	Kein absoluter Schutz vor Selbstbelastung	144
3.	Ausgleich der betroffenen Interessen	146
II.	Besondere datenschutzrechtliche Grenzen der Informationsgenerierung	149

1. Datenschutzrechtliche Relevanz der Netz- und Informationssicherheit	150
a) Datensicherheit im Verhältnis zum Datenschutz	151
b) Personenbeziehbarkeit von Maschinendaten	152
aa) Beispiel der IP-Adresse	153
bb) Personenbeziehbarkeit von IP-Adressen	154
2. Zur Rechtfertigung der Datenverarbeitung zum Zwecke der Netz- und Informationssicherheit	160
a) Datenverarbeitung durch Diensteanbieter und Infrastrukturbetreiber	160
aa) Verarbeitung datenschutzrechtlich geschützter Daten zur Gefahrenabwehr im Telekommunikationsrecht	161
bb) Verarbeitung datenschutzrechtlich geschützter Daten zur Gefahrenabwehr im Telemedienrecht und allgemeinen Datenschutzrecht	163
b) Datenverarbeitung durch NIS-Verwaltung	167
aa) Zur Rechtfertigung der Datenverarbeitung	167
bb) Grundsatz der Datenminimierung	170
cc) Zweckbindung und Regelungstiefe	173
III. Besondere Grenzen der Informationsgenerierung zum Schutz von Unternehmensgeheimnissen	179
1. Schutzbedarf von Unternehmensinformationen	180
2. Der öffentlich-rechtliche Schutz von Unternehmensinformationen bei Bestehen von Informationspflichten in der NIS-Verwaltung	180
a) Keine Anwendbarkeit des Datenschutzrechts auf juristische Personen	181
b) Schutz von Betriebs- und Geschäftsgeheimnissen	183
aa) Herleitung des Schutzes	183
bb) Beispiel der Sicherheitslücke	185
(1) Begriff der Sicherheitslücke	185
(2) Schutzvoraussetzungen	186
c) Besonderer Schutz für Betreiber kritischer Infrastrukturen im Rahmen von Meldepflichten	188
3. Schutz vor unbefugter Offenlegung durch das Verwaltungsgeheimnis	191
a) Beachtung der Verhältnismäßigkeit	191
b) Schutz durch das Verwaltungsgeheimnis	193
F. Zwischenergebnis	196

§ 4 Transfer von Informationen im Rahmen der europäischen Zusammenarbeit zur Gewährleistung der Netz- und Informationssicherheit	201
A. Funktion des Informationstransfers für die Sicherheitsgewährleistung	202
I. Kognitive Dimension des Europäischen Verwaltungsverbunds	202
II. Verwaltungskooperation im Bereich Sicherheit von Netz- und Informationssystemen	206
1. Europäisches Sicherheitsverwaltungsrecht als Informationsverwaltungsrecht	206
2. Informationskooperation zur Gewährleistung der Netz- und Informationssicherheit	208
B. Struktur des Informationsaustausches	209
I. Formen des europäischen Informationstransfers	209
1. Vielgestaltigkeit europäischer Informationsaustauschverfahren	210
2. Grundtypen europäischer Informationsaustauschmechanismen	212
II. Ausgestaltung der Informationszusammenarbeit durch die NIS-Richtlinie	213
1. Organisationsrechtliche Ausgestaltung	214
a) Strategischer Informationsaustausch in der Kooperationsgruppe	214
b) Operativer Informationsaustausch im CSIRTs- Netzwerk	215
c) Informationsaustausch außerhalb der NIS-Zusammenarbeit	215
2. Verfahrensrechtliche Ausgestaltung	215
a) Prävention durch Informations- und Wissensaustausch	216
aa) Sach- und Kontrollberichte	216
(1) Sachberichte über gemeldete Sicherheitsverletzungen	216
(2) Kontrollberichte über den Vollzug	218
(3) Telekommunikationsrechtliche Informationsbefugnis zur Erfüllung von Berichtspflichten	219
bb) Austausch von Erfahrung und bewährten Praktiken	220

(1) Austausch spezifischer Formen von Wissen über die Sicherheit	220
(2) Kooperationsgruppe als Wissensspeicher	222
cc) Konsultationspflichten	224
(1) Konsultation mit nationalen Strafverfolgungsbehörden	225
(2) Konsultation mit Datenschutzbehörden	227
(3) Konsultation als Teil des Notfallmanagements	229
b) Detektion von Gefahren durch Frühwarnmechanismus	231
aa) Rascher Austausch über Gefahren durch Frühwarnsysteme	232
bb) Frühwarnungen durch CSIRTs	232
c) Reaktion auf Sicherheitsvorfälle und Abschwächung von Risiken	235
aa) Horizontaler Informationsaustausch über Sicherheitsvorfälle	235
(1) Informationsaustausch in Deutschland	235
(2) Informationsaustausch zwischen den Mitgliedstaaten	237
bb) Horizontaler Informationsaustausch über Sicherheitsvorfälle mit vertikalen Bezügen	239
(1) Informationen zu einzelnen Sicherheitsvorfällen im CSIRTs-Netzwerk	239
(2) Informationen im Zusammenhang mit Sicherheitsvorfällen und über Computerkriminalität	242
cc) Reaktion auf einen Sicherheitsvorfall	244
(1) Austausch impliziten Wissens durch Übungen	244
(2) Koordinierte Reaktion	245
(3) Zusammenarbeit mit Datenschutzbehörden bei der Bearbeitung von Sicherheitsvorfällen bei wesentlichen Diensten	246
III. Förderung des Informationsaustausches	248
1. Grundsatz der loyalen Zusammenarbeit	248
a) Allgemeine Kooperationspflicht	249
b) Inhaltliche Anforderungen an auszutauschende Informationen	250
2. Rechtliche Sicherung des gegenseitigen Vertrauens	251
a) Vertrauen als Gelingensvoraussetzung der NIS-Informationskooperation	251

b) Konkrete Maßnahmen der Erwartungsstabilisierung	252
c) Umgang mit Ungewissheit als Gewissheit	254
3. Primärrechtliche Möglichkeiten der Stärkung des Wissenstransfers	254
a) Parallelität der mitgliedstaatlichen Informationsverarbeitung	254
b) Allgemeine Informationsbefugnis der Kommission	256
C. Besondere Grenzen des Informationstransfers	258
I. Grenzen des Informationstransfers durch den Datenschutz	258
1. Übermittlung nach Maßgabe des allgemeinen Datenschutzrechts	260
2. Übermittlung im Rahmen der Aufklärung von Cybergefahren zum Schutz kritischer Infrastrukturen	260
a) Übermittlung von Daten durch das Bundesamt für Verfassungsschutz	260
b) Übermittlung der im Rahmen der Fernmeldeaufklärung von Cybergefahren gewonnenen Daten	261
c) Übermittlung der im Rahmen der Ausland-Ausland- Fernmeldeaufklärung gewonnenen Daten	263
3. Besondere Zweckbindung für die Meldedaten beim BSI	264
II. Grenzen des Informationstransfers durch den Schutz unternehmensbezogener Daten	266
1. Anforderungen an den Austausch vertraulicher Informationen	268
2. Besondere Begrenzungen	270
a) Begrenzungen der ENISA und allgemeine unionsrechtliche Geheimhaltungspflicht	270
b) Begrenzungen der deutschen NIS-Behörden	271
aa) Weitergabe von Erkenntnissen aus Produkt- und Systemuntersuchungen an europäische NIS-Stellen	271
bb) Geringe Regelungsdichte zur Weitergabe vertraulicher Informationen durch die NIS-Behörden	272
III. Grenzen des Informationstransfers durch Organisationsrecht	275
1. Trennungsgebot und Informationsaustausch im Nationalen Cyber-Abwehrzentrum	275
a) Sicherheitsbehördliches Trennungsgebot	276
b) Reichweite des informationellen Trennungsprinzips	278
2. Unabhängigkeit der NIS-Behörde	280

a)	Stärkung der technischen Sicherheit durch Neutralität	280
b)	Unionsrechtliche Zulässigkeit weisungsfreier Räume	282
c)	Sachliche Rechtfertigung der Unabhängigkeit	284
aa)	Stärkung der Wissensfunktion durch Unabhängigkeit	284
bb)	Verfassungsrechtliche Einwände gegen organisationsrechtliche Unabhängigkeit	288
cc)	Veröffentlichung von Weisungen als Gestaltungsoption	290
IV.	Informationsverweigerungsrecht der Mitgliedstaaten zur Wahrung wesentlicher Sicherheitsinteressen	291
D.	Zwischenergebnis	294
§ 5	Distribution von Informationen über die Netz- und Informationssicherheit	299
A.	Funktion der Informationsdistribution für die Sicherheitsgewährleistung	300
I.	Sicherheit durch staatliche Informationstätigkeit	301
II.	Sicherheit durch Transparenz	305
1.	Begrenzung von Datenmacht am Beispiel des Datenschutzes	307
2.	Argumente aus der Kryptokontroverse gegen exklusives staatliches Wissen	308
3.	Transparenzgedanke in der Debatte um Freie Software	311
III.	Sicherheit durch Informationszugang und -weiterverwendung	313
B.	Aktives Informationshandeln	315
I.	Öffentlichkeitsbezogene Informationstätigkeit	315
1.	Allgemeine Anforderungen an Publikumsinformationen	316
a)	Erfordernis der Rechtsgrundlage	316
b)	Qualität der Information	317
2.	Aufklärung zur Sensibilisierung für Sicherheitsprobleme	318
a)	Berichte der NIS-Behörden	319
aa)	Bericht des Bundesamts für Sicherheit in der Informationstechnik	319
bb)	Bericht der Bundesnetzagentur	321
cc)	Bericht der Datenschutzaufsichtsbehörde	322
b)	Stellungnahmen der Datenschutzaufsichtsbehörden	323
c)	Information über Sicherheitsvorfälle	324

aa)	Unterrichtung über Sicherheitsverletzungen	324
(1)	Sicherheitsverletzungen bei Telekommunikationsunternehmen	324
(2)	Fehlende Rechtsgrundlage für das BSI	326
bb)	Veröffentlichung einer Verletzung des Schutzes personenbezogener Daten durch Verantwortliche	328
3.	Veröffentlichung von Sicherheitsanforderungen und Untersuchungsergebnissen	329
a)	Veröffentlichung des Sicherheitskatalogs	330
b)	Veröffentlichung der Erkenntnisse aus Produkt- und Systemuntersuchungen	330
4.	Warnungen vor Sicherheitslücken und sonstigen Gefahren	332
a)	Voraussetzungen und Reichweite des Tatbestands	332
b)	Responsible Disclosure als ermessensleitende Strategie für die Warnung vor Sicherheitslücken	333
5.	Empfehlungen von Sicherheitsmaßnahmen und Sicherheitsprodukten	337
a)	Empfehlung bei Gefahrenverdacht	337
b)	Problem eigendynamischer Verstärkungseffekte	340
c)	Besondere Anforderungen an die Informationsdarstellung	341
II.	Individualbezogene Informationstätigkeit	345
1.	Betreiber kritischer Infrastrukturen	345
2.	Information in informellen Zusammenschlüssen	347
3.	Datenschutzrechtlich Verantwortliche und Betroffene einer Verletzung	349
a)	Betroffene einer Datenschutzverletzung	349
b)	Individuelle Beratung in Fragen der Datensicherheit	350
C.	Reaktives Informationshandeln	351
I.	Grundrecht auf Informationszugang	351
1.	Grundsatz der Offenheit und Recht auf Zugang zu Dokumenten im Unionsrecht	352
2.	Verankerung der Informationsfreiheit im Grundgesetz	353
II.	Zugang zu Informationen bei den NIS-Stellen	354
1.	Zugang bei europäischen NIS-Stellen	355
a)	Reichweite der Transparenz-Verordnung und Verhältnis zur NIS-Richtlinie	355
b)	Zugang zu Informationen am Beispiel der ENISA	357
2.	Zugang bei nationalen NIS-Stellen	358
a)	Bundesamt für Sicherheit in der Informationstechnik	359

b) Bundesnetzagentur	359
c) Kein Zugang zu Informationen bei Nachrichtendiensten	360
III. Informationsinteresse und Geheimhaltungsbedürfnis	360
1. Reichweite der Ausnahme vom IFG im BSIG	362
2. Auswirkungen der allgemeinen Ausnahmen vom Informationszugangsrecht	364
a) Belange der Sicherheit	365
b) Geheimnisschutz auf Grund öffentlicher Belange	366
c) Schutz vertraulich erhobener und übermittelter Informationen	367
d) Datenschutz	368
e) Betriebs- und Geschäftsgeheimnisse	369
f) Geistiges Eigentum	370
3. Pauschalabwägung der Interessen im BSIG	371
IV. Bereitstellung und Verwendung der Informationen	374
1. Anforderungen an die Informationen	375
2. Weiterverwendung zugänglicher Informationen	376
3. Maschinenlesbare Bereitstellung von Daten	378
D. Zwischenergebnis	380
§ 6 Zusammenfassende Bewertung und Fazit	385
A. Beitrag des Informationsverwaltungsrechts zur Netz- und Informationssicherheit	385
I. Erkennung von Gefahren und systemischen Risiken	386
II. Europäisierte Informationskooperation auf Vertrauensbasis	387
III. Zugang zu und freie Weiterverwendung von generierten Informationen und produziertem Wissen als Teil der Sicherheitsgewährleistung	390
B. Intelligente Datenverarbeitung und Operationalisierung von Nichtwissen	391
Literaturverzeichnis	395
Sachregister	437

§ 1 Einleitung

A. Internetsicherheit als Wissensproblem

Das Internet vernetzt mit dem bislang dominierenden Internet-Protokoll weltweit Individuen und Dinge. Alle wesentlichen Bereiche und Funktionen in heutigen Gesellschaften sind abhängig von der Informations- und Kommunikationstechnologie Internet. Daten- und Informationsinfrastrukturen bilden die Nervenbahnen des gesellschaftlichen Lebens. Das Funktionieren des Internet hat mittlerweile essenzielle Bedeutung für den Einzelnen, die Gesellschaft, die Wertschöpfungsketten und die öffentliche Aufgabenerfüllung. Die Anzahl der Nutzer und Teilnehmer steigt und es kann davon ausgegangen werden, dass das Internet für Jahrzehnte die entscheidende Infrastruktur bleiben wird.

Ein Grundproblem, das es erschwert, die Sicherheit der das Internet bildenden Netz- und Informationssysteme zu gewährleisten, ist Komplexität. Im Laufe der Entwicklung des Internets haben sich ein Maß an Komplexität und ein Grad an Kopplung desselben mit sozialen Prozessen entwickelt, die für die Infrastruktur ebenso wie für Nutzer zur Gefahr werden können.¹ Komplex sind sowohl die Informationsinfrastrukturen als auch die Angriffe auf sie. Im Zuge von Innovationszyklen und damit einhergehenden technologischen Neuentwicklungen sowie inkrementellen Verbesserungen verringert sich die Systemkomplexität keineswegs, sondern erhöht sich tendenziell weiter. Angreifer sind innovativ und professionell und arbeiten mit leicht bedienbaren Werkzeugen. Vernetzte Systeme sind kaum isolierbar, IT-Sicherheitsumgebungen können durch manipulierte Hardware und Software kompromittiert werden und sind damit inhärent unsicher. Verschlüsselungen können schnell mit mittlerweile häufig angewandten Brute-Force-Methoden umgangen werden. Die Sicherheitslage erscheint auch deshalb als prekär, weil es als unmöglich gilt, Software zu schreiben, die keine Fehler enthält. Je nach Programmqualität liegt die Fehler-

¹ *Palfrey/Gasser*, Interop – The Promise and Perils of highly interconnected systems, 2012, S. 76; *Schneier*, Complexity the Worst Enemy of Security, CWHK, 17.12.2012; *King*, Science of Cyber-Security, Mitre Report JSR-10-102, 2010, S. 14; vgl. Erwägungsgrund 1 VO (EU) Nr. 526/2013; *Brown*, Research Handbook on Governance of the Internet, 2013, S. 152; Bundesministerium des Innern, Cyber-Sicherheitsstrategie für Deutschland, 2016, S. 7.

quote zwischen 5 und 0,0001 Prozent.² Bei anspruchsvolleren Programmen mit mehreren hundert Millionen Zeilen Code kann dies zu einer beträchtlichen Quantität an Angriffswegen führen. Die Anzahl an Sicherheitslücken, die für einen Hack ausgenutzt werden können, liegt bei ungefähr 5 Prozent. Hinzu kommt, dass nicht nur stetig neue Sicherheitslücken, sondern ebenso konstant neue Exploittechniken geschaffen werden, also Techniken, die dazu dienen, Sicherheitslücken auszunutzen.³

Die Ubiquität und gleichzeitige Interdependenz von Informationstechnologien lassen Kaskadeneffekte als ein realistisches und nicht zu ignorierendes Szenario erscheinen.⁴ Denn nicht nur ermöglicht die Vernetzung Angriffe aus großer Entfernung, sondern sie steigert die Anfälligkeit und Verwundbarkeit von Systemen und potenziert damit Angriffsvektoren.⁵

Aufgrund der Dynamik der digitalen Entwicklung lassen sich die Folgen von Störungen kaum vorhersagen. Denn zur Eigenschaft komplexer Systeme gehört auch, dass sich das Verhältnis von Ursache und Wirkung aufgrund des Grades der Abhängigkeiten und Wechselwirkungen der die Systeme konstituierenden Elemente nicht linear verhält und demnach Kausalverläufe keineswegs immer überschaubar und transparent sind.⁶ Kleine Veränderungen können disproportional Auswirkungen haben. Das Ideal von Voraussage und Kontrolle ist weitgehend unerreichbar, da die Faktoren, von denen individuelle Ereignisse abhängen, in der Regel so zahlreich sind, dass sie in ihrer Gesamtheit nicht ermittelt werden können.⁷ In der Cyber-Sicherheitsforschung wird aus diesem Grund zunehmend nach analogen Bewältigungsstrategien und erklärenden Mustern in

² *Gaycken*, Cybersecurity in der Wissensgesellschaft, in: Daase/Engbert/Junk (Hrsg.), *Verunsicherte Gesellschaft – Überforderter Staat*, 2013, S. 109 (115 f.).

³ *Gaycken/Lindner*, Zero Day Governance – A(n Inexpensive) Solution to the Cyber Security Problem, in: *Cyber Dialogue – What is Stewardship in Cyberspace*, 2012, S. 13.

⁴ *Petermann/Bradke/Lüllmann/Poetzsch/Riehm*, Was bei einem Blackout geschieht, Studien des Büros für Technikfolgen-Abschätzung beim Deutschen Bundestag, 2011, S. 31, 70 ff.

⁵ Vgl. Bundesamt für Sicherheit in der Informationstechnik, *Die Lage der IT-Sicherheit in Deutschland 2015*, 2015, S. 35; Kommission, *Impact Assessment accompanying the Proposal for a NIS Directive*, SWD(2013) 32 final, S. 13; Bundeskriminalamt, *Cybercrime*, Bundeslagebild, 2014, S. 12 ff.

⁶ Vgl. BVerfGE 120, 274 (306): „Informationstechnische Systeme haben mittlerweile einen derart hohen Komplexitätsgrad erreicht, dass ein wirkungsvoller sozialer und technischer Selbstschutz erhebliche Schwierigkeiten aufwerfen und zumindest den durchschnittlichen Nutzer überfordern kann.“

⁷ *von Hayek*, Die Theorie komplexer Phänomene, in: Kerber (Hrsg.), *Die Anmaßung von Wissen*, 1996, S. 281 (295); *Gaycken*, Cybersecurity in der Wissensgesellschaft, in: Daase/Engbert/Junk (Hrsg.), *Verunsicherte Gesellschaft – Überforderter Staat*, 2013, S. 109 (115 f.); *ders.*, Öffentliches Fachgespräch des Ausschusses Digitale Agenda des Deutschen Bundestages zum Thema IT-Sicherheit, A-Drs. 18(24)10, S. 3.

anderen Bereichen gesucht, die ebenfalls durch Komplexität gekennzeichnet sind. Wegen der Ähnlichkeit von Schadprogrammen mit pathogenen Infektionen werden etwa terminologische Anleihen bei der Epidemiologie genommen. So ist in der IT-Sicherheit von Viren, Würmern oder Infektionen die Rede.⁸

Dies zeigt, dass die Komplexität der technischen Basis und die Faktenkomplexität zugleich zu einer „hohen epistemischen Komplexität“ führen.⁹ Verschiedene Sichtweisen, Konzeptionierungen, Kategorisierungen, Differenzierungen, Klassifizierung und Kontextualisierungen mit Bezug auf technisch immer anspruchsvollere Netze, Systeme und Programme führen bei den Akteuren unweigerlich zu einer komplexeren Betrachtung der Probleme in der Internetsicherheit. Sie ist zwar auch erforderlich, um unzulässige oder unzuverlässige Simplifizierungen zu vermeiden. Allerdings führt sie auch dazu, dass selbst die Experten das Feld kaum mehr überblicken, Probleme erkennen, Schwierigkeiten priorisieren oder Verwundbarkeiten determinieren können.¹⁰

Da die Komplexität des Internets für menschliche Beobachter kaum mehr zu durchdringen ist, stellt sich die Netz- und Informationssicherheit für die Akteure als kognitive und epistemische Unsicherheit und damit als Herausforderung dar.¹¹

Organisationen verfolgen zur Mitigation von Gefahren für die Sicherheit grundsätzlich einen reduktionistischen Ansatz. Anders als es ein holistischer Ansatz erfordern würde, konzentrieren sich Unternehmen daher auf die IT-Sicherheit ihrer eigenen Systeme mit einem starken Fokus auf Kausalität. Somit gehören Schutzschichten wie Firewalls, Intrusion Detection Systems oder Anti-Viren-Programme zu verbreiteten Maßnahmen zur Abwehr von Gefahren für die IT-Sicherheit. Ein etablierter Ansatz im Risikomanagement ist außerdem das automatisierte Testen und Validieren der Systeme.¹² Problematisch an for-

⁸ Vgl. *Armstrong/Mayo/Siebenlist*, Complexity Science Challenges in Cybersecurity, 2009, S. 4; *Eckert*, IT-Sicherheit, 2000, S. 58 ff., 68 ff.

⁹ *Gaycken*, Cybersicherheit in der Wissensgesellschaft, in: *Daase/Engbert/Junk* (Hrsg.), Verunsicherte Gesellschaft – Überforderter Staat, 2013, S. 109 (117).

¹⁰ *Gaycken*, Cybersicherheit in der Wissensgesellschaft, in: *Daase/Engbert/Junk* (Hrsg.), Verunsicherte Gesellschaft – Überforderter Staat, 2013, S. 109 (120).

¹¹ Der Begriff „kognitiv“ wird für Vorgänge intellektueller Art verwendet, die sich innerhalb des Menschen abspielen, vgl. *Eberle*, Organisation der automatisierten Datenverarbeitung in der öffentlichen Verwaltung, 1976, S. 39, Fn. 31; *Dörner*, Die Logik des Mislingens – Strategisches Denken in komplexen Situationen, 11. Aufl. 2012, S. 61 f., *von Foerster*, The Curious Behavior of Complex Systems, in: *Linstone/Simmonds* (Hrsg.), Futures Research: New Directions, 1977, S. 104 (106 ff.), die veranschaulichen, dass Komplexität vor allem eine subjektive Größe ist, was heißt, dass die Wahrnehmung, ob eine Situation komplex ist oder nicht, von der jeweiligen Person abhängt. Kognitive Kompetenz kann aber in Erweiterung der rein anthropozentrischen Perspektive auch in Operationsformen und Organisationen manifestiert sein. Dazu unten unter § 3 B.

¹² Etwa durch Penetrationstests, siehe *Eckert*, IT-Sicherheit, 2014, S. 210.

malen Verfahren ist jedoch, dass selbst dann, wenn Problemstellungen in der Informatik in Logik, Mathematik und Algorithmen ausgedrückt werden können, nicht sichergestellt ist, dass sie vollständig konsistent oder in endlicher Zeit entscheidbar sind.¹³ Hinzu kommt das Problem der Informationsasymmetrien. Das adäquate Erkennen von Risiken und Gefahren für die Netz- und Informationssicherheit ist für kleine Einheiten wie Unternehmen sehr kostenintensiv. Infolge fehlender Investitionsanreize und Moral Hazard können epistemische Unsicherheiten das Niveau der Netz- und Informationssicherheit stagnieren oder sogar sinken lassen.¹⁴

Bei allgemeinerer Betrachtung wird deutlich, dass das Wissensproblem in der Cybersicherheit *pars pro toto* für die Wissensprobleme der vernetzten Informations- und Wissensgesellschaft steht.¹⁵ Bei diesen Gesellschaftsbeschreibungen handelt es sich um Bedeutungsträger, die den Komplexitätszuwachs einer Gesellschaft zusammenfassen.¹⁶ Es sind die „funktionsspezifischen Operationsweisen“ der gesellschaftlichen Bereiche, in denen Wissen wissenschaftlich organisiert und zum zentralen Faktor wird, die für moderne Gesellschaften diese übergreifenden Beschreibungen rechtfertigen.¹⁷ Die Karriere des Internets hat die allgemeine Paradigmenverschiebung, die zu einer Neuordnung in eine Informations- und Wissensverteilung führte, mitverursacht.¹⁸ Charakteristisch für die Wissensgesellschaft ist, dass wegen der Spezialisierung und Ausdifferenzierung der gesellschaftlichen Bereiche kein relevanter Akteur allein über

¹³ Zu diesem fundamentalen Problem *Sassaman/Patterson/Bratus/Shubina*, The Halting Problems of Network Stack Insecurity, login Vol. 36 (No. 6), 2011, 22 (22 f.). Ob sich das Problem zukünftig durch künstliche Intelligenz und Quantencomputing lösen lässt, sei hier dahingestellt.

¹⁴ Moral Hazard bezeichnet im Zusammenhang mit Internetsicherheit das Phänomen, dass sich private Betreiber von Netz- und Informationssystemen sich einer kostenintensiven Verantwortung für Sicherheit entziehen würden, weil sie auf eine staatliche Intervention im Falle von Sicherheitsvorfällen spekulierten. Dazu *Irion*, The Governance of Network and Information Security in the European Union, in: Krüger/Nickolay/Gaycken (Hrsg.), The Secure Information Society, 2013, S. 5 ff.; *Andersson/Malm*, Public-Private Partnership and the Challenge of Critical Infrastructure Protection, in: Dunn/Mauer (Hrsg.), International CIIP Handbook 2006, Vol. II, 2006, S. 139 (143); *Hämmerli/Renda*, Protecting Critical Infrastructure in the EU, 2010, S. 49 f.; vgl. *Bauer/van Eeten*, Telecommunications Policy 33 (2009), 706 (710 f.).

¹⁵ Vgl. zur wissenssoziologischen Perspektive auch *Werle/Schimank* (Hrsg.), Gesellschaftliche Komplexität und kollektive Handlungsfähigkeit, 2000, S. 12; *Roßnagel/Wedde/Hammer/Pordesch*, Die Verletzlichkeit der ‚Informationsgesellschaft‘, 2. Aufl. 1989, S. 28, 42, 46 ff.

¹⁶ Vgl. *Vesting*, Zwischen Gewährleistungsstaat und Minimalstaat. Zu den veränderten Bedingungen der Bewältigung öffentlicher Aufgaben in der „Informations- und Wissensgesellschaft“, in: Hoffmann-Riem/Schmidt-Abmann (Hrsg.), Verwaltungsrecht in der Informationsgesellschaft, 2015, S. 101 (107 ff.).

¹⁷ So *Weingart/Carrrier/Krohn* (Hrsg.), Nachrichten aus der Wissensgesellschaft, 2007, S. 38.

¹⁸ Vgl. *Hoeren*, NJW 1998, 2849 (2854).

entscheidungsrelevantes Wissen verfügt. Das handlungs- und entscheidungsrelevante Wissen ist stattdessen gesamtgesellschaftlich und in den Teilbereichen dezentral vorhanden, d. h., eine zentrale Stelle, welche die Informationen aggregiert vorrätig hält, existiert grundsätzlich nicht, auch nicht in den gesellschaftlichen Subbereichen.

Aus der Dezentralisierung des Wissens folgt, dass das entscheidungsrelevante Wissen für die Bewältigung öffentlicher Aufgaben problemorientiert zusammengetragen werden muss.¹⁹ Gleiches gilt für den Bereich der Internetsicherheit. Kollektiv besteht maßgebliches Wissen über den Zustand der Systeme. Vor allem nach der Privatisierung und Deregulierung der IKT-Infrastruktur ist das Wissen jedoch gesellschaftsweit verstreut.²⁰ So sind etwa Informationen über kritische IT-Schwachstellen und Sicherheitslücken, sofern überhaupt bekannt, auf verschiedene Unternehmen, Personen oder Behörden verteilt und nur fragmentiert vorhanden.

Komplexität hat als Problembegriff zwar Entlastungspotenzial. Doch sind komplexe Systeme nicht vorschnell mit komplizierten Systemen gleichzusetzen. Komplexität darf nicht zum Deckmantel für Resignation werden, indem mit der Unterstellung von gesellschaftlicher Selbstorganisation das Fehlen von Gestaltungsversuchen von vorneherein zu entschuldigen.²¹ Wird die Gewährleistung der Internetsicherheit als Wissensproblem aufgefasst,²² so stellt sich vor allem für den Staat als wissensbasierte Organisation²³ die Frage, wie das Recht mit diesem Problem umgeht. Unter der Prämisse, dass Rechtswissenschaft „nicht allein oder vorrangig als normtextorientierte Interpretationswissenschaft verstanden, sondern [...] als problemlösungsorientierte Handlungs- und Entscheidungswissenschaft konzipiert werden [muss]“,²⁴ ist danach zu fragen, welche rechtlichen Instrumente dazu beitragen können, Probleme zu lösen.

¹⁹ Vgl. *Wollenschläger*, Wissensgenerierung im Verfahren, 2009, S. 34 ff.; *Ladeur*, Postmoderne Rechtstheorie: Selbstreferenz – Selbstorganisation – Prozeduralisierung, 2. Aufl. 1995, S. 209 f.

²⁰ Siehe dazu die als Bangemann-Bericht bekannt gewordenen Empfehlungen vom 26.05.1994 an den Europäischen Rat von Korfu „Europa und die globale Informationsgesellschaft“, 1994.

²¹ Zum zeithistorischen Wandel des Begriffs Komplexität weg von einem, der dafür stand, Phänomene in ihrer Ganzheit zu erfassen, hin zu einem Problembegriff *Leendertz*, Das Komplexitätssyndrom. Gesellschaftliche Komplexität als intellektuelle und politische Herausforderung in den 1970er Jahren, MPIfG Discussion Paper 15/07.

²² Im Kontext der Energieregulierung *Herzmann*, Konsultationen – Eine Untersuchung von Prozessen, kooperativer Maßstabskonkretisierung in der Energieregulierung, 2010, S. 33 ff.

²³ *Voßkuhle*, Das Konzept des rationalen Staates, in: Schuppert/Voßkuhle (Hrsg.), Governance von und durch Wissen, 2008, S. 13 (16); vgl. *Schulz*, Rewi 3 (2012), 330 (330).

²⁴ *Hoffmann-Riem*, Regulierungswissen in der Regulierung, in: Bora/Henkel/Reinhard, Wissensregulierung und Regulierungswissen, 2014, S. 135 (138).

Die vorliegende Arbeit nimmt das geschilderten Wissensproblem zum Anlass zu untersuchen, wie das Recht zur Lösung des Problems der Internetsicherheit beitragen kann. Die These lautet, dass das Informationsverwaltungsrecht mit seiner epistemischen Funktion zur Bewältigung des Wissensproblems einen Beitrag zur Gewährleistung der Sicherheit von Netz- und Informationssystemen in der Europäischen Union zu leisten vermag. Im Nachfolgenden wird untersucht, mit welchen informationsverwaltungsrechtlichen Instrumenten zur Initiierung, Strukturierung und Organisation von Informationen und Wissen dieser Beitrag zur Internetsicherheit geleistet werden könnte.

B. Aufbau der Untersuchung

In einem ersten Schritt werden Internetsicherheit und Informationsverwaltungsrecht einander zugeordnet (§ 2). Dabei wird der Untersuchungsgegenstand, die Gewährleistung der Internetsicherheit in Europa, zunächst begrifflich gefasst und losgelöst vom rechtlichen Kontext in seinen technischen Eigenschaften betrachtet. Doch ohne Theorie bleiben die Fakten ohne Aussagekraft. Nach der Betrachtung der technischen Dimension werden daher die extrajuristische Dimension des Wissensproblems und die epistemische Funktion des Informationsverwaltungsrechts entfaltet, um herauszuarbeiten, wie Recht als Steuerungsfaktor – Steuerung verstanden als indirekter Einfluss hinsichtlich eines Ziels und nicht etwa im Sinne der Beherrschung eines Zustands oder einer linearen Einwirkung – im Kontext des Internets Wirkung in der Sicherheitsgewährleistung entfalten kann. Zur weiteren Bestimmung des Beitrags des Informationsverwaltungsrecht unterscheidet die Untersuchung, dem Informationszyklus der administrativen Informationsverarbeitung folgend, Generierung, Transfer und Distribution sicherheitsrelevanter Informationen durch die informationsverarbeitende Administrative.

Die Generierung von Informationen über die Internetsicherheit ist grundlegend für die Erkenntnisgewinnung durch die Verwaltung (§ 3). Durch die Bestimmung der Reichweite der verfassungsrechtlichen Pflicht zur Informationsgenerierung und des die Akteure bestimmenden Organisationsrechts sowie die Betrachtung der rechtlichen Regelungen zur Generierung von sicherheitsbezogenen Informationen kann nachvollzogen werden, ob und welche Informationen bei den jeweiligen privaten Betreibern und Anbietern erhoben werden können. Diese Untersuchung lässt Aussagen darüber zu, in welchem Ausmaß das Wissensproblem durch Recht berücksichtigt und abgebildet wird und inwieweit dies noch eingefordert werden muss. Die Bewertung der Wirksamkeit der informationsverwaltungsrechtlichen Instrumente hängt auch davon ab, inwieweit das

Recht Grenzen kalkulierten Nichtwissens setzt. Besondere Grenzen werden hinsichtlich des Selbstbelastungsschutzes, des Datenschutzes und des Schutzes unternehmensbezogener Daten identifiziert.

Nach der Betrachtung der Generierung von Informationen wendet sich der Blick auf den Transfer von Informationen, d. h. auf die Weitergabe von Informationen im Rahmen der europäischen Kooperation im Bereich der Netz- und Informationssicherheit (§ 4). Dabei zeigt sich, dass die Union auch und gerade in sicherheitsbezogenen Politikbereichen auf Informationskooperation angewiesen ist, um handlungs- und entscheidungsrelevantes Wissen zu generieren und so Kompetenz- und Vollzugsdefizite im Bereich der Netz- und Informationssicherheit auszugleichen. Die Richtlinie (EU) 2016/1148 zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union (NIS-Richtlinie) bezweckt, einen Rahmen für die Zusammenarbeit auf europäischer Ebene zu schaffen, und steht daher im Zentrum der Untersuchung des grenzüberschreitenden Informationstransfers. Besondere Begrenzungen für den Informationsfluss können neben dem Schutz von personenbezogenen und unternehmensbezogenen Daten aus dem Organisationsrecht folgen.

Die Generierung und der Transfer von Informationen dienen den nationalen und europäischen Informationsbedürfnissen der Verwaltung. Da vor allem Unternehmen und Bürgerinnen und Bürger als Hersteller, Anwender und Nutzer von Produkten und Systemen im Bereich der IT-Sicherheit auf eine funktionierende Internetinfrastruktur angewiesen sind, stellt sich die Frage, wie die durch die Verwaltung erhobenen Informationen und wie das so geschaffene Wissen weitergehend zur Sicherheitsgewährleistung genutzt werden kann. Da die Verfolgung von Individualinteressen durch unterschiedliche Eigenrationalitäten, Verhaltensmuster und Erfahrungsbestände eine entscheidende Schubkraft zur Verwirklichung von Gemeinwohl ist, wird schließlich untersucht, ob und wie die gesammelten Informationen durch Distribution, d. h. durch rechtliche Informationsbeziehungen der Verwaltung zu Privaten, in der Gewährleistung der Internetsicherheit fruchtbar gemacht werden können (§ 5). Zugrunde gelegt wird dabei die Annahme, dass das Informationshandeln des Staates nicht nur dem demokratischen Partizipationsgedanken verpflichtet ist, sondern darüber hinaus auch den gewandelten kognitiven Bedingungen der Gesellschaft.

Wegen der technischen Konvergenz und der mitunter einheitlichen Gefahren für die Netz- und Informationssicherheit können bestimmte Regelungsmaterien nicht immer auseinandergelassen werden. So kann die zivile Sicherheit nicht als streng von der militärischen Sicherheit des Internets getrennt erfasst werden. Die Untersuchung beschränkt sich indes auf die Aspekte der zivilen Sicherheit, zumal in der europäischen NIS-Kooperation ein Informationsaustausch mit militärischen Stellen nicht ausdrücklich vorgesehen ist. Sicherheit in der Informa-

tionstechnik wird zudem zu wichtigen Teilen präventiv durch das Polizeirecht und repressiv durch das Strafrecht und Strafverfolgungsrecht verfolgt. Diese Materien sind zum einen schon vielfach untersucht worden und zum anderen würden die legislativen Entwicklungen hier eigene monografische Behandlungen rechtfertigen.²⁵ Gegenstand der Arbeit ist daher der sich auf europäischer Ebene entwickelnde Bereich der Netz- und Informationssicherheit außerhalb der Abwehr polizeirechtlicher Gefahren und der Strafverfolgung.²⁶ Soweit informationsrechtliche Schnittstellen hinsichtlich der Datenflüsse der NIS-Zusammenarbeit zu Stellen relevant werden, die Daten zu Zwecken der Polizei- und Strafverfolgung verarbeiten, werden diese Rechtsbereiche in die Untersuchung mit einbezogen.

²⁵ Vgl. *Saloven/Grant/Hanell/Makai/Hansen/Belevicius/Pohnitzer*, Study on the status of information exchange amongst law enforcement authorities in the context of existing EU instruments, 2010, S. 84 f.

²⁶ Die Cybersicherheitsstrategie der Europäischen Union, JOIN(2013) 1 final, S. 20, teilt das „Thema der Cybersicherheit“ in drei zentrale Bereiche auf, für die unterschiedliche Rechtsrahmen gelten. Neben der Netz- und Informationssicherheit sind dies die Strafverfolgung und die Verteidigung. Im Sinne dieser Strategie konzentriert sich die Arbeit auf Rechtsfragen des erstgenannten Bereichs.

§ 2 Internetsicherheit und Informationsverwaltungsrecht

Die Untersuchung des Beitrags des Informationsverwaltungsrechts zur Internetsicherheit in Europa erfordert wegen der begrifflichen Unschärfe eine eingrenzende Bestimmung des Begriffs der Internetsicherheit (A.). Eine kurze Skizzierung der Funktionsweise des Internets und der tatsächlichen wie rechtlichen Grenzen seiner Regulierbarkeit (B.) sollen zu der Frage leiten, wie Informationsverwaltungsrecht zur Lösung des Wissensproblems und damit zur Gewährleistung der Internetsicherheit in Europa beitragen kann (C.).

A. Schutzzielbezogene Eingrenzung der Internetsicherheit auf Netz- und Informationssicherheit

Der Begriff der Internetsicherheit ist aufgrund seiner verschiedenen Verwendungsmöglichkeiten unscharf. Gemeint sein kann die Sicherheit des Internets (Internet als Schutzobjekt), die Sicherheit im Internet (Internet als Medium zur Übertragung rechtswidriger Inhalte) oder die Sicherheit vor dem Internet (Internet als Angriffsmittel).¹ Der im Kontext von Internet und Sicherheit verwendete

¹ Grundsätzlich können je nach Typ des Angriffs auf eine NIS-Infrastruktur und der Angreifer die Begriffe Cyberkriminalität, Cyberspionage, Cybersabotage oder Cyberkrieg abgegrenzt werden. Dabei geht es um Verstöße gegen Vermögensrechte im weiten Sinne, um Einbrüche in fremde Datenbanken staatlicher oder nicht staatlicher Unternehmen und um staatliche Versuche, Interessen internetbasiert durchzusetzen, *Bendiek*, Europäische Cybersicherheitspolitik, 2012, S. 7. Unter den Bedrohungen mit geringem bis mittlerem Schadenpotenzial werden weiter Formen des Cyberaktivismus und Cybervandalismus diskutiert, *Chiesa/Ducci/Ciappi*, Profiling Hackers, 2009; *Dunn Caveltly*, Cyber(Un)Sicherheit: Grundlagen, Trends und Herausforderungen, in: Schieren (Hrsg.), Neue Medien, alte Fragen? Das Internet in der Politik, 2012, S. 66 ff. So bezieht sich Cyberkriminalität eher auf Verstöße gegen Eigentums- und Vermögensrechte von Privaten, während Cyberspionage Einbrüche in Datenbanken von staatlichen und nicht staatlichen Unternehmen durch fremde Staaten beschreibt. Unter Cyberwar kann der Versuch eines Staates verstanden werden, einen anderen Staat nachhaltig zu schädigen, vgl. *Robinson/Disley/Potoglou/Reding/Culley/Penny/Botterman/Carpenter/Blackman/Millard*, Feasibility Study for a European Cybercrime Centre,

Begriff der Cybersicherheit ist nicht wesentlich schärfer. Er steht eher in einem sicherheitspolitischen Zusammenhang und verweist auf die Gesamtheit der Politiken, Organisationen und Verfahren, die auf die Gewährleistung der Sicherheitseigenschaften von Informations- und Telekommunikationsinfrastrukturen gerichtet sind.² Im europäischen Primärrecht findet sich lediglich der denkbar weite kompetenzrechtliche Begriff der Computerkriminalität in Art. 83 Abs. 1 UAbs. 2 AEUV aus dem Politikbereich des Raums der Freiheit, der Sicherheit und des Rechts (Art. 67 ff. AEUV). Dort umfasst der Kriminalitätsbereich das Internet sowohl als Angriffsobjekt als auch als Tatmittel, d. h., auch inhaltsbezogene Straftaten wie Aussagedelikte oder Straftaten gegen das geistige Eigentum, die mittels Computersystemen begangen werden, sind erfasst.³ In Ermangelung eines im europäischen Primärrecht verankerten Begriffs der Internetsicherheit ist es für die weitere Operationalisierung des Begriffs erforderlich, eine schutzzielbezogene Eingrenzung vorzunehmen.

Als Ansatzpunkt für die schutzzielbezogene Eingrenzung kann der Begriff der IT-Sicherheit herangezogen werden. Zwar besteht ein abgeschlossenes Rechtsgebiet der IT-Sicherheit nicht und der Bereich zeichnet sich durch verstreute Einzelregelungen aus.⁴ Eine Definition der IT-Sicherheit findet sich jedoch im BSIG, dessen § 2 Abs. 2 lautet: „Sicherheit in der Informationstechnik [...] bedeutet die Einhaltung bestimmter Sicherheitsstandards, die die Verfügbarkeit, Unversehrtheit oder Vertraulichkeit von Informationen betreffen, durch Sicherheitsvorkehrungen 1. in informationstechnischen Systemen, Komponenten oder Prozessen oder 2. bei der Anwendung von informationstechnischen Systemen, Komponenten oder Prozessen.“ IT-Sicherheit bezieht sich damit auf die in der Vorschrift genannten Schutzziele, also die Verfügbarkeit, Unversehrtheit im Sinne von Integrität und Vertraulichkeit von Informationen, die elektronisch gespeichert sind oder derart verarbeitet werden.⁵ Diese Schutzziele wer-

2012, S. 17–55. Neben Vermögenswerten kann auch die staatliche Sicherheit ein gefährdetes Rechtsgut sein. Es lassen sich für die NIS neben anthropogenen Gefahren auch naturgegebene Gefahrenquellen anführen, *Saurugg*, Die Netzwerkgesellschaft und Krisenmanagement 2.0, 2012, S. 74.

² ITU, Definition of cybersecurity, ITU-T X.1205, abrufbar unter: <http://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx>.

³ *Vogel/Eisele*, in: Grabitz/Hilf/Nettesheim (Hrsg.), AEUV/EUV, 57. Aufl. 2015, Art. 83 AEUV, Rn. 62; siehe auch das Übereinkommen des Europarates über Computerkriminalität vom 23.11.2011 (*Cybercrime Convention*), BGBl. 2008 II S. 1242, 1243, 2010 II S. 218, einschließlich des Zusatzprotokolls vom 28. Januar 2003 betreffend die Kriminalisierung mittels Computersystemen begangener Handlungen rassistischer und fremdenfeindlicher Art, BGBl. 2011 II S. 290, 291, 843.

⁴ Vgl. *Schmidl*, NJW 2010, 476 (477); *Spindler*, MMR 2008, 7 (8 ff.).

⁵ *Heckmann*, MMR 2006, 280 (281).

Sachregister

- Anbieter
 - digitale Dienste 69, 78
 - Telekommunikationsdienste 60, 74, 161
 - Telemedien 69, 163
- Ausland-Ausland-Telekommunikation 126 ff., 199, 263 f.
- Behavioral Law and Economics 341
- Berichte 216 ff., 319 ff.
- Betreiber
 - kritische Infrastrukturen 65, 76, 260 ff., 345 f.
 - wesentliche Dienste 65
 - Telekommunikationsnetze 60, 74, 161
- Betriebs- und Geschäftsgeheimnisse, Schutz von 183 ff., 369 ff.
- Bewährte Praktiken 220 ff.
- Beweisverwertungsverbot 146 ff.
- Binnenmarkt 58 ff., 65, 201, 205 f., 272, 293, 331, 388 f.
- Bundesamt für Bevölkerungsschutz und Katastrophenhilfe 47, 51, 229
- Bundesamt für Sicherheit in der Informationstechnik 45, 359
- Bundesamt für Verfassungsschutz 49, 260
- Bundesnachrichtendienst 48, 360
- Bundesnetzagentur 47, 321, 359
- Computerkriminalität 122, 242 f.
- Computer Security Incident Response Teams (CSIRTs) 52 f.
- CSIRTs-Netzwerk 215, 239 ff.
- Cybersicherheit, *siehe* Netz- und Informationssicherheit
- Darstellung von Informationen 341 ff.
- Daseinsvorsorge 34 ff., 40
- Datenschutz
 - europäisches Primärrecht 56
 - und Gefahrenabwehr 160 ff.
 - Zweckbindung 173 ff., 264 f.
 - Grenzen der Informationsverarbeitung 149 ff., 258 ff., 368 f.
- Datenschutzbehörde 48, 246 f., 322 ff.
- DE-CIX 15, 125, 129
- Empfehlungen 77, 221, 228, 244, 316, 330, 333, 337 ff., 344
- Epistemische Unsicherheit 3 f., 393
- Erfahrung 28, 103, 121, 134, 137, 203, 216, 219 ff., 228, 231, 234, 241, 245, 252, 348
- EU-Intelligence and Situation Centre 45, 263
- Europäische Agentur für Netz- und Informationssicherheit (ENISA) 44, 270, 357 f.
- Europäisches Infrastrukturrecht 56 f.
- Europäisches Katastrophenschutzrecht 57 f.
- Europäisches Statistikrecht 58
- Europäisches Zentrum zur Bekämpfung der Cyberkriminalität (EC3) 225 f.
- Fernmeldeaufklärung 122 ff., 163 f.
- Freie Software 311 ff.
- Frühwarnungen 53, 91, 175, 231 ff., 246, 389
- Geheimnisschutz 366 f.
- Geistiges Eigentum 19, 370
- Generalbefugnis, informationelle 120
- Gewährleistungsverantwortung 34 ff., 39 ff., 64, 115, 196, 303 f., 373, 386
- Grundsatz der loyalen Zusammenarbeit 248 ff.

- Informationsdarstellung 341 ff.
 Informationssicherheit, *siehe* Netz- und Informationssicherheit
 Informationssysteme 206 ff., 213, 222 ff.
 Informationsverwaltungsrecht 22
 – epistemische Funktion 6
 – Distribution von Informationen 299 ff.
 – Generierung von Informationen 31 ff.
 – Transfer von Informationen 201 ff.
 Informationsverweigerungsrecht 291 ff.
 Informationszugangsfreiheit 351 ff.
 Informeller Informationsaustausch 51, 71, 135, 240, 243, 347
 Infrastruktur des Internets 13 ff., 56
 Intelligente Datenverarbeitung 391 ff.
 Internetregulierung 16 ff., 386
 IP-Adresse 153 ff.
 IT-Sicherheit, *siehe* Netz- und Informationssicherheit
 IT-Sicherheitsprodukte 110, 271, 330

 Komplexität 1 ff., 59, 111, 117 f., 134, 187, 202, 262, 284, 302, 310, 374
 Konsultation 215, 224 ff., 249
 Kooperationsgruppe 214 f., 222 f.
 Kryptokontroverse 308 ff.

 Lernen 28, 203 f., 219, 222, 234, 303, 335, 391 ff.
 Lernverbund 203, 255, 294, 388

 Maschinenlesbarkeit von Daten 108, 365, 378 ff.
 Mehrebenensystem 202 ff., 213
 Meldepflichten 194, 197 f., 200, 216, 237, 247, 265, 269, 308, 324, 346, 368, 373, 382, 386 f., 391
 – Telekommunikationsunternehmen 80 ff., 104 ff.
 – Betreiber wesentlicher Dienste und Kritischer Infrastrukturen 87 ff.
 – Anbieter digitaler Dienste 93 ff.
 – Datenschutzverletzungen 99 ff.
 – Selbstbelastungsschutz 142 ff.
 – datenschutzrechtliche Grenzen 149 ff.

 Nationales Cyber-Abwehrzentrum 51, 275 ff.

 Need-to-know-Prinzip 237, 389
 Need-to-share-Prinzip 237, 389
 Nemo-tenetur-Grundsatz, *siehe* Selbstbelastungsschutz
 Netz- und Informationssicherheit 9, 58, 60, 150 ff., 213 ff., 251 ff., 318 ff.
 Nichtwissen 33, 149, 199, 391 ff.
 NIS-Richtlinie 7, 16
 Nudging 303

 Open Government 306, 380
 Open Source, *siehe* Freie Software
 OTT-Dienste 60 ff., 196, 386

 Publikumsinformation 315 ff., 325 ff., 341, 380, 390

 Raum der Freiheit, der Sicherheit und des Rechts 54
 Responsible Disclosure 333 ff., 382, 390
 Risikovororge 33, 59

 Schutzpflicht 32 ff., 38, 64 f., 196, 303, 386
 Selbstbelastungsschutz 144 ff., 200
 Sicherheitsaudits 77 f., 136, 236, 363
 Sicherheitsnachweise 74 ff., 386
 Sicherheitskatalog 136, 330
 Sicherheitskonzept 74 ff., 86, 106 f., 119, 321
 Sicherheitslücken 2, 5, 14, 16, 47, 51, 81, 89, 93, 103, 107, 109, 136 f., 185 ff., 231, 239, 269, 271 f., 281 f., 309 ff., 332 ff.
 Sicherheitspflichten, materiell-rechtliche 70, 79, 112 f., 120 f., 135, 141, 143, 172, 189, 227, 273, 288
 Sicherheitsstandards 10, 46, 76, 78, 103, 135 f., 138, 197, 229, 325, 363
 Sicherheitsverletzung 80 ff., 216 ff., 219, 235, 238 ff., 247, 324 ff.
 Sicherheitsverwaltungsrecht 206 f., 302
 Sicherheitsvorfall 235 ff., 324 ff.
 Soft- und Hardware 108 f., 110 f., 198, 330 f.
 Statistik 174, 348
 Steuerung 6, 21, 24, 41, 115, 117, 175, 178, 218, 222, 224, 299, 301 f., 316, 327, 341, 390

- Strafverfolgung 225 ff., 237, 242, 277 f.,
290
- Strategische Fernmeldeaufklärung 49,
122 ff.
- Schwachstellen, *siehe* Sicherheitslücken
- Transparenz 26, 305 ff., 311 ff., 355 ff.
- Trennungsgebot 49, 275 ff.
- Trennungsprinzip, *siehe* Trennungsgebot
- Unabhängigkeit der NIS-Behörde 280 ff.
- Ungewissheit 117, 227, 254, 345, 392
- Unternehmensinformationen, Schutz von
179 ff., 266 ff., 369 f.
- Unterrichtung 212, 217, 237, 238, 265,
316, 324 ff.
- Urheberrecht 18, 370
- Verschlüsselung 1, 15, 188, 281, 308 ff.
- Vertrauen 251 ff., 387 ff.
- Verwaltungsexternes Wissen 134 ff.
- Verwaltungsgeheimnis 191 ff., 366
- Verwaltungsverbund 202 f., 205, 232, 251
- Warnung 47, 53, 91, 109, 110, 160, 303,
316, 327, 331, 332 ff., 382, 390
- Weiterverwendung von Informationen
376 ff.
- Wissen 1 ff., 26 ff., 38, 42 ff., 73, 86, 104,
114 ff., 118 f., 134 ff., 140, 167, 173, 185,
196, 199, 205, 216 ff., 220 ff., 227, 231,
234, 236, 247, 245, 252, 256, 278
- Zero-Day-Exploits, *siehe* Sicherheitslücken