CAROLIN KEMPER

Cybergefahrenabwehrrecht

Beiträge zum Sicherheitsrecht und zur Sicherheitspolitik
20

Mohr Siebeck

Beiträge zum Sicherheitsrecht
und zur Sicherheitspolitik

herausgegeben von

Jan-Hendrik Dietrich, Klaus Ferdinand Gärditz
und Kurt Graulich

20

Carolin Kemper

Cybergefahrenabwehrrecht

Die staatliche Abwehr von Gefahren für die Cybersicherheit privater IT-Systeme

Mohr Siebeck

Carolin Kemper, geboren 1993; Studium zur Unternehmensjuristin (LL.B.) an der Universität Mannheim und der Jagiellonen-Universität Krakau; 2018 Erste Juristische Prüfung (Mannheim); Rechtsreferendariat und 2020 Zweites Staatsexamen am Landgericht Mannheim; Forschungsreferentin am Deutschen Forschungsinstitut für öffentliche Verwaltung Speyer; 2025 Promotion (Speyer); Postdoktorandin am Hasso-Plattner-Institut in Potsdam.
orcid.org/0000-0003-1790-0710

ISBN 978-3-16-200479-6 / eISBN 978-3-16-200480-2
DOI 10.1628/978-3-16-200480-2

ISSN 2568-731X / eISSN 2569-0922
(Beiträge zum Sicherheitsrecht und zur Sicherheitspolitik)

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliographie; detaillierte bibliographische Daten sind über *https://dnb.dnb.de* abrufbar.

Gedruckt auf alterungsbeständiges Papier.

Mohr Siebeck GmbH & Co. KG, Wilhelmstraße 18, 72074 Tübingen, Deutschland
www.mohrsiebeck.com, info@mohrsiebeck.com

Für Steve Blum

Vorwort

Die vorliegende Dissertation entstand zwischen 2021 und 2024 während meiner Tätigkeit als Forschungsreferentin am Deutschen Forschungsinstitut für öffentliche Verwaltung in Speyer und wurde im September 2025 von der Deutschen Universität für Verwaltungswissenschaften Speyer angenommen.

Die Arbeit berücksichtigt die aktuelle Rechtslage, insbesondere die Neufassung des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik seit der Umsetzung der NIS-2-Richtlinie. Literatur und Rechtsprechung habe ich bis zur Abgabe der Arbeit im Jahr 2024 ausgewertet. Wesentliche Quellen, insbesondere solche, die sich mit der NIS-2-Umsetzung befassen, sind seit der Abgabe ergänzt worden. Außerdem erfuhr die Arbeit einiges an Restrukturierung, um die Vorschläge des Zweitgutachtens aufzugreifen.

Herrn Professor Dr. Mario Martini danke ich vielmals dafür, dass er die Arbeit betreut und mich im Rahmen meiner Tätigkeit als Forschungsreferentin gefördert hat.

Herrn Professor Dr. Stefan Korte danke ich für die zügige Erstellung des Zweitgutachtens und ausdrücklich für seine hilfreichen Anmerkungen und weiterführenden Ideen, die das vorliegende Werk prägen und verbessert haben.

In diese Arbeit sind die Ideen, Gedanken und Impulse zahlreicher Personen eingeflossen, denen mein Dank für den inspirierenden fachlichen Austausch sowie die mentale Unterstützung gilt:

Besonders möchte ich meinen (ehemaligen) Kolleginnen und Kollegen am Forschungsinstitut für öffentliche Verwaltung danken, insbesondere Jonas Botta, Luci Haspinger, Martin Feldhaus, Rene Hermann, Thomas Kienle, Inken Kramme, Jonas Lange, Luise Lautenbach, Paul Seeliger und David Wagner. Danken möchte ich auch meiner ehemaligen Kollegin Beate Bukowski, insbesondere für das Lektorat dieser Arbeit.

Herzlich danken möchte ich auch Steve Ritter für die zahlreichen Ratschläge und kritischen Hinweise, die bis zum Schluss in die Arbeit eingeflossen sind.

Für die inhaltliche Unterstützung und wertvolle Expertise sei auch Sven Herpig (Interface) besonders hervorgehoben. Durch ihn erhielt ich Zugang zu interdisziplinären Perspektiven der aktiven Cyberabwehr.

Von besonderer Bedeutung war auch die Zusammenarbeit mit Nicolas Ziegler: Als Sparringpartner konnte ich mit ihm zentrale Denkansätze weiterentwickeln.

Mein Dank gebührt auch Max Petras und Victoria Guijarro Santos für das inspirierende Miteinander und den ständigen fachlichen wie persönlichen Rückhalt in unserer Promotionsgruppe.

Ebenso möchte ich Professorin Dr. Hannah Ruschemeier für ihre wertvollen Ratschläge in Karriere- und Fachfragen danken.

Nicht zuletzt danke ich auch meinem früheren Chef Herrn Professor Dr. Hans-Joachim Cremer. Er hat mich das „juristische Handwerkszeug" gelehrt und meine Leidenschaft für die Rechtswissenschaft geweckt.

Mein tiefer Dank richtet sich an Michael Kolain, der mich in den letzten fünf Jahren beruflich begleitet und geprägt hat.

An letzter – und wichtigster – Stelle möchte ich meiner Familie danken: Meine Eltern, Gabriele und Dr. Bernd-Michael Kemper, haben mich auf vielfältige Weise unterstützt, indem sie u. a. nach thematisch relevanten Fachartikeln Ausschau gehalten haben, von denen viele Eingang in diese Arbeit fanden. Die Promotionsphase war zudem intensiv geprägt von der Schwangerschaft und den ersten Lebensjahren meiner Tochter, Luna. Sie macht den Abschluss dieser Arbeit umso besonderer.

Diese Arbeit ist meinem Partner Steve Blum gewidmet: Er hat sie wie kein Zweiter geprägt – durch zahlreiche Diskussionen, Korrekturlesen, aber auch durch seine emotionale Unterstützung und Bestärkung.

Speyer, im November 2025 *Carolin Kemper*

Inhaltsverzeichnis

Teil II
Cybersicherheit durch Gefahrenabwehr

Teil III
Maßnahmen der Cybergefahrenabwehr

Teil IV
Organisation der Cybergefahrenabwehr

Abbildungsverzeichnis

Abkürzungsverzeichnis[1]

a. a. O.	am angegebenen Ort
a. E.	am Ende
a. F.	Alte Fassung
ABl.	Amtsblatt
AG KRITIS	Arbeitsgruppe Kritische Infrastrukturen
APT	Advanced Persistent Threat
ASOG Bln	Allgemeines Gesetz zum Schutz der öffentlichen Sicherheit und Ordnung in Berlin
AtG	Gesetz über die friedliche Verwendung der Kernenergie und den Schutz gegen ihre Gefahren
Aufl.	Auflage
AusschussDrs.	Ausschussdrucksache
AVwVMeldeVf	Allgemeine Verwaltungsvorschrift über das Meldeverfahren
AWV	Außenwirtschaftsverordnung
BaFIN	Bundesanstalt für Finanzdienstleistungsaufsicht
Bay., bay.	Bayern, bayerisch
Bbg., bbg.	Brandenburg, brandenburgisch
BBK	Bundesamt für Bevölkerungsschutz und Katastrophenhilfe
BeckOK	Beck'scher Online-Kommentar
BfDI	Bundesbeauftragte(r) für Datenschutz und Informationsfreiheit
BfV	Bundesamt für Verfassungsschutz
BGB	Bürgerliches Gesetzbuch
BGBl.	Bundesgesetzblatt
BGH	Bundesgerichtshof
BImSchV	Verordnung zur Durchführung des Bundes-Immissionsschutzgesetzes
BKA	Bundeskriminalamt
Bln, bln.	Berlin, berlinerisch
BMI	Bundesministerium des Innern
BND	Bundesnachrichtendienst
BNDG	Gesetz über den Bundesnachrichtendienst
BNetzAG	Gesetz über die Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen
BNetzAgentur	Bundesnetzagentur
BPolG	Gesetz über die Bundespolizei (Bundespolizeigesetz)

[1] Vgl. auch *Kirchner*, Abkürzungsverzeichnis der Rechtssprache (11. Aufl. 2024).

BR	Bundesrat
Brem, brem.	Bremen, bremisch
BSH	Bundesamt für Seeschifffahrt und Hydrographie
BSI	Bundesamt für Sicherheit in der Informationstechnik
BSIG	Gesetz über das Bundesamt für Sicherheit in der Informationstechnik
BStatG	Gesetz über die Statistik für Bundeszwecke
BT	Bundestag
BVerfG	Bundesverfassungsgericht
BVerfGE	Entscheidungen der amtlichen Sammlung des Bundesverfassungsgerichts
BVerfSchG	Gesetz über die Zusammenarbeit des Bundes und der Länder in Angelegenheiten des Verfassungsschutzes und über das Bundesamt für Verfassungsschutz
BVerwG	Bundesverwaltungsgericht
BW, bw.	Baden-Württemberg, baden-württembergisch
CER-Richtlinie	Richtlinie über die Resilienz kritischer Einrichtungen (EU) 2022/2557
CERT	Computer Emergency Response Team
CIR	Cyber- und Informationsraum (militärischer Organisationsbereich der Bundeswehr)
CISA	Cybersecurity and Infrastructure Security Agency
C&C-Server	Command-and-Control-Server
CRA, Cyberresilienz-VO	Cyberresilience Act, Verordnung über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen (EU) 2024/2847
CSA	Cybersecurity Act, Rechtsakt zur Cybersicherheit, Verordnung (EU) 2019/881
CSG BW	Gesetz für die Cybersicherheit in Baden-Württemberg
CSIRT	Computer Security Incident Response Team
CVD-Leitlinie	Leitlinie des BSI zum Coordinated Vulnerability Disclosure (CVD)-Prozess
DDG	Digitale-Dienste-Gesetz
DDoS-Angriff	„Distributed Denial of Service“-Angriff
DMA	Digital Markets Act, Verordnung über bestreitbare und faire Märkte im digitalen Sektor (EU) 2022/1925
DORA	Verordnung über die digitale operationale Resilienz im Finanzsektor (EU) 2022/2554
DoS-Angriff	„Denial of Service“-Angriff
DRDoS-Angriff	„Distributed Reflected Denial of Service“-Angriff
Drs.	Drucksache
DSGVO	Datenschutz-Grundverordnung
DVO	Durchführungsverordnung
E	Entwurf
ebd.	ebenda
EGMR	Europäischer Gerichtshof für Menschenrechte
ehem.	ehemalig, ehemalige, ehemaliger, ehemaliges
Einf.	Einführung
Einl.	Einleitung

engl.	englisch
ENISA	Die Agentur der Europäischen Union für Cybersicherheit
ENISA-VO	Verordnung zur Errichtung der Europäischen Agentur für Netz- und Informationssicherheit (EG) Nr. 460/2004
EnWG	Gesetz über die Elektrizitäts- und Gasversorgung
Erwgr.	Erwägungsgrund
EuGH	Europäischer Gerichtshof
f., ff.	folgende Seite bzw. Seiten
FBI	Federal Bureau of Investigation
FS	Festschrift
Fn.	Fußnote
FS	Festschrift
G	Gesetz
gem.	gemäß
GeschGehG	Geschäftsgeheimnisgesetz
GPSR	General Product Safety Regulation, Verordnung über die allgemeine Produktsicherheit (EU) 2023/988
GRCh	Europäische Grundrechtecharta
HdB	Handbuch
Hervorh.	Hervorhebung
Hess., hess.	Hessen, hessisch
HITSiG	Hessisches IT-Sicherheitsgesetz
Hmb., hmb.	Hamburg, hamburgisch
Hrsg., hrsg.	Herausgeber, herausgegeben
Hs.	Halbsatz
HStR	Handbuch des Staatsrechts, hrsg. v. Josef Isensee und Paul Kirchhof
i. e. S.	im engeren Sinne
i. R. v.	im Rahmen von
i. S. v.	im Sinne von
i. Ü.	im Übrigen
i. V. m.	in Verbindung mit
i. H. v.	in Höhe von
IoT	Internet of Things bzw. Internet der Dinge
IP-Adresse	Internet-Protocol-Adresse
IT	Informationstechnik
IT-Sicherheit	Sicherheit von Informationstechnik
IT-Sicherheitsgesetz 2.0	Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (BGBl. 2021 I, S. 1122)
ITSiV-PV	Verordnung zur Gewährleistung der IT-Sicherheit der im Portalverbund und zur Anbindung an den Portalverbund genutzten IT-Komponenten (BGBl. 2022 I, S. 18)
IT-System	informationstechnisches System
IuK-Technik	Informations- und Kommunikationstechnik
Jg., Jge.	Jahrgang, Jahrgänge
JI-RL, JI-Richtlinie	Richtlinie zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Ver-

	folgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr (EU) 2016/680
KRITIS	Kritische Infrastrukturen
KRITIS-Betreiber	Betreiber Kritischer Infrastrukturen bzw. Betreiber kritischer Anlagen
lit.	litera
LSA	Sachsen-Anhalt
LT	Landtag
LVerfGSchG	Landesverfassungsschutzgesetz
LVwG	Landesverwaltungsgesetz
m. Anm.	mit Anmerkung
MAC-Adresse	Media Access Control-Adresse
MAD	Militärischer Abschirmdienst
MEPolG	Musterentwurf eines einheitlichen Polizeigesetzes
MIRT	Mobile Incident Response Team
MüG	Marktüberwachungsgesetz
MÜ-VO	Verordnung über Marktüberwachung und die Konformität von Produkten (EU) 2019/1020
MV, mv	Mecklenburg-Vorpommern, mecklenburg-vorpommerisch
n. F.	Neue Fassung
NCSC	National Cyber Security Centre
Nds., nds.	Niedersachsen, niedersächsisch
NIS2-RL, NIS-2-Richtlinie	Richtlinie über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union (EU) 2022/2555
NIS-2-Umsetzungsgesetz	Gesetz zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung
NIS-RL, NIS-Richtlinie	Richtlinie über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union (EU) 2016/1148
NPOG	Niedersächsisches Polizei- und Ordnungsbehördengesetz
NRW, nrw.	Nordrhein-Westfalen, nordrhein-westfälisch
NSA	National Security Agency
OSINT	Open Source Intelligence
OT	Operational Technology
OVG	Oberverwaltungsgericht
OZG	Gesetz zur Verbesserung des Onlinezugangs zu Verwaltungsleistungen (Onlinezugangsgesetz)
PAG	Polizeiaufgabengesetz
PC	Personal Computer
POG	Polizei- und Ordnungsbehördengesetz
PolG	Polizeigesetz
PolR	Polizeirecht
PrALR	Preußisches Allgemeines Landrecht
ProdHaftG	Produkthaftungsgesetz
ProdSG	Produktsicherheitsgesetz
R	Recht
RefE	Referentenentwurf
RFC	Request for Comments

RhPf, rhpf.	Rheinland-Pfalz, rheinland-pfälzisch
RL	Richtlinie
Rn.	Randnummer
Rspr.	Rechtsprechung
Saarl., saarl.	Saarland, saarländisch
Sachs., sächs.	Sachsen, sächsisch
SächsISichG	Sächsisches Informationssicherheitsgesetz
SächsPVDG	Sächsisches Polizeivollzugsdienstgesetz
SCADA-System	„Supervisory Control and Data Aquisition"-System
SchlH, schlh.	Schleswig-Holstein, schleswig-holsteinisch
Slg.	Sammlung
SOG	Sicherheits- und Ordnungsgesetz
st.	ständig
StGB	Strafgesetzbuch
Störfall-VO	Zwölfte Verordnung zur Durchführung des Bundes-Immissionsschutzgesetzes (Störfall-Verordnung)
StPO	Strafprozessordnung
str.	streitig, strittig, umstritten
StVG	Straßenverkehrsgesetz
sublit.	Unterbuchstabe
TDDDG	Gesetz über den Datenschutz und den Schutz der Privatsphäre in der Telekommunikation und bei digitalen Diensten
Thür., thür.	Thüringen, thüringisch
TK-Anbieter	Anbieter von Telekommunikationsdiensten
TKG	Telekommunikationsgesetz
TM-Anbieter	Anbieter von Telemedienangeboten
TM-Angebot	Telemedienangebot
TMG	Telemediengesetz
TOR	The Onion Router
TTDSG	Gesetz über den Datenschutz und den Schutz der Privatsphäre in der Telekommunikation und bei Telemedien
u. U.	unter Umständen
UAbs.	Unterabsatz
ÜAnlG	Gesetz über überwachungsbedürftige Anlagen
Urt.	Urteil
US	United States
USA	United States of America, Vereinigte Staaten von Amerika
Var.	Variante
VG	Verwaltungsgericht
VGH	Verwaltungsgerichtshof
VO	Verordnung
Vol.	Volume, Band
Vorb.	Vorbemerkung
VwGO	Verwaltungsgerichtsordnung
VwVfG	Verwaltungsverfahrensgesetz
Ziff.	Ziffer
ZKA	Zollkriminalamt

Teil I

Cybergefahrenabwehr als Staatsaufgabe

§ 1 Einleitung

Cybersicherheit ist eine grundlegende Voraussetzung für das Funktionieren unserer Gesellschaft, denn Informationstechnik ist allgegenwärtig und sie ist verletzlich.[1] Gefahren für die Cybersicherheit gehören längst zum Alltag. Maßgeblich sind dabei weniger die großen, katastrophalen Cyberangriffe, die Blackouts oder gar Unfälle in Atomkraftwerken verursachen könnten.[2] Denn tagtäglich richten unzählige Cyberangriffe Schäden an – und können jeden treffen.

Als Russland im Jahr 2022 seinen Angriffskrieg gegen die Ukraine begann, erwarteten viele einen „Cyberkrieg".[3] Tatsächlich legte ein Angriff auf den Satellitennetz-Provider Viasat den Internetzugang ukrainischer Kundinnen und Kunden – unter anderem auch den des ukrainischen Militärs – lahm.[4] Der Angriff hatte europaweite Auswirkungen; zum Beispiel waren in Deutschland

---

[1] Vgl. *Roßnagel/Wedde/Hammer/Pordesch*, Die Verletzlichkeit der „Informationsgesellschaft" (2. Aufl. 1989), S. 5 ff., 79 ff. Siehe auch BT-Drs. 11/7029, S. 1; *Hornung/Schallbruch*, in: Hornung/Schallbruch/Bäcker, IT-Sicherheitsrecht (2. Aufl. 2025), § 1 Rn. 1 ff.; *Leisterer*, Internetsicherheit in Europa (2018), S. 2 f.; *Olejnik/Kurasinski*, Philosophy of Cybersecurity (2024), S. 2 ff.; *Wischmeyer*, Informationssicherheit (2023), S. 3 ff.

[2] *Röhrlich*, Hackerangriffe auf Atomkraftwerke – Abwehrstrategien sind schwierig zu entwickeln, Deutschlandfunk vom 08.07.2016. Das Schreckensszenario wird z. T. auch als „Cyber Pearl Harbor" bezeichnet: *Panetta*, Remarks by Secretary Panetta on Cybersecurity to the Business Executives for National Security. Siehe auch *Bumiller/Shanker*, Panetta Warns of Dire Threat of Cyberattack on U.S, The New York Times vom 11.10.2012; *Goldman/Warner*, Why a Digital Pearl Harbor Makes Sense … and Is Possible, in: Perkovich/Levite (Hrsg.), Understanding Cyber Conflict (2017), S. 147. Freilich ist das Gefahrenpotenzial für Kritische Infrastrukturen nicht auf Cyberangriffe begrenzt – Sabotageakte oder Fehler können ebenfalls zum Ausfall oder der Beeinträchtigung von Kritischen Infrastrukturen führen, vgl. *Nolte*, Flugausfälle durch gekapptes Glasfaserkabel: Der Fehler liegt bei der Lufthansa, heise Online vom 18.02.2023; *Sawall*, Glasfaser: Anschlag auf Bahn-Kabel erfolgte mit Insiderwissen, Golem.de vom 10.10.2022.

[3] Vgl. bspw. *Knoll*, Streitkräfteeinsatz zur Verteidigung gegen Cyberangriffe (2020), S. 37 ff.; *Olejnik/Kurasinski*, Philosophy of Cybersecurity (2024), S. 141 ff. *Kello*, The Virtual Weapon and International Order (2017), S. 17.

[4] *Der Spiegel*, „Cyber-Kollateralschaden" auch in Deutschland: Satellitennetzwerk Viasat offenbar gezielt in Osteuropa gehackt, 05.03.2022, https://www.spiegel.de/netzwelt/web/viasat-satellitennetzwerk-offenbar-gezielt-in-osteuropa-gehackt-a-afd98117-5c32-4946-ab8a-619f1e7af024.

über 3.000 Windräder nicht mehr zur Fernwartung erreichbar.[5] Außerdem trennte Ende 2023 ein Cyberangriff auf den Telekommunikationsdienstleister Kyivstar rund 24 Millionen ukrainische Kundinnen und Kunden vom Internet.[6] Hinzu kommen zahlreiche, aber nur begrenzt effektive, Angriffe auf Banken und Verwaltungsbehörden mit sog. „Wiper"-Schadsoftware, die Daten befallener Systeme löscht;[7] ferner überlasteten sog. „Denial-of-Service"-Angriffe ukrainische Webseiten mit Anfragen, sodass diese nicht mehr abrufbar waren (sog. Web-Defacement).[8] Ein Angriff auf ukrainische Umspannwerke, der zu Stromausfällen führen sollte, blieb dagegen erfolglos.[9] Im Vergleich dazu konnte die russische Gruppe „Sandworm" im Jahr 2015 einen mehrstündigen Blackout für ungefähr 80.000 ukrainische Kundinnen und Kunden erreichen[10] und im Oktober 2023 gelang es russischen Angreifenden aber, (auch) durch einen Cyberangriff die Stromversorgung zu beeinträchtigen.[11] Größere strategische Erfolge durch Cyberoperationen gelangen Russland folglich nicht[12] – Russland führt den Krieg gegen die Ukraine hauptsächlich mit konventionellen Methoden und kinetischen Waffen; Cyberangriffe sollen diese nur ergänzen (sog. hybride Kriegsführung).[13]

Man könnte daher zu dem Schluss kommen, dass die Gefahren für die Cybersicherheit gar nicht so gravierend seien und physischen Bedrohungen nicht

---

[5] *Biermann/Wolfangel*, Cyberkrieg: Angriff im Rücken der ukrainischen Armee, Die Zeit vom 23.02.2023.

[6] *Stöckel*, Ukraine: Russische Hacker verbrachten wohl Monate im Kyivstar-Netz, Golem.de vom 05.01.2024.

[7] *Holland*, Ukraine-Krieg: So viele Angriffe mit zerstörerischen Wipern wie nie zuvor, heise Online vom 24.02.2023; *Greenberg*, Ukraine Suffered More Wiper Malware in 2022 Than Anywhere, Ever, WIRED vom 22.02.2023.

[8] *Conger/Sanger*, Hackers Claim to Target Russia With Cyberattacks and Leaks, The New York Times vom 22.04.2022; *Lindern/Polke-Majewski/Biermann*, Cyberangriff auf die Ukraine: Digitale Nadelstiche, Die Zeit vom 16.02.2022. vgl. auch *BSI*, Die Lage der IT-Sicherheit in Deutschland 2022, S. 11, 43 ff. Kritisch; *Brenner*, J. Crim. L. & Criminology 97 (2007), 379 (390 ff.).

[9] Vgl. *ESET*, Industroyer2: Angriffe auf ukrainische Energiewirtschaft, 12.04.2022. Vgl. auch *Greenberg*, Pipedream Malware: Feds Uncover „Swiss Army Knife" for Industrial System Hacking, WIRED vom 13.04.2022; *Dragos, Inc.*, Pipedream: Chernovite's Emerging Malware Targeting Industrial Control Systems (2022).

[10] Zetter, Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid, WIRED vom 03.03.2016.

[11] Mäder, Cyberattacke auf Stromnetz: Russische Hacker mit neuartigem Vorgehen, NZZ vom 09.11.2023.

[12] Siehe u. a. *Gibney*, Was ist mit Russlands Cyberwar?, Spektrum.de vom 02.04.2022; *Schmidt*, Russlands Krieg: Was droht uns im Cyberspace?, heise Online vom 16.03.2022.

[13] *Burt*, The hybrid war in Ukraine, Microsoft On the Issues vom 27.04.2022; *Hartmann*, Hybride und konventionelle Kriegführung in der Ukraine vom 19.11.2023; *Knoll*, Streitkräfteeinsatz zur Verteidigung gegen Cyberangriffe (2020), S. 59 ff.; *Schmidt*, Russlands Krieg: Was droht uns im Cyberspace?, heise Online vom 16.03.2022; *Tamminga*, SWP-Aktuell 2015 Nr. 27, S. 1 ff.

einmal im Ansatz gleichkämen. Allerdings muss das auch nicht das Ziel sein: Cyberangriffe können ein zweckmäßiges Mittel sein, um gegnerischen Staaten zu schaden, ohne die Intensität eines bewaffneten Angriffs (und damit den Kriegszustand) zu erreichen. Russland führt schon seit Jahren digitale Feldzüge gegen die Ukraine – immer unter dem Deckmantel der Cyberkriminalität. Am 27. Juni 2017 löschte das Schadprogramm „NotPetya" die Daten zahlreicher IT-Systeme in der Ukraine (und weltweit).[14] Der Name „NotPetya" rührt daher, dass IT-Sicherheitsexpertinnen und -experten zu Beginn des Angriffs dachten, es handle sich um die Ransomware Petya. Später stellte sich heraus, dass NotPetya keine Ransomware, sondern ein Wiper war: Das Programm verschlüsselte die Daten, um sie zu zerstören; die Erpressungsnachrichten waren lediglich eine Finte.[15] NotPetya ist ein Wurm, d. h. ein Schadprogramm, das sich selbstständig verbreitet.[16] Diese Schadsoftware infizierte zunächst eine ukrainische Buchhaltungssoftware, breitete sich dann aber rasch aus und setzte die IT-Systeme in Krankenhäusern, Banken und der Verwaltung außer Betrieb – und traf schätzungsweise zehn Prozent der Computer des Landes.[17] Die Anlage des ehemaligen Atomkraftwerks Tschernobyl war ebenso betroffen wie Geldautomaten und Kartenzahlungssysteme.[18] Zum Beispiel waren das deutsche Pharma- und Chemieunternehmen Merck,[19] die dänische Reederei Maersk und das russische Staatsunternehmen Rosneft betroffen.[20] Allein der Schaden von Maersk soll im neunstelligen Bereich liegen.[21] Dieses Schadensausmaß dürften von den Angreifenden nicht beabsichtigt gewesen sein.

---

[14] Vgl. u. a. *Bendiek/Schulze*, Attribution als Herausforderung für EU-Cybersanktionen (Oktober 2021), S. 26 ff.; *Perlroth*, This Is How They Tell Me The World Ends (2021), S. 339 ff.; *Rhysider*, NotPetya, Darknet Diaries Episode 54 vom 24.12.2019.

[15] Vgl. *Greenberg*, The Untold Story of NotPetya, the Most Devastating Cyberattack in History, WIRED vom 21.08.2018; *Schmidt*, Petya/NotPetya: Kein Erpressungstrojaner, sondern ein „Wiper", heise Online vom 29.06.2017.

[16] *BKA*, Bundeslagebild Cybercrime 2017, S. 14.

[17] *BKA*, Bundeslagebild Cybercrime 2017, S. 14; *Greenberg*, The Untold Story of NotPetya, the Most Devastating Cyberattack in History, WIRED vom 21.08.2018.

[18] *Greenberg*, The Untold Story of NotPetya, the Most Devastating Cyberattack in History, WIRED vom 21.08.2018; *Perlroth*, This Is How They Tell Me The World Ends (2021), S. 339.

[19] Merck schätzte seinen Schaden auf ca. 870 Millionen US-Dollar, *Greenberg*, The Untold Story of NotPetya, the Most Devastating Cyberattack in History, WIRED vom 21.08.2018.

[20] *Greenberg*, The Untold Story of NotPetya, the Most Devastating Cyberattack in History, WIRED vom 21.08.2018. Siehe auch *U.S. Department of Justice*, Six Russian GRU Officers Charged, 19.10.2020 sowie *Auchard*, New computer virus spreads from Ukraine to disrupt world business, Reuters vom 27.06.2017.

[21] *Perlroth*, This Is How They Tell Me The World Ends (2021), S. 140. Der komplette Betrieb des Unternehmens kam zum Erliegen, *Auchard*, New computer virus spreads from Ukraine to disrupt world business, Reuters vom 27.06.2017.

Die USA und die EU schreiben NotPetya russischen Akteuren zu, allerdings bestehen hierfür lediglich Indizien; eine eindeutige Attribution ist nicht möglich.[22] Jedenfalls scheint klar, dass es sich angesichts der Komplexität des Angriffs um einen staatlichen Akteur handeln muss.[23] Das Schadprogramm nutzte u. a. EternalBlue, ein von der US-amerikanischen National Security Agency (NSA) entwickeltes Werkzeug, um eine Sicherheitslücke in Windows zu nutzen und sich volle Kontrolle über betroffene Systeme zu verschaffen.[24]

NotPetya veranschaulicht das große Schadenspotenzial von Cyberangriffen und nähert sich der Schwelle zum „Cyberkrieg" an.[25] Es handelt sich jedoch nur um *einen* Vorfall – Cyberangriffe und Schadprogramme wüten indessen permanent. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) warnt seit Jahren vor einer angespannten Bedrohungslage.[26] Eine besonders große Bedrohung stellt Ransomware dar: Der Begriff Ransomware setzt sich aus *ransom* (engl. für Lösegeld) und *ware* (von Software) zusammen; es handelt sich um Schadsoftware, die Daten verschlüsselt und diese den Betroffenen entzieht, um Lösegeld zu erpressen.[27] Sie nimmt pandemische Ausmaße an[28]

---

[22] *U.S. Department of Justice*, Six Russian GRU Officers Charged, 19.10.2020; *Rat der Europäischen Union*, EU verhängt erstmals Sanktionen als Reaktion auf Cyberangriffe, 30.07.2020; siehe den der DurchführungsVO (EU) 2020/1125. Vgl. auch *Auchard*, New computer virus spreads from Ukraine to disrupt world business, Reuters vom 27.06.2017.

[23] *NATO Cooperative Cyber Defence Centre of Excellence*, NotPetya and WannaCry Call for a Joint Response from International Community, https://ccdcoe.org/news/2017/notpetya-and-wannacry-call-for-a-joint-response-from-international-community/. Siehe auch *Bendiek/Schulze*, Attribution als Herausforderung für EU-Cybersanktionen (Oktober 2021), S. 27 f.; *Scherschel*, 3 Jahre NotPetya: Der Erpressungstrojaner, der keiner war, heise Online vom 27.06.2020.

[24] *Greenberg*, The Untold Story of NotPetya, the Most Devastating Cyberattack in History, WIRED vom 21.08.2018.

[25] Von Cyberkrieg sprechen u. a. *Greenberg*, The Untold Story of NotPetya, the Most Devastating Cyberattack in History, WIRED vom 21.08.2018; *Moore*, Offensive Cyber Operations (2022), S. 163 f. Dagegen entschied ein US-amerikanisches Gericht, dass NotPetya keinen Kriegsfall darstelle, vgl. *Krempl*, Kein Kriegsfall: Versicherung muss für Ransomware-Schaden durch NotPetya zahlen, heise Online vom 05.05.2023.

[26] *BSI*, Die Lage der IT-Sicherheit in Deutschland 2024, S. 8 ff.; *BSI*, Die Lage der IT-Sicherheit in Deutschland 2023, S. 11; *BSI*, Die Lage der IT-Sicherheit in Deutschland 2022, S. 11; *BSI*, Die Lage der IT-Sicherheit in Deutschland 2021, S. 9 f.; *BSI*, Die Lage der IT-Sicherheit in Deutschland 2020, S. 9; *BSI*, Die Lage der IT-Sicherheit in Deutschland 2019, S. 7 f. Siehe ferner das Lagebild der Agentur der Europäischen Union für Cybersicherheit: *ENISA*, Threat Landscape 2023, S. 6.

[27] *Büchel/Hirsch*, Internetkriminalität (2. Aufl. 2020), S. 87 ff.; *Kochheim*, Cybercrime und Strafrecht in der Informations- und Kommunikationstechnik (2. Aufl. 2018) Rn. 445.

[28] Vgl. zur Verbreitung *Atug*, Ransomware als Business Case in der organisierten Kriminalität, in: Rüdiger/Bayerl (Hrsg.), Handbuch Cyberkriminologie 2, S. 345 ff.; *Kropotov* u. a., What Decision-Makers Need to Know About Ransomware Risk, Trend Micro Research (2023), S. 16 ff.

und trifft Unternehmen wie staatliche Stellen.[29] Zudem akquirieren Botnetze Hunderttausende unsichere IoT-Geräte.[30] Sicherheitslücken in weitverbreiteter Software gefährden Millionen von Nutzenden.[31] Krankenhäuser müssen die medizinische Versorgung einschränken, was das Leben und die Gesundheit von Patientinnen und Patienten gefährdet – insbesondere in Notfällen.[32] Sind Verwaltungsbehörden betroffen, gefährdet dies die Funktionsfähigkeit des Staates und beeinträchtigt Menschen, wenn sie z. B. keine Sozialhilfe mehr ausgezahlt bekommen.[33] Angriffe auf große Unternehmen, staatliche Stellen oder Kritische Infrastrukturen sind aber zusätzlich attraktiv, da sich höhere Lösegelder bzw. Verkaufspreise für gestohlene Daten erzielen lassen (sog. „Big Game Hunting").[34] Auch Privatpersonen sind exponiert, wenn Cyberkriminelle Daten abgreifen: In Finnland verschafften sich Angreifende Zugriff auf die Daten psychotherapeutischer Praxen und drohten, diese zu veröffentlichen.[35] Nach einem Datenleck der Online-Plattform Ashley Madison, einer Dating-Webseite für Seitensprünge, wurden Informationen über außereheliche Affären veröffentlicht.[36]

---

[29] *Stöckel*, Südwestfalen IT: Cyberangriff legt IT-Dienste vieler deutscher Kommunen lahm, Golem.de vom 30.10.2023. Siehe auch den Podcast „You are fucked – Deutschlands erste Cyberkatastrophe" vom MDR zum Ransomwarevorfall des Landkreis Anhalt-Bitterfeld, https://www.mdr.de/mdr-sachsen-anhalt/podcast/you-are-fucked/index.html.

[30] Internet of Things bzw. Internet der Dinge, d. h. vernetzte Geräte. Vgl. bspw. *Goodin*, New, more-powerful IoT botnet infects 3,500 devices in 5 days, Ars Technica vom 01.11.2016. Siehe allgemein zur Unsicherheit von IoT-Geräten: *Heckmann/Paschke*, in: Bräutigam/Kraul/Bauer, Internet of Things (2021), § 10 Rn. 21 ff.; *Kleinhans*, Internet of Insecure Things (07.12.2017), S. 5 ff.; *Sohr/Kemmerer*, in: Kipker u. a., Cybersecurity (2. Aufl. 2023), Kapitel 3 Rn. 2421 ff.

[31] Siehe u. a. *Knop*, Kritische Word-Lücke: Proof-of-Concept-Code veröffentlicht, heise Online vom 07.03.2023.

[32] *Knop*, Ransomware-Angriff: Krankenhaus muss hunderte Operationen absagen, heise Online vom 07.03.2023; *Krempl*, Bundesregierung: Deutlich mehr Cyberangriffe auf Kliniken und Versorger, heise Online vom 26.11.2020; *Spinnler*, Kliniken im Visier der Hacker, tagesschau.de vom 28.06.2021; *Stock*, Missing Link: Ransomware-Angriffe auf Krankenhäuser gefährden Menschenleben, heise Online vom 28.01.2024. Siehe auch *Olejnik/Kurasinski*, Philosophy of Cybersecurity (2024), S. 96 ff.

[33] *dpa*, Nach Cyberangriff: Rhein-Pfalz-Kreis erwartet Normalbetrieb im Frühsommer, heise Online vom 12.01.2023, https://www.heise.de/news/Nach-Cyberangriff-Rhein-Pfalz-Kreis-erwartet-Normalbetrieb-im-Fruehsommer-7457667.html; *Heidtmann*, Ransomware-Attacke: Landkreis Anhalt-Bitterfeld wird erpresst, Süddeutsche Zeitung vom 15.07.2021.

[34] *Atug*, Ransomware als Business Case in der organisierten Kriminalität, in: Rüdiger/Bayerl (Hrsg.), Handbuch Cyberkriminologie 2, S. 345 (355 f.); *BSI*, Die Lage der IT-Sicherheit in Deutschland 2022, S. 11.

[35] *Holland*, Psychotherapeuten gehackt: Finnische Patienten und Praxen werden erpresst, heise Online vom 27.10.2020.

[36] *Schirrmacher*, Nach Ashley-Madison-Hack: Erbeutete Daten veröffentlicht, heise Online vom 19.08.2015; siehe auch *Segall*, Pastor outed on Ashley Madison commits suicide, CNN vom 11.03.2023.

Wer findet nicht mindestens eine eigene E-Mail-Adresse in geleakten Datensätzen mithilfe der Webseite haveibeenpwned.com?

Bedrohlich sind daher nicht einzelne Staaten oder Cyberkriminellen-Gruppen, entscheidend ist weniger der *eine* große Konflikt. Auch wenn die großen Cyberangriffe von Antagonisten wie den USA, Russland, China, Nordkorea oder dem Iran als die primäre Bedrohung im Cyberraum erscheinen, rührt die kritische Cybersicherheitslage von vielen verschiedenen Akteuren her, die alle unterschiedliche Interessen verfolgen.

Sobald Sicherheitslücken öffentlich oder in kriminellen Kreisen bekannt werden, wittern Cyberkriminelle rentable Angriffsmöglichkeiten – und ihre Angriffszyklen verkürzen sich.[37] Dienste wie Shodan finden automatisiert geeignete Angriffsziele. Werkzeuge und Baukästen wie Metasploit ermöglichen es, den passenden Exploit (die Schadsoftware zum Ausnutzen einer Sicherheitslücke) mit der gewünschten Payload (die Transportlast, die das eigentliche Angriffsziel verfolgt, z. B. Ransomware)[38] zu verbinden, sodass selbst Amateure Schaden anrichten können.

Angesichts dessen kann kein IT-System als sicher gelten: Die Frage ist nicht, *ob* ein System über Sicherheitslücken verfügt – sondern *welche* Schwachstellen existieren.[39] Wer lange und intensiv genug sucht, wird Schwachstellen finden; meistens reicht jedoch der Blick in frei zugängliche Schwachstellen-Datenbanken, fachspezifische Nachrichten oder Handelsforen für bislang unbekannte Sicherheitslücken (sog. Zero-Day-Schwachstellen, die dem Hersteller „null Tage" bekannt sind).[40] Ein erklärter Cyberkrieg ändert an dieser Bedrohungslage nur wenig,[41] denn dieses Gefahrenpotenzial besteht für alle IT-Systeme – permanent.

Diese Gefahrenlage für die IT-Sicherheit verlangt nach einer kohärenten, multidimensionalen und nationalen Cybersicherheitspolitik, die Cybersicherheit nicht den Kräften des Marktes oder den einzelnen Nutzenden überlässt. Das Recht kann an mehreren Stellschrauben drehen, um die Cybersicherheit zu verbessern: Notwendig sind vertragliche und deliktische Haftungs- und Einstandspflichten der Hersteller von IT-Produkten, die strafrechtliche Sanktionierung von Cyberangriffen und (die dafür erforderlichen) Ermittlungsbefugnisse, sowie eine öffentlich-rechtliche Risikoregulierung. Doch diese Bausteine verhindern nicht alle Cyberangriffe – sie können lediglich die allgemeine

---

[37] *BSI*, IT-Grundschutz-Kompendium (2023), IT-Grundschutz – Basis für Informationssicherheit, S. 2.

[38] Siehe *Froehlich/Loshin*, payload (computing), TechTarget vom 2021.

[39] Wie Gene Spafford es einmal sagte: „The only truly secure system is one that is powered off, cast in a block of concrete and sealed in a lead-lined room with armed guards – and even then I have my doubts." (zitiert nach https://spaf.cerias.purdue.edu/quotes.html).

[40] *BSI*, Zero-Day-Exploit, https://web.archive.org/web/20230526140324/https://www.bsi.bund.de/SharedDocs/Glossareintraege/DE/Z/Zero-Day-Exploits.html.

[41] *BSI*, Die Lage der IT-Sicherheit in Deutschland 2022, S. 22.

Grundsicherheit von IT-Systemen erhöhen oder Angreifende im Nachhinein bestrafen. Es bedarf aber auch Handlungsmöglichkeiten, um akuten Gefahren zu begegnen. Die Politik rekurriert regelmäßig auf die Forderung nach Befugnissen für das „Zurückhacken" (sog. „Hackbacks" oder digitale Gegenschläge).[42] Die Abwehr von Gefahren für die Cybersicherheit kann jedoch mithilfe einer ganzen Reihe von Maßnahmen gelingen. Manche dieser Maßnahmen beschränken sich auf die Gewinnung von Informationen über Bedrohungen, manche unterstützen Betroffene eines Cyberangriffs oder geben Betreibern bei der Absicherung ihrer IT-Systeme Hilfestellung.

Im folgenden Abschnitt (A.) stellen vier vergangene Cyberangriffe exemplarisch dar, welche Auswirkungen möglich sind und welche Strategien Betroffene und staatliche Stellen zur Bewältigung von Vorfällen verfolgt haben. Dabei zeigt sich, dass Betroffene – wie auch die Allgemeinheit – auf staatliche Unterstützung bei der Bewältigung von Gefahren für die Cybersicherheit angewiesen sind (B.). Als Garant für Sicherheit ist der Staat gefragt: Die Abwehr von Gefahren für die Cybersicherheit fällt unter die staatliche Aufgabe der Gefahrenabwehr. Diese Arbeit erkundet, inwiefern die gefahrenabwehrrechtliche Dogmatik auf die Abwehr von Gefahren für die Cybersicherheit anwendbar ist. Zugleich systematisiert sie die Befugnisse der Cybergefahrenabwehr.

A. Allgegenwärtige Gefahren für unsere Gesellschaft

Die folgenden vier Beispiele von Cybervorfällen dienen zum einen dazu, Angriffsvektoren und Vorgehensweisen der Angreifenden sowie (potenzielle) Auswirkungen dazustellen. Sie sollen aber auch zeigen, welche Gefahrenabwehrmaßnahmen staatliche Stellen ergriffen haben oder hätten ergreifen können, um die Vorfälle zu bewältigen.

Die Sicherheitslücke *Log4Shell* (I.) verdeutlicht die Komplexität moderner Software: Die Unsicherheit einer Komponente reicht aus, um unzählige Systeme zu gefährden. Dass auch ein relativ banaler Ransomware-Angriff gravierende Auswirkungen für die Versorgung der Bevölkerung haben kann, zeigt der Colonial-Pipeline-Vorfall (II.). Das dritte Beispiel veranschaulicht den Ablauf eines klassischen Cyberangriffs: Angreifende suchen eine Sicherheitslücke und nutzen diese aus, um sich möglichst umfassend Zugriff auf das Ziel-

[42] *Greis*, Cyberabwehr: Faeser will Grundgesetz für Hackbacks ändern, Golem.de vom 03.04.2023; *Metzger/Stoll*, Faeser: BKA muss Putins Hacker stoppen können, ZDF vom 31.03.2023; siehe auch ein Jahr zuvor *Krempl*, Cyberverteidigung: EU-Kommission fordert Hackbacks zum digitalen Gegenschlag, heise Online vom 11.11.2022; siehe aber auch *Grüner/dpa*, IT-Sicherheit: Faeser lehnt Hackbacks offenbar doch ab, Golem.de vom 01.05.2022. Hackbacks forderte auch die vorherige Bundesregierung: *Biselli*, Hackback im Bundespolizeigesetz: Seehofer wollte den digitalen Gegenangriff starten, netzpolitik.org vom 29.01.2020.

system zu verschaffen. Die Sicherheitslücke betraf eine häufig eingesetzte Anwendung und exponierte zahlreiche Unternehmen weltweit (*Microsoft Exchange Server*, III.). Angreifende können aber auch komplexe Angriffsstrukturen aufbauen, indem sie IT-Systeme übernehmen, in eine Befehlsstruktur einbinden und ein sog. Botnetz aufbauen. Ein Beispiel hierfür ist *Emotet* (IV).

I. Log4Shell

Im November 2021 versetzte eine bislang unbekannte Sicherheitslücke in der weitverbreiteten Open-Source-Bibliothek Log4j die IT-Branche in Angst und Schrecken:[43] Log4j bietet ein Paket mit Programmcode für die Programmiersprache Java und protokolliert Aktivitäten von Anwendungen.[44] Es lässt sich kostenlos und leicht in Anwendungen integrieren, ohne dass Entwicklerinnen oder Entwickler selbst Logging-Funktionalitäten erstellen müssen; dementsprechend findet sich Log4j in vielen Software-Architekturen wieder.[45]

Die Sicherheitslücke – Log4Shell getauft – ermöglicht es Angreifenden, mit Log4j eine „Shell" (eine Schnittstelle) auf dem Zielsystem zu etablieren und damit nicht nur Programmcode zu loggen, sondern auch auszuführen.[46] Dadurch lassen sich anfällige System kontrollieren.[47] Die Sicherheitslücke betraf Hunderte Millionen von IT-Systemen und IT-Produkten, da Java eine der am häufigsten verwendeten Programmiersprachen und Log4j in vielen Java-Anwendungen integriert ist.[48] Betroffene konnten aber nicht ohne Weiteres klären, ob ein Softwareprodukt oder ein konkretes IT-System betroffen ist, da

---

[43] Siehe hierzu Apache Log4j, https://logging.apache.org/log4j/2.x/. Vgl. auch die Berichterstattung: *Hunter/Vynck*, The „most serious" security breach ever is unfolding right now. Here's what you need to know, The Washington Post vom 20.12.2021; *Woodyard*, „Critical vulnerability": Smaller firms may find it harder to stop hackers from exploiting Log4j flaw, USA TODAY vom 16.12.2021. Siehe auch *cy*, Log4Shell – Bug oder Feature, YouTube vom 21.05.2022, https://media.ccc.de/v/gpn20-60-log4shell-bug-oder-feature.

[44] *BSI*, Kritische „Log4Shell" Schwachstelle in weit verbreiteter Protokollierungsbibliothek Log4j (CVE-2021-44228), 12.01.2022, S. 1.

[45] *BSI*, Warnstufe Rot: Schwachstelle Log4Shell führt zu extrem kritischer Bedrohungslage, 16.12.2021.

[46] https://nvd.nist.gov/vuln/detail/CVE-2021-44228; *Hunter/Vynck*, The „most serious" security breach ever is unfolding right now. Here's what you need to know, The Washington Post vom 20.12.2021; *Lim*, Apache Log4j Vulnerability Explained, Swarmnetics vom 05.02.2022.

[47] *Newman*, A Log4j Vulnerability Has Set the Internet „On Fire", WIRED vom 10.12.2021.

[48] *statista*, Programmiersprachen weltweit laut PYPL-Index im März 2024, https://de.statista.com/statistik/daten/studie/678732/umfrage/beliebteste-programmiersprachen-weltweit-laut-pypl-index/. Siehe auch *Barrett*, The Next Wave of Log4J Attacks Will Be Brutal, WIRED vom 16.12.2021; *Hunter/Vynck*, The „most serious" security breach ever is unfolding right now. Here's what you need to know, The Washington Post vom 20.12.2021.

Stichwortverzeichnis