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.

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

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 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 disproportionale 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 Misslingens – 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-Aßmann (Hrsg.), Verwaltungsrecht in der Informationsgesellschaft, 2015, S. 101 (107 ff.).

[17] So *Weingart/Carrier/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 Organisation[23] 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 auseinandergehalten 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*/*Hanel*/*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 Schadenspotenzial werden weiter Formen des Cyberaktivismus und Cybervandalismus diskutiert, *Chiesa/Ducci/Ciappi*, Profiling Hackers, 2009; *Dunn Cavelty*, 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