Going dark – Signals Intelligence im IT-Zeitalter

Herausgegeben von
JOSEF FRANZ LINDNER und
JOHANNES UNTERREITMEIER

Beiträge zum Sicherheitsrecht und zur Sicherheitspolitik
10

Mohr Siebeck

Beiträge zum Sicherheitsrecht
und zur Sicherheitspolitik

herausgegeben von

Jan-Hendrik Dietrich, Klaus Ferdinand Gärditz
und Kurt Graulich

10

Going dark – Signals Intelligence im IT-Zeitalter

Herausgegeben
von

Josef Franz Lindner
und Johannes Unterreitmeier

Mohr Siebeck

Josef Franz Lindner ist Inhaber des Lehrstuhls für Öffentliches Recht, Medizinrecht und Rechtsphilosophie und Geschäftsführender Direktor des Instituts für Bio-, Gesundheits- und Medizinrecht an der Universität Augsburg.

Johannes Unterreitmeier ist Ministerialrat und Leiter des Sachgebiets für Verfassungsschutz-, Waffen- und Versammlungsrecht sowie Vereinsverbote am Bayerischen Staatsministerium des Innern, für Sport und Integration.
orcid.org/0000-0003-1101-3950

ISBN 978-3-16-161290-9 / eISBN 978-3-16-161291-6
DOI 10.1628/978-3-16-161291-6

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 *http://dnb.dnb.de* abrufbar.

Das Buch wurde von Martin Fischer in Tübingen aus der Minion gesetzt und von Laupp und Göbel in Gomaringen auf alterungsbeständiges Werkdruckpapier gedruckt und gebunden.

Printed in Germany.

Vorwort

„Going dark" im Internet … das ist die zentrale Herausforderung der Sicherheitsbehörden im 21. Jahrhundert. Terroristen und Extremisten auf der ganzen Welt nutzen die modernen Kommunikationswege, um zu rekrutieren, Botschaften des Hasses zu verbreiten oder Anschläge auf die freiheitliche Gesellschaft zu koordinieren. Kriminelle rund um den Globus bieten über das Netz auch hier in Deutschland Drogen, Waffen, Menschen und vieles mehr an. Sie alle können sich mit Hilfe der heutigen Verschlüsselungstechnik anonym im „Dark Net" bewegen.

Wie können unsere Sicherheitsbehörden mit dieser Entwicklung mithalten? Brauchen sie neue Befugnisse zur Überwachung, um dem sogenannten „Going-dark"-Effekt wirksam begegnen zu können? Welche Chancen und Risiken bieten „Backdoors", strategische Internetaufklärung oder „Hackback"? Wo liegen die verfassungsrechtlichen Grenzen? Unter dem Titel „Going dark – Signals Intelligence im IT-Zeitalter" suchte die Fachtagung der Reihe „Recht auf Sicherheit" hierzu zukunftsfähige Antworten. Die vom Bayerischen Staatsministerium des Innern, für Sport und Integration initiierte Veranstaltungsreihe wendet sich an Vertreter aus der Wissenschaft ebenso wie aus Politik, Justiz und Verwaltung sowie der Zivilgesellschaft. Auf diese Weise soll eine Plattform zu einem übergreifenden fachlichen Austausch eröffnet werden.

Hochkarätige Referenten aus Politik, Wissenschaft und Gesellschaft näherten sich am 4. Oktober 2021 in München dem Thema im Spannungsfeld von Freiheit und Sicherheit im Cyberspace aus unterschiedlicher Perspektive. Der Tagungsband dokumentiert die Vorträge der Fachtagung sowie den Verlauf der Podiumsdiskussion. Teilweise enthält die hier gedruckte Fassung der Vorträge auch Aktualisierungen sowie Teile, die von den Referenten aus Zeitgründen gekürzt oder ganz weggelassen werden mussten.

Die Organisation und inhaltliche Konzeption der Veranstaltung erfolgte durch das Sachgebiet E4 „Verfassungsschutz-, Waffen- und Versammlungsrecht; Vereinsverbote" des Bayerischen Staatsministeriums des Innern, für Sport und Integration. Ohne die tatkräftige Unterstützung der Mitarbeiterinnen und Mitarbeiter dieses und anderer Sachgebiete aus der ganzen Abteilung hätte die Tagung nicht stattfinden können. Ein ganz besonderer Dank gilt Herrn Oberregierungsrat Christof Gregor und Frau Regierungsrätin Kathrin Aicher, die die wesentliche Last der Organisation und inhaltlichen Vorbereitung getragen haben. Es ist ihr Verdienst, dass die Tagung trotz schwierigster Rahmenbedingungen überhaupt stattfinden konnte, denn die weiter anhaltende Corona-Pandemie machte eine zweimalige Verschiebung der ursprünglich bereits für den 7. Mai 2020

geplanten Tagung und zuletzt eine kurzfristige Verlegung des Veranstaltungsorts notwendig. Gemeinsam mit Herrn Regierungsrat Michael Ruhland und Herrn Regierungsamtsrat Thomas Becker haben sie das Tagungskonzept immer wieder an die sich fortlaufend ändernde pandemische Lage und die dadurch bedingten infektionsschutzrechtlichen Vorgaben angepasst und mit unermüdlichem Einsatz für einen reibungslosen Ablauf der Veranstaltung gesorgt.

München im Juni 2022

Josef Franz Lindner
Johannes Unterreitmeier

Inhaltsverzeichnis

Begrüßung und Einführung

Heinz Huber

I. „Going dark“: Auswirkungen der Verschlüsselung auf die „Signals Intelligence“

Unter dem Begriff „Going dark“, mit dem wir diese Fachtagung überschrieben haben, versteht man im Sicherheitsbereich das Versiegen von Informationskanälen für die Sicherheitsbehörden in der digitalen Welt aufgrund von Verschlüsselung und anderen Technologien.[1] Die „Signals Intelligence“, mithin die technische Fernmeldeaufklärung, ist von allen nachrichtendienstlichen und polizeilichen Mitteln der Ermittlung hiervon am meisten betroffen. Eine Ende-zu-Ende-Verschlüsselung von Textnachrichten verhindert beispielsweise, dass die Sicherheitsbehörden den Inhalt der Kommunikation zwischen islamistischen oder rechtsextremistischen Gefährdern oder Tatverdächtigen auch ohne unmittelbaren Zugriff auf deren Endgeräte mitverfolgen können.

1. Crypto Wars der 1990er Jahre

Derartige Problemstellungen sind seit Beginn des IT-Zeitalters bekannt. Bereits in den 1990er Jahren wurde in den USA unter dem Schlagwort „Going dark“ eine Debatte im Zuge der sogenannten Crypto Wars geführt.[2] Damals versuchte die US-Regierung, die Ausfuhr der gerade aufkommenden nicht-militärischen Verschlüsselungstechnologien zu beschränken und Unternehmen zum Vorhalten von Entschlüsselungssystemen zu verpflichten – letztlich ohne Erfolg. Zum einen konnte durch die Exportkontrollen nicht verhindert werden, dass starke Verschlüsselungsalgorithmen weltweit entwickelt und in die USA importiert wurden. Nach einer gerichtlichen Entscheidung in den USA[3] konnte diese Politik auch nicht weiter aufrechterhalten werden. Zum anderen zeigte die Pflicht zum Vorhalten einer staatlichen Zugriffsmöglichkeit auf verschlüsselte Daten erhebliche Sicherheitslücken auf.[4]

---

[1] *Schulze*, Going Dark? Dilemma zwischen sicherer, privater Kommunikation und den Sicherheitsinteressen von Staaten, APuZ 46–47/2017, 23.

[2] *Castro/McQuinn*, Unlocking Encryption: Information Security and the Rule of Law, ITIF, März 2016, S. 7 f.

[3] *Bernstein v. United States Department of Justice*, No. 97–16686 (9th Cir. May 6, 1999).

[4] *Castro/McQuinn* (o. Fußn. 2), S. 7 f.

2. FBI vs. Apple

In jüngerer Zeit wurde die Debatte insbesondere durch den ehemaligen FBI-Direktor James Brien Comey im Zuge des islamistischen Terroranschlags in San Bernardino im Dezember 2015 wiederbelebt,[5] bei dem 14 Menschen getötet und 21 weitere verletzt wurden.[6] Das Technologieunternehmen Apple weigerte sich seinerzeit trotz einer vorliegenden gerichtlichen Verfügung[7], die Sicherheitsbehörden bei der Entschlüsselung des iPhones eines Täters zu unterstützen. Die Entschlüsselung gelang schließlich nur mit Hilfe eines privaten Dritten; der Kostenaufwand betrug angeblich 1 Million US-Dollar.[8]

3. Herausforderungen für die deutschen Sicherheitsbehörden

Der „Going-dark"-Effekt stellt aber auch hierzulande die Sicherheitsbehörden von Bund und Ländern vor große Herausforderungen. Das betrifft nicht nur die Verschlüsselung von Nachrichten. Die Verschleierung der eigenen Identität im Internet ist mittels eines Virtual Private Network für jedermann möglich. Die omnipräsente Vernetzung von virtuellem und analogem Leben – Stichwort: Internet der Dinge – ist so eng, dass eine Unterscheidung zwischen digitalem und realem Lebensraum kaum mehr möglich ist. Und für den transnationalen Cyberraum sind Grenzsteine und Schlagbäume nicht existent, nationale und föderale Kompetenzen damit irrelevant.[9]

II. Unterschiedliche Lösungsansätze

Auf diese Herausforderungen müssen wir dringend Antworten finden. Die bislang vorgeschlagenen Herangehensweisen könnten nicht unterschiedlicher sein:[10] Die Ansätze reichen von einem vollständigen Verbot jeglicher starken

[5] *Yates/Comey*, Statement before the United States Senate Judiciary Committee at a Hering Entitled „Going Dark: Encryption, Technology, and the Balance Between Public Safety and Privacy", presented July 8, 2015, https://www.judiciary.senate.gov/download/07-08-15-yates-and-comey-joint-testimony (zuletzt aufgerufen am 20.7.2022); *Volz/Hosenball*, FBI director says investigators unable to unlock San Bernardino shooter's phone content, reuters.com v. 9.2.2016.

[6] *Stern*, Attentat von San Bernardino: FBI stuft Attacke als Terrorakt ein, stern.de v. 5.12.2015.

[7] *Blankenstein*, Judge Forces Apple to Help Unlock San Bernardino Shooter iPhone, nbcnews.com v. 17.2.2016.

[8] *Tanfani*, Race to unlock San Bernardino shooter's iPhone was delayed by poor FBI communication, report finds, latimes.com v. 27.3.2018.

[9] *Unterreitmeier*, Das Internet als Herausforderung der inneren Sicherheit im beginnenden 21. Jahrhundert, in: Verein Deutscher Verwaltungsgerichtstag e. V. (Hrsg.), Dokumentation: 19. Deutscher Verwaltungsgerichtstag Darmstadt 2019, 2020, S. 199 ff.

[10] Zum verfassungsrechtlichen Rahmen vgl. *Dietrich*, Der Einsatz von Verschlüsselungstechniken zwischen Grundrechtsschutz und staatlicher Sicherheitsgewährleistung, GSZ 2021, 1 ff.

kryptografischen Technologien[11] bis hin zur Forderung nach einem „Recht auf Verschlüsselung".[12] Letzteres soll etwa dazu führen, dass Telekommunikations- und Telemedienanbieter verpflichtet werden können, eine Ende-zu-Ende-Verschlüsselung einzusetzen, oder dass staatliche Behörden IT-Sicherheitslücken unverzüglich an das Bundesamt für Sicherheit in der Informationstechnik zu melden haben.[13] Das Bundesverfassungsgericht stellte hierzu jüngst fest, dass die grundrechtliche Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme keinen Anspruch gegen den Staat begründe, jede unerkannte IT-Sicherheitslücke, wie zum Beispiel sogenannte Zero-Day-Exploits, sofort und unbedingt dem Hersteller zu melden. Allerdings sei eine Regelung erforderlich, wie bei der Entscheidung über ein Offenhalten unerkannter Sicherheitslücken der Zielkonflikt zwischen dem notwendigen Schutz vor Infiltration durch Dritte einerseits und der Ermöglichung von Quellen-Telekommunikationsüberwachungen andererseits aufzulösen ist.[14]

Daneben fordern einige eine weitreichende Klarnamenpflicht im digitalen Raum,[15] während andere hierdurch das Recht auf informationelle Selbstbestimmung und die Meinungsfreiheit in Gefahr sehen.[16] Und wo sich Befürworter einer verstärkten Inanspruchnahme von privaten Unternehmen und Dritten bei der Bekämpfung von Hass und Hetze im Netz finden,[17] stehen ihnen Verfechter des staatlichen Gewaltmonopols gegenüber, die stattdessen für rein strafrechtliche Lösungen plädieren.[18]

---

[11] Vgl. *Halliday/Shah*, Pakistan to ban encryption software, theguardian.com v. 30.8.2011.

[12] Antrag der *FDP-Fraktion* „Recht auf Verschlüsselung – Privatsphäre und Sicherheit im digitalen Raum stärken", BT-Drs. 19/5764 v. 13.11.2020.

[13] Antrag der *FDP-Fraktion* (o. Fußn. 12), S. 2.

[14] Vgl. BVerfGE 158, 170 Rn. 43 f. (IT-Sicherheitslücken); kritisch: *Dietrich*, Schriftliche Stellungnahme zur Sachverständigenanhörung vor dem Ausschuss für Inneres und Heimat des Deutschen Bundestages am 27.1.2020 zu BT-Drs. 19/5764, S. 5 ff.

[15] *Focus online*, Gegen Hass im Netz: Schäuble fordert Klarnamenpflicht für Internetnutzer, focus.de v. 13.1.2020.

[16] *York*, Gute Gründe für Pseudonymität – und gegen eine Klarnamenpflicht, netzpolitik.org v. 20.7.2016.

[17] Vgl. hierzu das Gesetz zur Änderung des Netzwerkdurchsetzungsgesetzes v. 3.6.2021 (BGBl. I S. 1436). Zur Problematik siehe auch *Riemenscheider/Lutz*, #HateSpeech – Shitstorms als Kampfmittel organisierter Strukturen, DuD 2021, 371 ff.

[18] Das Gesetz zur Bekämpfung des Rechtsextremismus und der Hasskriminalität v. 30.3.2021 (BGBl. I S. 441) soll die „zunehmende Verrohung der Kommunikation" im Internet und den sozialen Medien, durch die „nicht nur das allgemeine Persönlichkeitsrecht der Betroffenen, sondern auch der politische Diskurs in der demokratischen und pluralistischen Gesellschaft angegriffen und in Frage gestellt" wird (BT-Drs. 19/17741, S. 1), eindämmen, indem u. a. das materielle Strafrecht im Bereich der Beleidigungsdelikte und der Bedrohung geschärft und eine Meldepflicht der Anbieter sozialer Netzwerke für bestimmte strafbare Inhalte (§ 3a NetzDG) geschaffen wurden; vgl. hierzu *Engländer*, Die Änderungen des StGB durch das Gesetz zur Bekämpfung des Rechtsextremismus und der Hasskriminalität, NStZ 2021, 385 ff.; zum rechtspolitischen Streit im Gesetzgebungsverfahren vgl. *Neuerer*, Neuer Streit über Gesetz gegen Hass im Internet, handelsblatt.com v. 16.1.2020.

III. Spannungsfeld zwischen Recht auf Privatsphäre und Recht auf Sicherheit

Derartige Konflikte sind nicht neu. Seit Gründung der Bundesrepublik versucht die Gesellschaft die Balance zu finden zwischen dem individuellen Recht auf Privatsphäre und dem Recht jedes Einzelnen auf Sicherheit bzw. Schutz vor und Aufklärung von Straftaten, vor allem wenn diese – wie es das Bundesverfassungsgericht für Straftaten „mit dem Gepräge des Terrorismus" formuliert hat – „auf eine Destabilisierung des Gemeinwesens" zielen.[19] Immer wieder aufs Neue verschiebt der unumgängliche technologische Fortschritt das Gleichgewicht in die eine oder andere Richtung.[20] Genau dies geschieht gerade durch die immer weiter entwickelten Methoden der Verschlüsselung oder Anonymisierung in der digitalen Welt – zu Lasten der Sicherheit. Unsere Fachtagung „Going dark – Signals Intelligence im IT-Zeitalter" hat es sich zum Ziel gesetzt, dieses komplexe Spannungsfeld aus verschiedenen Blickwinkeln zu beleuchten, und will einen Beitrag dazu leisten, fachlich fundierte und praktisch umsetzbare Lösungen zu suchen.

Begeben wir uns also gemeinsam auf den Weg, das Thema „Going dark" zu erhellen.

[19] BVerfGE 141, 220 Rn. 96 (BKA-Gesetz).

[20] *Tait*, Testimony before the United States Senate Judiciary Committee at a Hearing Entitled „Encryption and Lawful Access: Evaluating Benefits and Risks to Public Safety and Privacy", presented December 10, 2019, S. 1, https://www.judiciary.senate.gov/imo/media/doc/Tait%20Testimony.pdf (zuletzt aufgerufen am 20.7.2022).

Rechtspraktischer Standpunkt: (Kein) Recht auf Sicherheit im Internet?

Joachim Herrmann

I. „Going dark" als existenzielle Herausforderung für die innere Sicherheit

Der islamistische Attentäter von Würzburg, der im Juli 2016 in einem Regionalzug mehrere Menschen mit einer Axt und einem Messer schwer verletzte, wurde sogar noch während der Tatausführung von IS-Hintermännern im Nahen Osten über verschlüsselte Messengernachrichten „ferngesteuert"; ebenso übrigens auch der Ansbacher Attentäter, der wenige Tage später mit einem Sprengsatz sich selbst tötete und dabei 15 Menschen verletzte und zuvor, als er nicht durch die Polizeisperrung kam, ausdrücklich nachfragte, was er denn jetzt tun sollte.[1] Auch Anis Amri schickte bei seinem schrecklichen Anschlag im Dezember 2016 auf dem Berliner Breitscheidplatz noch während der Fahrt mit dem gestohlenen Lkw über Telegram Nachrichten an Dritte.[2] Das alles zeigt die große Bedeutung, die modernen Kommunikationsmitteln heutzutage auch bei Attentaten zukommt.

Wenn solche brutalen und verheerenden Attentate begangen werden, stellen sich die Bürgerinnen und Bürger zu Recht die Frage: Hätten die Sicherheitsbehörden das nicht verhindern können? In Gerichtsverfahren, Parlamentarischen Untersuchungsausschüssen und wissenschaftlichen Gutachten werden diese Fälle dann ja mit enormem Aufwand untersucht. Und ja, es finden sich dann auch immer wieder Hinweise, dass Informationen bisweilen nicht berücksichtigt, falsch eingeordnet oder nicht rechtzeitig weitergegeben wurden. Wenngleich wir auf Bundesebene feststellen können, dass mit der Einrichtung der entsprechenden Terrorabwehrzentralen sowohl gegen islamistische Anschläge wie auch gegen rechtsextremistische Anschläge der Informationsaustausch zwischen den verschiedenen Sicherheitsbehörden von Bund und Ländern wesentlich besser geworden ist und das auch die Grundlage dafür war, dass in den letzten Jahren

[1] Vgl. *Rieger/Frischlich/Rack/Bente*, Digitaler Wandel, Radikalisierungsprozesse und Extremismusprävention im Internet, in: Ben Slama/Kemmesies (Hrsg.), Handbuch Extremismusprävention, S. 373 unter Verweis auf *Leyendecker/Mascollo*, Die Chats der Attentäter von Würzburg und Ansbach mit dem IS, sueddeutsche.de v. 14.9.2016.

[2] Vgl. den Bericht des „Amri-Untersuchungsausschusses" des Deutschen Bundestags, BT-Drs. 19/30800, S. 232 ff.; *Sydow*, Flucht von Anis Amri: 77 Stunden quer durch Europa, spiegel.de v. 5.1.2017.

eine Reihe von Anschlägen rechtzeitig verhindert werden konnten.[3] Ich will aber schon auch deutlich sagen: Wer die Frage, warum so etwas passieren konnte, wenn es dann doch geschieht, allein mit behördlichen und damit letztendlich auch menschlichen Fehlern beantworten will, verschließt die Augen davor, dass wir es hier zugleich mit strukturellen Problemen ganz grundsätzlicher Art zu tun haben. Sie ergeben sich aus den enormen Fortschritten der Informationstechnik und nehmen dabei völlig neue Dimensionen an: Drastisch vor Augen geführt hat uns das im vergangenen Jahr der Fall EncroChat, einem Instant-Messengerdienst, der ein verschlüsseltes Kommunikationsnetz mit speziellen Kryptohandys anbot. Nachdem es im Rahmen von Ermittlungen, die durch Europol koordiniert wurden, französischen und niederländischen Behörden gelungen war, sich Zugriff auf einen Server von EncroChat zu verschaffen, bestätigte sich ein schrecklicher Verdacht: Das Netzwerk wurde fast ausschließlich von der Organisierten Kriminalität (OK) genutzt – allein im zweiten Quartal 2020 konnten die Behörden mehr als 100 Millionen Nachrichten mitlesen.[4] Vor den Augen der Ermittler öffnete sich das Tor zu einer Welt voller Abgründe, in der Brutalität und Grausamkeit an der Tagesordnung stehen.[5] Nach Mitteilung des Bundeskriminalamts (BKA) wurden allein in Deutschland bislang mehr als 2.250 Ermittlungsverfahren eingeleitet, mehr als 750 Haftbefehle vollstreckt und mehrere Tonnen an Drogen sichergestellt.[6] Viele der Verdächtigten verfügten über illegale Waffen, teilweise sogar verbotene Kriegswaffen.

---

[3] Bundesinnenminister *Horst Seehofer* hat kürzlich die Zahl der seit dem Jahr 2000 verhinderten Terroranschläge mit 23 beziffert, vgl. die Pressemeldung: Seehofer zu Terrorismusgefahr: 23 Anschläge seit 2000 verhindert, tagesschau.de v. 11.9.2021. Zur Bilanz verhinderter jihadistischer Terroranschläge siehe ferner die Antwort der Bundesregierung auf eine Kleine Anfrage von Abgeordneten und der Fraktion Die Linke, BT-Drs. 19/17610.

[4] Vgl. *Borchers*, Staatlich abgehörter Messenger – Der kriminalistische Fallout von EncroChat, c't 2021, Heft 17, S. 130 f.; *Klaubert*, EncroChat-Ermittlungen: Whatsapp der organisierten Kriminalität, faz.net v. 6.7.2021.

[5] Vgl. *Süddeutsche Zeitung*, Polizei entdeckt mutmaßliche Folterkammer, sueddeutsche.de v. 7.7.2020.

[6] Vgl. *Bundeskriminalamt,* Bundesweite Ermittlungen nach der Auswertung von Encrochat-Daten erfolgreich; Pressemitteilung v. 6.7.2021; zur Verwertbarkeit der Daten im Strafprozess vgl. OLG Bremen, Beschl. v. 18.12.2020 – 1 Ws 166/20, NStZ-RR 2021, 158 ff.; OLG Hamburg, Beschl. v. 29.1.2021 – 1 Ws 2/21, BeckRS 2021, 2226; OLG Köln, Beschl. v. 31.3.2021 – 2 Ws 118/21, BeckRS 2021, 18722; OLG Schleswig, Beschl. v. 29.4.2021 – 2 Ws 47/21, BeckRS 2021, 10202; OLG Rostock, Beschl. v. 11.5.2021 – 20 Ws 121/21, BeckRS 2021, 11981; OLG Brandenburg, Beschl. v. 9.8.2021 – 2 Ws 113/21 (S), BeckRS 2021, 23902; OLG Celle, Beschl. v. 12.8.2021 – 2 Ws 250/11, BeckRS 2021, 24319; KG, Beschl. v. 30.8.2021 – 2 Ws 79, 93/21, BeckRS 2021, 24213; *Pauli*, Zur Verwertbarkeit der Erkenntnisse ausländischer Ermittlungsbehörden – EncroChat, NStZ 2021, 146 ff.; a. A. *Derin/Singelnstein*, Verwendung und Verwertung von Daten aus massenhaften Eingriffen in informationstechnische Systeme aus dem Ausland (Encrochat), NStZ 2021, 449 ff.; vgl. ferner *Sehl*, „Encrochats" vor deutschen Gerichten: Der verbotene Datenschatz aus Frankreich?, lto.de v. 11.8.2021.