HEINRICH BÖLL STIFTUNG
INTERNATIONALE POLITIK

E-PAPER

Vorder-, Hinter- & Falltüren:

Zum staatlichen Umgang mit Verschlüsselung

GPPi
GLOBAL PUBLIC POLICY INSTITUTE

MIRKO HOHMANN

Eine Publikation der Heinrich-Böll-Stiftung, Januar 2018

Vorder-, Hinter- & Falltüren: Zum staatlichen Umgang mit Verschlüsselung

Von Mirko Hohmann

Inhaltsverzeichnis

Zusammenfassung

Seit Jahrzehnten schwelt der Streit um die Nutzung und mögliche Regulierung von Verschlüsselungstechnologien. Auf der einen Seite wird gefordert, dass Nutzer ihre Daten mithilfe starker Verschlüsselung uneingeschränkt schützen dürfen sollen, und zwar nicht nur vor dem Zugriff von Kriminellen oder Unternehmen, sondern auch vor staatlichem Zugang. Auf der anderen Seite argumentieren einige Vertreter von Sicherheits- und Strafverfolgungsbehörden, dass keine Technologie so entwickelt sein dürfe, dass sie einen Zugriff durch den Staat unmöglich macht. Sie führen in dem Zusammenhang an, dass sie in einem veränderten technischen Umfeld immer häufiger im Dunkeln tappen («going dark»), da ihnen wichtige Informationen auf Grund einer stärkeren Nutzung von Verschlüsselungstechnologien nicht zugänglich sind.

In regelmäßigen Abständen fordern staatliche Vertreter daher, Zugriffsmöglichkeiten zu Daten auf Speichermedien oder Kommunikationsdaten gesetzlich und technisch zu verankern. Diese müssten auf Vorlage eines Durchsuchungsbefehls zugänglich sein. Während der ersten großen Diskussion um das Thema in den 1990er Jahren wurde ein direkter Zugang zu Geräten gefordert, also vorbei an den Unternehmen durch die «Hintertür.» In den letzten Jahren werden vermehrt Regulierungen vorgeschlagen, die Unternehmen zwingen würden, ihre Technologie so zu entwickeln, dass sie den Behörden gewünschte Daten im Zweifel zur Verfügung stellen können; der Zugriff erfolgt also durch die «Vordertür.»

Während staatliche Behörden in die Lage versetzt werden müssen, den durch die Digitalisierung entstandenen Herausforderungen zu begegnen, sind die Forderungen nach einem gesetzlich garantierten Zugang weder zielführend noch wünschenswert – aus drei Gründen:

- **Mangelnde Notwendigkeit:** Während Behördenvertreter argumentieren, dass sie vermehrt «im Dunkeln» tappen, lässt sich im Gegenteil anführen, dass wir uns im «goldenen Zeitalter der Überwachung» befinden. Denn immer mehr Kommunikation findet online statt und lässt sich entsprechend nachverfolgen und mithören. Beide Argumentationslinien werden oft nur anekdotisch gestützt. Eine im Rahmen der Studie durchgeführte Analyse öffentlich verfügbarer Daten zu Problemen der Behörden mit Verschlüsselungstechnologien legt allerdings keine zwingende Notwendigkeit für neue Lösungen nahe.
- **Unklare Umsetzung:** Weltweit existieren hunderte verschiedener Verschlüsselungstechnologien; fast die Hälfte davon ist kostenlos online verfügbar. Es ist daher zu bezweifeln, dass Regulierungen einzelner Staaten einen nachhaltigen Effekt auf die Verfügbarkeit solcher Technologien für Kriminelle hätten, da sich immer Ausweichmöglichkeiten finden lassen. Zudem ist unklar, wie Forderungen nach staatlichem Zugang technisch umgesetzt werden sollten.
- **Negative Auswirkungen:** Während die Notwendigkeit und Umsetzung möglicher Regulierungen unklar bleiben, lassen sich die negativen Externalitäten solcher

Maßnahmen konkret aufzeigen. Diese würden:

1) die IT-Sicherheit der Nutzer durch neue Schwachstellen schmälern,
2) das Vertrauen in die Technologieindustrie gefährden und
3) autoritären Staaten, die seit Jahren einen solchen Zugriff fordern, Auftrieb geben und so Menschenrechte weltweit bedrohen.

Anstatt vage Forderungen zur Unterwanderung von Verschlüsselungstechnologien zu stellen, sollten Behörden ihren Fokus auf alternative Ermittlungsmethoden lenken, um Risiken für die öffentliche Sicherheit auch im digitalen Raum effektiv zu begegnen. Konkret bieten sich dabei Reformen in den folgenden Bereichen besonders an:

- **Personal und Ausbildung:** Durch den digitalen Fortschritt wandeln sich auch die Anforderungen an Ermittlungsarbeit konstant. Behörden sollten bei dieser Arbeit deshalb durch mehr IT-Spezialisten gestärkt werden. Außerdem ist es notwendig, das Wissen um den Umgang mit digitalen Beweismitteln sowie neue Methoden und Taktiken durch Maßnahmen wie Trainings gezielt zu fördern – in Sicherheits- und Strafverfolgungsbehörden ebenso wie in den Staatsanwaltschaften und Gerichten.
- **Reform der internationalen Rechtshilfe:** Wenn Daten außerhalb der Jurisdiktion eines Staates liegen und die nationalen Behörden deshalb keinen Zugriff darauf haben, sind diese im ersten Moment genauso wenig hilfreich wie verschlüsselte Daten. Mit Blick auf die Internationalität der digitalen Wirtschaft ist es daher notwendig, die internationale Rechtshilfe neu aufzusetzen, um grenzüberschreitende Ermittlungen zu vereinfachen.
- **Staatliches Hacking:** Durch die Online-Durchsuchung oder die Quellen-Telekommunikationsüberwachung können Behörden Verschlüsselungstechnologien umgehen, da sie so auf Daten auf dem Endgerät zugreifen können, bevor diese verschlüsselt werden. Solche staatlichen Hacking-Methoden, die in der Regel Schwachstellen in Soft- und Hardware ausnutzen, werden im digitalen Zeitalter eine zunehmend wichtige Rolle spielen, sind aus guten Gründen aber auch höchst umstritten. Umso notwendiger ist es, offene technische und rechtliche Fragen zu klären und von staatlicher Seite möglichst transparente Prozesse für das Management von Schwachstellen zu erarbeiten, um diese an die Hersteller weiterzugeben.

Umstrittenen Forderungen nach Vorder- oder Hintertüren für staatliche Akteure kann mit Reformen in diesen Bereichen begegnet werden. Entsprechend sollten sich alle beteiligten Anspruchsgruppen – auch der Privatsektor und die Zivilgesellschaft – in einen konstruktiven Dialog hierzu einbringen. So lässt sich auch verhindern, dass andere strittige Ermittlungsmethoden wie die Vorratsdatenspeicherung oder Bemühungen zur Datenlokalisierung weiter vorangetrieben werden. Abschließend ist noch einmal zu betonen, dass es jenen Vertretern von staatlicher Seite, die eine Regulierung von Verschlüsselungstechnologien fordern, obliegt, die Notwendigkeit solcher Reformen ebenso wie ihre technische Umsetzung klar und überzeugend darzulegen. Was die Begründung und Informationsvermittlung anbelangt, sind sie hier in der Bringschuld.

Einleitung

Wie kaum ein anderes Thema versinnbildlicht die Diskussion um die Verwendung von Verschlüsselungstechnologien die Frage nach den Fähigkeiten und Grenzen von Sicherheits- und Strafverfolgungsbehörden im digitalen Umfeld. Die einen fordern, Nutzer sollten ihre Daten mithilfe starker Verschlüsselung komplett vor dem Zugriff durch Unternehmen, Kriminelle und Sicherheitsbehörden schützen können. Die anderen meinen, Informationen auf Smartphones und die Kommunikation zwischen Nutzern müssten für Ermittler im Zweifel einsehbar sein, um deren Fähigkeit zur Gefahrenerkennung und Aufklärung von schweren Straftaten zu bewahren. Im Spannungsfeld zwischen öffentlicher Sicherheit und der informationellen Selbstbestimmung von Nutzern stellen sich schwierige Fragen: Über welche Wege sollen staatliche Behörden an die Daten von Kriminellen gelangen? Wo setzen Bürgerrechte solchen Zugriffen Grenzen? Und wie sollten Technologien, die sowohl für legale als auch illegale Zwecke eingesetzt werden können, reguliert werden?

Die Debatte um Verschlüsselung wird in diesem Zusammenhang mit besonderer Vehemenz geführt. Spezielle Aufmerksamkeit erregt der Streit zwischen Apple und dem US-amerikanischen Federal Bureau of Investigation (FBI) im Jahr 2015, als Apple nicht Willens war, die Sicherheitsmechanismen auf dem iPhone eines Terroristen zu umgehen – obwohl das FBI einen entsprechenden Gerichtsbescheid vorgelegt hatte. Im Anschluss wurden die Forderungen nach staatlicher Regulierung von Verschlüsselungstechnologien laut, eine Forderung, die schon in den 1990er Jahren breit diskutiert wurde. Die Obama-Administration entschied sich allerdings, auf einen kooperativen Austausch mit den Unternehmen zu setzen und keine Gesetzesänderungen voranzubringen.[1][2] US-Präsident Trump forderte noch im Wahlkampf, man müsse iPhones «öffnen» können, und auch andere Mitglieder seines Kabinetts äußerten sich ähnlich.[3][4] Noch haben sie ihren Worten aber keine Taten folgen lassen.

Auch in Europa nahm die Diskussion an Fahrt auf. Laut dem 2016 verabschiedeten Investigatory Powers Bill in Großbritannien müssen Unternehmen auf Anordnung des Staates «elektronische Sicherungen» von Daten entfernen.[5] In der Schweiz können Telekommunikationsanbieter dazu verpflichtet werden, die Kommunikation von Individuen an die Behörden zu übermitteln und «[v]on ihnen angebrachte Verschlüsselungen» zu löschen.[6] In Deutschland haben solche Forderungen bisher keine Mehrheit, aber auch hier gibt es immer wieder Rufe danach, dass jedwede Kommunikation mitgelesen werden können müsse.[7]

Die USA nehmen in dieser Diskussion aus verschiedenen Gründen eine besondere Rolle ein. Erstens haben alle großen Technologieunternehmen, um deren Daten beziehungsweise Verschlüsselung sich die Diskussion dreht, ihren Sitz dort. Hierzu gehören Apple, Facebook (sowie dessen Tochterunternehmen WhatsApp) und Google. Zweitens führt diese Konzentration an relevanten Unternehmen in den USA dazu, dass der regulatorische Ansatz der US-Regierung einen besonderen Einfluss auf die Verbreitung (oder Einschränkung) von Verschlüsselungsmethoden hat. Verstärkt wird dies dadurch, dass die USA den weltweit größten Absatzmarkt für Technologieprodukte stellen und somit durch ihre

Entscheidungen auch ausländische Unternehmen beeinflussen können. Drittens wird die Diskussion zu dem Thema nirgendwo so öffentlich und intensiv geführt wie in den USA. Sicherheits- und Strafverfolgungsbehörden beziehen eindeutig Stellung und im Kongress werden verschiedene Gesetzesvorstöße diskutiert; gleichzeitig setzen sich Wissenschaftler und Aktivisten intensiv mit dem Thema auseinander und publizieren regelmäßig zu der Thematik.

In Europa sind zwar die technischen Rahmenbedingungen und die damit einhergehenden Probleme in der operativen Arbeit der Behörden ähnlich, die Herausforderungen gestalten sich allerdings noch komplizierter. Denn die USA haben aufgrund der Dichte an Technologieunternehmen einen besseren Zugang zu den Unternehmen und damit auch Zugriff auf ihre Daten. Für europäische Nationen stellen somit nicht nur verschlüsselte Daten ein Problem dar, sondern auch lesbare Daten, die aber auf amerikanischen Servern liegen.

Ziel der Studie ist es, die verschiedenen Argumentationsmuster für und gegen die unterschiedlichen Regulierungen von Verschlüsselungstechnologien anhand der Debatte in den USA herauszuarbeiten und zu bewerten. Denn aus Sicht staatlicher Behörden machen die Forderungen nach einer Regulierung von Verschlüsselungstechnologien auf den ersten Blick durchaus Sinn: Man möchte nichts unversucht lassen, um an die Informationen möglicher Krimineller zu gelangen. Wie im Folgenden gezeigt wird, greift diese Argumentation aber zu kurz. Denn die zunehmende Digitalisierung schafft auch für Ermittler ganz neue Möglichkeiten und es fehlt bisher der Nachweis der tatsächlichen Notwendigkeit einer solchen Regulierung, die immer auch negative Auswirkungen, beispielsweise auf die wirtschaftliche Entwicklung von Ländern, Persönlichkeitsrechte und im Bereich der Meinungsfreiheit hätte. Zudem bleiben wichtige Fragen bezüglich der Umsetzung einer Regulierung und ihrer tatsächlichen Wirksamkeit offen. Eine Ausführung dieser Argumente erfolgt im ersten Teil.

Aufbauend auf dieser Analyse werden im zweiten Teil Möglichkeiten staatlicher Behörden diskutiert, an die Daten von Verdächtigen und Kriminellen zu gelangen, ohne dass Verschlüsselung beeinträchtigt werden müsste. Denn es ist nicht zu leugnen, dass Ermittler durch deren Einsatz vor zunehmende Herausforderungen gestellt werden. Um mögliche Kurzschlussreaktionen in dieser sehr emotional geführten Diskussion zu vermeiden, gilt es schon jetzt, Überlegungen zu den Möglichkeiten der Ermittler in einer verschlüsselten Welt anzustellen. Diese erstrecken sich über den Ausbau des Personals, über eine verbesserte internationale Rechtshilfe bis hin zu staatlich reguliertem Hacking.

Teil I
Verschlüsselung: Eine umkämpfte Technologie

Einführung: Verschlüsselungstechnologien

Was so abstrakt klingt, berührt die Meisten von uns tagtäglich. Oft ohne es zu wissen, kommen Nutzer regelmäßig in Kontakt mit verschiedenen Verschlüsselungstechnologien. Diese sichern Internetseiten, werden beim Transfer von persönlichen Daten oder Finanztransaktionen online eingesetzt, tragen dazu bei, dass Festplatten nur ihren legitimen Nutzern zur Verfügung stehen und sind Teil vieler E-Mail- und Messenger-Anbieter.

Auch wenn es Unterschiede in den Technologien gibt, ist die Grundidee immer gleich: Durch einen Algorithmus werden lesbare Daten («Klartext,» im Englischen «plaintext») in unlesbare Daten («Geheimtext,» im Englischen «ciphertext») umgewandelt.[8] Die Rückumwandlung in lesbaren Text – die Entschlüsselung – ist nur durch einen bei der Verschlüsselung verwendeten Schlüssel möglich. So werden zwei Grundpfeiler der IT-Sicherheit gestärkt: die Vertraulichkeit und Integrität von Daten, also deren Schutz vor unbefugter Preisgabe und ihre Unversehrtheit.[9] Denn ohne den korrekten Schlüssel lassen sich die Daten nicht lesen oder verändern. Häufig dient Verschlüsselung auch der Authentifizierung und stellt sicher, dass man online mit der korrekten Person oder Website kommuniziert.[10]

Es ist wichtig, zwischen zwei Arten der Verschlüsselung zu unterscheiden: Die Verschlüsselung von Daten auf Speichermedien («data at rest») und von Daten bei der Übertragung («data in motion»).[11] Verschlüsselte Speicherung bezieht sich zum Beispiel auf Bilder, Videos und Nachrichten, die sich auf Computern, Smartphones, Tablets und externen Festplatten befinden.[12] Ergänzend dazu sichert die verschlüsselte Übertragung die Kommunikation zwischen zwei oder mehreren Geräten oder Nutzern in der Form von Telefonaten, E-Mails, Chats und online-Transaktionen. Verdeutlichen lässt sich der Unterschied an Cloud-Anwendungen: Dort werden Daten idealerweise sowohl bei der Übertragung in die Cloud verschlüsselt als auch bei der Speicherung in der Cloud. So haben zu jedem Zeitpunkt nur der Nutzer und Anbieter Zugriff auf die lesbaren Daten; in vielen Fällen kennt sogar nur der Nutzer den für die Entschlüsselung nötigen Schlüssel.

«Going dark!»: Die Positionen der Sicherheits- und Strafverfolgungsbehörden

Aufgrund der weiten Verbreitung sowie der zunehmenden Digitalisierung unserer Leben lassen sich solche Sicherheitstechnologien nicht mehr aus dem Alltag wegdenken. Milliarden Nutzer, Unternehmen, Regierungen und andere Organisationen verlassen sich darauf.

Gleichzeitig setzen auch Verbrecher Verschlüsselung vermehrt ein, um ihre Daten vor dem Zugriff des Staates zu sichern. Dies stellt Sicherheits- und Strafverfolgungsbehörden zunehmend vor Herausforderungen bei ihren Ermittlungen. Behörden in einer Vielzahl an Ländern haben die Diskussion um die – aus ihrer Sicht – Nachteile der Technologie daher in den letzten Jahren in den öffentlichen Raum gebracht. Stellvertretend für den teilweise sehr heterogenen Staatsapparat meldete sich in den USA der ehemalige Chef des Federal Bureau of Investigation (FBI), James Comey, in verschiedenen Anhörungen, Vorträgen und Interviews zu Wort.[13][14] Zentral in seiner Argumentation ist die Aussage, dass das FBI und andere Behörden in vielen Fällen zwar die gesetzliche Ermächtigung besitzen, um eine Nachricht zu lesen oder ein Telefonat abzuhören, ihnen aber die technischen Möglichkeiten fehlen, dies auch tatsächlich zu tun – da die Daten verschlüsselt sind. Somit drifteten die Behörden immer weiter ins Dunkle ab, im Englischen spricht man vom «going dark.» Diese Entwicklung gefährde die öffentliche Sicherheit.

Das Argument lässt sich auf die Unterschiede der Verschlüsselung herunterbrechen: Für «data in motion» konnten die Behörden in der Vergangenheit Telefon- und Mobilfunkunternehmen verpflichten, Schnittstellen vorzuhalten, um bei Vorlage eines richterlichen Beschlusses die Gespräche individueller Verdächtiger mitzuhören oder Textnachrichten zu lesen. Diese Möglichkeit liegt nicht mehr vor, wenn Nutzer Anwendungen wie WhatsApp oder Signal nutzen, die die Kommunikation so Ende-zu-Ende verschlüsseln, dass nur noch die Nutzer selbst Zugang zu dem Klartext haben. Ähnlich verhält es sich für «data at rest»: Während Behörden in der Vergangenheit mit der Festplatte oder Smartphone und einem richterlichen Beschluss in der Hand durch den Hersteller des Gerätes Zugang erhalten konnten, setzen letztere vermehrt auf solch sichere Verschlüsselung, dass sie selbst keinen Zugriff mehr haben. Was dem Nutzer erhöhte Sicherheit und Privatsphäre verspricht, ist den Behörden ein Dorn im Auge.[15]

Ex-FBI Direktor Comey und andere staatliche Vertreter argumentieren, dass die zunehmende Verschlüsselung Konsequenzen auf verschiedenen Ebenen hat.[16] Erstens wirke sie sich auf die Fähigkeiten der Behörden aus, Verbrechen zu vermeiden, da die Planung illegaler Aktivitäten wie Drogenhandel oder terroristische Anschläge «im Dunkeln» durchgeführt werden könne. Zweitens werde die Verfolgung von Straftaten erschwert, da das Erheben von digitalen Beweisen – in der Form von lesbarer Kommunikation – mit erheblichem Aufwand verbunden und oft unmöglich sei. Alles in allem würden neue Arten der Kommunikation so zu erheblicher Verzögerung führen und die Behörden zwingen, Ressourcen für Ermittlungsarbeiten aufzubringen, die dann nicht anderweitig eingesetzt werden könnten.[17]

Ein neues technisches Umfeld

Aus Sicht staatlicher Dienste ist nicht die Existenz der Verschlüsselung das Problem, denn diese gibt es seit Jahrzehnten und wird es definitiv weiterhin geben. Vielmehr geht es um das Zusammenspiel zweier technischer Entwicklungen: Erstens findet Kommunikation mehr denn je digital statt. Zweitens hat sich die tatsächliche Anwendung von

Verschlüsselungstechnologien dramatisch erhöht, vor allem aufgrund der Bemühungen von Unternehmen, solche Technologien immer nutzerfreundlicher anzubieten.

Der erste Trend ist wenig überraschend. Während online-Kommunikation noch vor 20 Jahren ein Nischenphänomen war, lässt sich diese heute nicht mehr wegdenken. Statt Briefen werden E-Mails verschickt, Telefonate werden per Internet geführt, soziale Medien und Chat-Anwendungen sind die Norm, und zwar für legale und illegale Zwecke. Um das zu verdeutlichen: Im Jahr 2016 wurden weltweit 21 Millionen WhatsApp-Nachrichten verschickt, 150 Millionen E-Mails verschickt und 350.000 Tweets erstellt – in jeder einzelnen Minute.[18]

Zweitens findet diese Kommunikation in einem immer sichereren Umfeld statt. Das liegt vor allem an der Rolle einiger (amerikanischer) Technologie-Unternehmen. Nach den Enthüllungen von Edward Snowden schlug nicht nur der US-Regierung, sondern auch vielen amerikanischen Firmen eine Welle des Misstrauens entgegen. Um dieser zu begegnen und auf die höhere Nachfrage nach stärker geschützten Produkten zu reagieren, erhöhten Firmen wie Microsoft, Apple, Facebook und Google rasant die Sicherheit vieler ihrer Produkte, oft in Form verbesserter Verschlüsselungstechnologien. Zudem reagierte der Markt für Smartphone-Anwendungen entsprechend, sodass das Angebot an verschlüsselten Kommunikationsmöglichkeiten rasant stieg.[19] Ganz allgemein stieg in den letzten Jahren das Angebot sogenannter Over-The-Top-(OTT)-Dienste, also von online-Diensten, die über Apps und Geräte ohne die Einbindung von Internet- und Telekommunikationsanbietern laufen. Das Besondere an diesen OTT-Diensten wie WhatsApp oder Skype ist, «dass die Betreiber auf die Kontrolle solcher digitalen Leistungen [keinen] wesentlich Einfluss nehmen (können).»[20] So können zum Beispiel keine Schnittstellen eingesetzt werden.

Als Resultat dieser Trends sind sichere Informations- und Kommunikationstechnologien, die in der Vergangenheit mit viel Aufwand verbunden waren und ein gutes technisches Verständnis voraussetzten, heute oft nur einen Klick entfernt. Einen weiteren Unterschied macht, dass die Technologien nicht mehr auf das Zutun der Nutzer vertrauen, sondern standardmäßig eingesetzt werden.[21] Ein Beispiel hierfür ist die Entscheidung von WhatsApp, auf Ende-zu-Ende Verschlüsselung umzustellen. Durch ein Software-Update erhielten so von heute auf morgen über eine Milliarde Nutzer Zugang zu einer Kommunikationsmethode, die für staatliche Behörden nicht mitzulesen ist.[22] Zudem bemühen sich viele Unternehmen, die eigenen Möglichkeiten der Wiederherstellung verschlüsselter Daten zu reduzieren. Konkret heißt das zum Beispiel, dass es selbst für Anbieter wie Apple nicht möglich ist, eigene Smartphones der aktuellsten Generation auszulesen, weder auf Nachfrage der Nutzer bei Verlust des Passworts noch aufgrund einer richterlichen Anordnung.[23][24] Für Behörden bedeutet das, dass der Umweg des Zugriffs über Unternehmen keine Option mehr ist, was zum Beispiel zu dem Streit nach dem Anschlag in San Bernadino führte.[25][26]

Die Forderungen: Hinter- und Vordertüren

Als Resultat dieser Entwicklungen forderten Vertreter von Sicherheitsbehörden andere Wege, um sich für Ermittlungen Zugang zu relevanten, verschlüsselten Daten zu verschaffen. Hier lassen sich zwei Forderungen unterscheiden:[27] Bereits in den 1990er Jahren gab es Forderungen nach «Hintertüren», also direkte Zugriffsmöglichkeiten der staatlichen Behörden auf Verschlüsselungstechnologien. In den letzten Jahren wurden weniger spezifische Forderungen laut und Behörden versuchten, die Unternehmen lediglich dazu zu verpflichten, den Gerichtsbescheiden zu folgen, ohne vorzuschreiben, wie.

Hintertüren: Direkter Zugriff in den 1990er Jahren

Der Begriff der Hintertür bezieht sich auf einen Mechanismus, mit dem ein Akteur, wie zum Beispiel eine Sicherheitsbehörde, direkt auf verschlüsselte Daten zugreifen kann. Dies geschieht entweder über eine Kopie des privaten Schlüssels,[28] die dann bei der Regierung oder einer zivilgesellschaftlichen Organisation hinterlegt wird (auch «key escrow» genannt),[29] oder über eine bewusst eingebaute Schwachstelle im Algorithmus.

Die Idee ist simpel: Wie früher bei Telefonanlagen werden Schnittstellen eingebaut, über die Ermittler mit einem richterlichen Bescheid auf die Kommunikation von Individuen unverschlüsselt zugreifen können – ohne, dass es die Verdächtigen mitbekommen. In den USA existiert für die Verpflichtung der Kommunikationsunternehmen zum Einbau einer Schnittstelle eine gesetzliche Grundlage (der «Communications Assistance for Law Enforcement Act»). Diese stammt allerdings aus dem Jahr 1994 und schließt moderne Kommunikationsmethoden daher nicht ein.[30]

Die Diskussion um mögliche Hintertüren wurde vor allem im ersten «Kryptokrieg» in den 1990er Jahren in den USA geführt. Damals schlug die Regierung um Bill Clinton vor, den sogenannten Clipper Chip als zusätzlichen Zugang in alle in den Vereinigten Staaten hergestellten Telekommunikationsgeräte einzubauen, um so einen de facto Zugang für die Regierung zu schaffen.[31][32] Gegen diese Idee stellte sich damals eine relativ heterogene Gruppe aus Internetaktivisten, Akademikern und Telekommunikationsunternehmen, was dazu führte, dass die Idee 1996 verworfen wurde. Die Regierung sprach sich von nun an dafür aus, die Nutzung von Verschlüsselungstechnologien zu vereinfachen, um amerikanischen Bürgern zu helfen, «ihre Privatsphäre, geistiges Eigentum und andere wertvolle Informationen zu schützen.»[33]

Vordertüren: Der Umweg über den Privatsektor

Vor allem Probleme mit der technischen Umsetzung stellten die Clinton-Administration vor große Herausforderungen.[34] Dies erkannten auch die Behörden an, was sich in der aktuellen Debatte widerspiegelt.[35] Im aktuellen, zweiten «Kryptokrieg» wurden Forderungen nach einem Mechanismus wie dem Clipper Chip selten vorgebracht. Stattdessen wurde die breite Forderung nach allgemeinem «lawful access», also gesetzlichem Zugang aufgestellt, die Ausführung aber nicht weiter definiert. Konkret heißt das, dass Unternehmen zwar Verschlüsselung nutzen können, sich aber die Möglichkeit offenhalten sollen, die Daten in

ihren eigenen Produkten auf Vorlage eines richterlichen Beschlusses entschlüsselt vorzulegen – wie, das bleibt ihnen überlassen.

Ein solcher Ansatz unterscheidet sich von dem, was oft als Hintertür beschrieben wurde, insofern, als dass Anbieter von Soft- und Hardware Zugang zu den Schlüsseln haben, und nicht die Regierung. Der Staat verlangt nicht eine spezielle Lösung, sondern er erlegt den Unternehmen die Pflicht auf, technische Unterstützung zu leisten, um verschlüsselte Daten zu lesen.[36] Der Bau der «Hintertür» wird also an die Unternehmen ausgelagert, bei welchen der Staat dann mit einem Gerichtsbescheid anklopfen kann. Daher auch der Begriff der «Vordertür.»

Die Art der Ausführung variiert. In den USA wurde im Jahr 2016 zum Beispiel der «Compliance with Court Orders Act» diskutiert. Der Vorschlag wendet sich an Software- und Hardwarehersteller, an Dienstleister elektronischer Kommunikation und andere Anbieter von Produkten zur Datenverarbeitung und -speicherung und nimmt diese in die Pflicht, jedweden Datensatz in Klartext umzuwandeln oder den Behörden bei der Umwandlung zu helfen.[37] Das Gesetz, das so keine Mehrheit gefunden hat, hätte also de facto alle Anbieter gezwungen, Nutzerdaten auslesen zu können. Ende 2017 sprach sich Rod Rosenstein, stellvertretender US-Justizminister, für die Entwicklung von «verantwortungsvoller Verschlüsselung» aus; einer aus seiner Sicht sicheren Verschlüsselung, die aber trotzdem auf einen Gerichtsbescheid hin lesbar sein müsste.[38]

In Großbritannien sieht der 2016 verabschiedete «Investigatory Powers Bill» vor, dass Unternehmen dazu gezwungen werden können, «elektronische Sicherungen» von Daten zu entfernen.[39] Das Gesetz ergänzt zwar, dass dies nur im «praktikablen» Rahmen stattzufinden habe; die Definition von Praktikabilität bleibt allerdings aus. Ähnlich gestaltet es sich in der Schweiz, wo Telekommunikationsdienstleister verpflichtet sind, bei Vorlage eines Gerichtsbescheids die Kommunikation an die Behörden zu übermitteln und «[v]on ihnen angebrachte Verschlüsselungen» zu entfernen.[40] Ähnliche Vorstöße finden sich zum Beispiel auch in Frankreich und Brasilien.[41] Selbst in Deutschland, wo sich die Regierung seit Jahrzehnten für sichere Informationssysteme stark macht, werden immer wieder vereinzelte Stimmen laut, die einen staatlichen Zugang einfordern.[42]

Die Kritik: Notwendigkeit, Umsetzung und externe Effekte

Wie schon in den 1990er Jahren vereint die Frage um einen möglichen staatlichen Zugang zu verschlüsselter Kommunikation eine große Bandbreite verschiedener Akteure, die sich gegen einen möglichen staatlichen Zugang aussprechen. Selbst aus staatlicher Sicht wird oft Zurückhaltung gefordert, Strafverfolgungs- und Sicherheitsbehörden sind hier keineswegs als homogene Gruppe zu verstehen. Die Argumente gegen mögliche Hinter- oder Vordertüren lassen sich grob in drei Gruppen aufteilen:

(1) Eine unterschiedliche Auffassung der von staatlichen Behörden angeführten Herausforderungen,

(2) Zweifel an der möglichen Umsetzbarkeit der Lösungsansätze, sowie

(3) die Warnung vor negativen Konsequenzen auf Nutzer und Wirtschaft.

Diese Argumente werden im Folgenden näher betrachtet, vor allem mit Bezug auf die in den letzten Jahren geforderten Möglichkeiten des rechtlichen Zugriffs.

Ist Zugriff notwendig?

Kritiker zweifeln zunächst an der Behauptung der Behörden, dass sie jetzt oder demnächst «im Dunkeln» tappen würden. Vielmehr habe die Digitalisierung dazu geführt, dass wir uns heute im «goldenen Zeitalter der Überwachung» befänden – mehr Überwachungsmöglichkeiten habe es nie gegeben.[43] Schließlich habe ein Großteil der Kommunikation bis vor wenigen Jahren offline stattgefunden und war somit viel schwieriger zu überwachen; selbst beim Abhören von Telefonaten war ein Live-Mitschnitt möglich, aber keine rückwirkende Ermittlung.[44]

Der Politologe Peter Swire argumentiert, dass die negativen Auswirkungen, die Verschlüsselungstechnologien auf die Überwachungsmöglichkeiten der Behörden haben, durch drei Trends mehr als ausgeglichen würden.[45] Erstens hätten die meisten Menschen heutzutage fast permanent ein Smartphone bei sich, das die Bewegungsabläufe der Nutzer speichert und so die Verfolgung von Verdächtigen erleichtert. Zweitens seien selbst bei verschlüsselter Kommunikation noch Aussagen darüber möglich, wer mit wem kommuniziert hat. Diese sogenannten Metadaten böten den Behörden hilfreiche Einblicke in das soziale Umfeld von Individuen. Drittens ließen sich durch das Zusammentragen von Informationen, die Privatunternehmen über einzelne Personen sammeln, ganze «digitale Dossiers» erstellen. Die Möglichkeit, so viele Informationen in so kurzer Zeit zusammenzutragen, habe es so nie gegeben. Das Verhalten der Sicherheits- und Strafverfolgungsbehörden erklärt Swire mit dem Phänomen der Verlustaversion: Die Verluste an Ermittlungstätigkeiten durch zunehmende Verschlüsselung wiegen bei den staatlichen Behörden schwerer als die tatsächlichen Gewinne an Möglichkeiten durch andere Technologien.[46]

Eine Studie des Berkman Centers der Universität Harvard, an der auch ehemalige Mitarbeiter verschiedener Sicherheitsbehörden mitwirkten, ergänzt diese Argumentation um zwei weitere Punkte:[47] Erstens sei es unwahrscheinlich, dass Verschlüsselungstechnologien wirklich universell eingesetzt werden würden. Die Geschäftsmodelle vieler Unternehmen beruhten auf Datenanalyse, welche durch Verschlüsselung erschwert würde. Auch die Rückgewinnung von verlorenen Daten, zum Beispiel bei Verlust eines Passworts durch den Nutzer, werde so erschwert. Zweitens weisen die Autoren auf die Entwicklung hin, dass im Rahmen des Internets der Dinge immer mehr Geräte online vernetzt würden. Dies schaffe ganz neue Überwachungsmöglichkeiten. In der Summe kommt die Studie daher zu dem Schluss, dass staatliche Behörden langfristig nicht im Dunkeln tappen würden, sondern ganz im Gegenteil mehr Ermittlungsansätze als in der Vergangenheit hätten.[48]

Die Datenlage

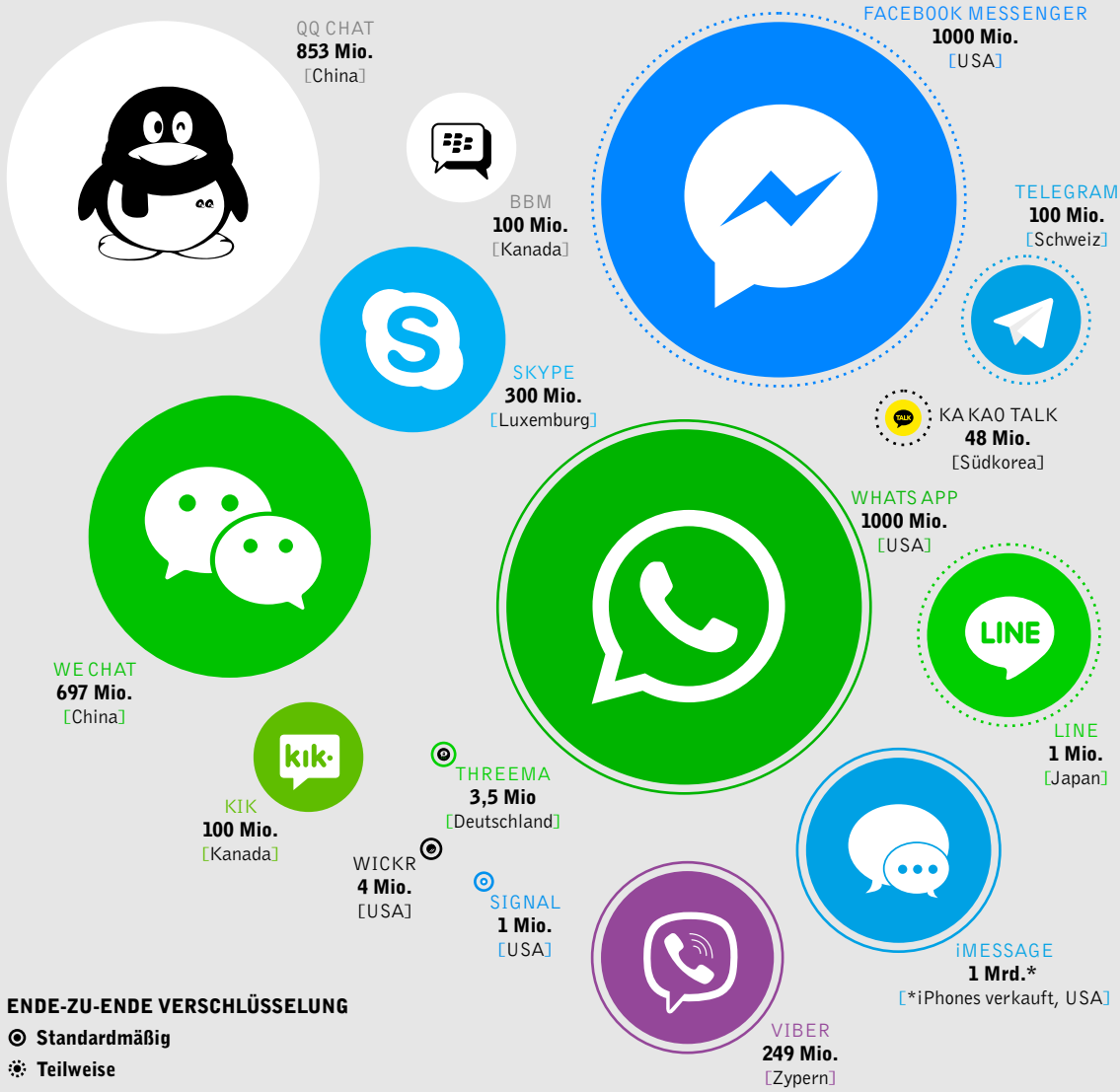
Leider ist die Datenlage nicht solide genug, um eine abschließende Einschätzung zu liefern, vor welche Herausforderungen Behörden durch Verschlüsselungstechnologien gestellt werden. Allerdings lassen verfügbare Daten einige erste Schlussfolgerungen zu.

In den USA wurden im Jahr 2016 3.168 Anträge zur Telekommunikationsüberwachung genehmigt.[49] Ein Großteil davon fiel auf Telefone, und dort besonders auf tragbare Geräte, also Handys, Smartphones oder Smartphone-Anwendungen. In insgesamt 57 Fällen stießen die Behörden auf verschlüsselte Kommunikation und in 80 Prozent der Fälle war es ihnen aufgrund dieser nicht möglich, ein Gespräch mitzuhören oder eine Nachricht mitzulesen. Diese Anzahl der Fälle ist zwar sehr gering, aus zwei Gründen lässt sich aber nicht daraus schließen, dass die Behörden keine Probleme haben. Erstens lässt sich ein starker Anstieg feststellen: Zwischen 2001 und 2015 kam es insgesamt nur 154 Mal vor, dass Verschlüsselung ein Problem darstellte.[50] Zweitens lässt sich argumentieren, dass in den meisten Fällen Anträge gar nicht erst gestellt werden, wenn sich herausstellt, dass Verschlüsselung verwendet wird, da die Erfolgsaussichten zu gering sind, um damit etwas zu erreichen[51].

Diese Sichtweise wird unterstützt durch Daten zur Nutzung verschlüsselter Kommunikation. Laut Schätzungen von Lewis, Zheng und Carter werden aktuell 18 Prozent der weltweiten Kommunikation über Messenger-Dienste Ende-zu-Ende verschlüsselt und sind somit zugänglich nur für die Nutzer selbst.[52] Eine Übersicht der größten Messenger-Dienste, ihrer Nutzerzahlen und der Art der Verschlüsselung lässt sich Grafik 1 entnehmen. Es gibt wenig Grund zur Annahme, dass die Zahl der illegitimen Nutzer solcher Technologien sich in der Breite stark von diesem Durchschnitt unterscheiden. Aus der Grafik lässt sich eine weitere Schlussfolgerung ziehen: So mag der weltweite Teil an unzugänglicher Kommunikation bei rund 18 Prozent liegen. Dieser Anteil erhöht sich aber schlagartig, wenn man sich auf westliche Staaten konzentriert, da hier Dienste wie Facebook, iMessage oder WhatsApp viel weiter verbreitet sind (während QQ Chat und WeChat fast nicht genutzt werden). Insofern ist die Wahrscheinlichkeit für westliche Dienste, in einer Ermittlung auf verschlüsselte Kommunikation zu stoßen, um einiges höher als die der chinesischen Ermittler.

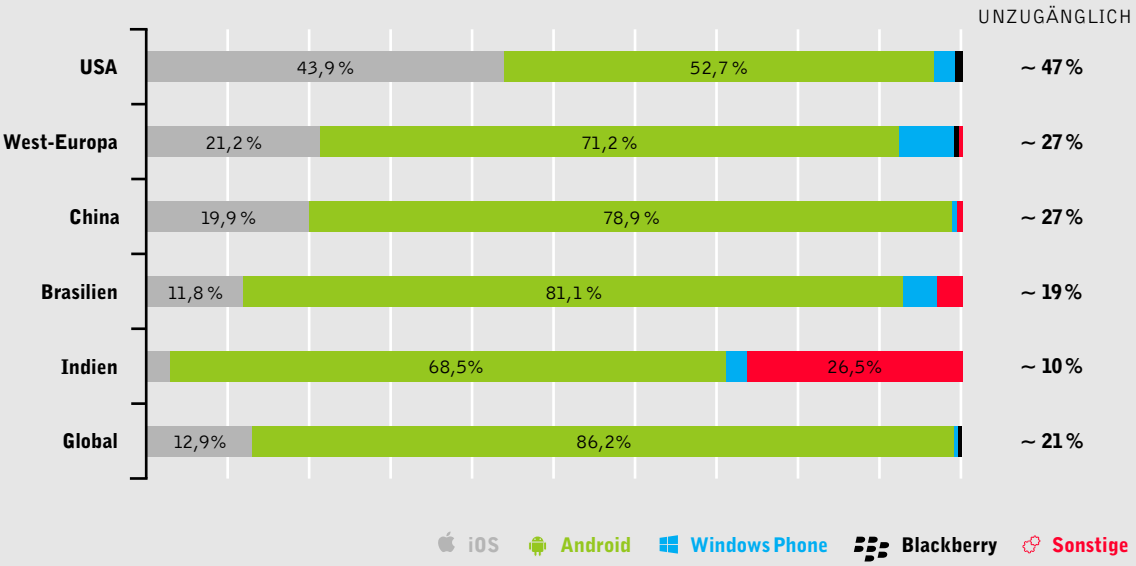
Neben den Daten zur verschlüsselten Kommunikation gibt es auch Informationen zu der Verschlüsselung von mobilen Endgeräten. Laut Apple lief im Oktober 2015 auf 91 Prozent aller iPhones eine Software, die Daten so verschlüsselt, dass sie für das Unternehmen selbst nicht mehr auslesbar sind.[53] Für Android-Geräte belief sich diese Nummer auf 23 Prozent.[54] Auf Grundlage dieser Daten in Kombination mit Nutzerdaten haben Lewis, Zheng und Carter den Anteil an Geräten, der Behörden weltweit unzugänglich ist, auf 21 Prozent geschätzt (siehe Grafik 2). Gleichzeitig ist auch hier wieder ein regionaler Trend zu erkennen: Aufgrund der schnelleren Updates und der verstärkten Nutzung von teureren (und oft sichereren) Geräten, liegen die Zahlen vor allem in Westeuropa und den USA besonders hoch – mit Anteilen von 27 beziehungsweise 47 Prozent der nicht lesbaren Geräte.

Abb.1: Verbreitung von Ende-zu-Ende Verschlüsselung in Messenger-Diensten weltweit
Nach monatlich aktiven Nutzer/innen und Ursprungsland



Quelle: James A. Lewis, Denise E. Zheng und William A. Carter The Effect of Encryption on Lawful Access to Communications and Data. CSIS Report. Washington, DC: Center for Strategic and International Studies, 2017; eigene Darstellung.

Abb.2: Anteil der unzugänglichen Geräte am Smartphone-Markt
Anteile der nicht zugänglichen Geräte basiert auf der Annahme, dass 95% der iOS-Geräte und 10% der Android-Geräte durch vollständige Verschlüsselung geschützt werden.



Quelle: James A. Lewis, Denise E. Zheng und William A. Carter The Effect of Encryption on Lawful Access to Communications and Data. CSIS Report. Washington, DC: Center for Strategic and International Studies, 2017; eigene Darstellung.

Ein letzter Indikator ist die Zahl der Smartphones, die Behörden vorliegen und die sie trotz eines entsprechenden gerichtlichen Bescheids nicht auslesen können. Diese Zahlen für die USA lassen sich Tabelle 1 entnehmen. In der Liste führend ist New York City, mit über 400 Geräten, zu denen es laut eigener Angabe keinen Zugriff gab. Um die Zahl in Kontext zu setzen, muss man erwähnen, dass die Staatsanwaltschaft des New York County jährlich über 100.000 Fälle bearbeitet.[55] Bei ungefähr 400 Geräten pro Jahr, die nicht ausgelesen werden können, bedeutet dies, dass in 0.4 Prozent der Fälle Probleme durch unzugängliche Geräte entstehen.

Tabelle 1:[56] Geräte ohne Zugriffsmöglichkeiten der Behörden

Behörde	Anzahl Geräte	Zeitraum
Staatsanwaltschaft New York City (Manhattan)	423	Okt. 2014–Okt. 2016
Polizei Los Angeles	300	Bis 2016
Polizei Charlotte-Mecklenburg	160	Bis 2016
Staatsanwaltschaft Suffolk County (Boston)	151	Bis 2016
Los Angeles County Sheriff	150	Bis 2016
Polizei Austin	45	Bis 2016
Regionales Computerforensiklabor Chicago	30	Erstes Halbjahr 2016

Quelle: Lewis, Zhang, and Carter, «The Effect of Encryption on Lawful Access to Communications and Data»: S. 15; eigene Darstellung.

In der Summe reichen die bisher öffentlich gemachten Zahlen nicht aus, um eine abschließende Schlussfolgerung zu den Herausforderungen durch Verschlüsselungstechnologien zuzulassen. Trotzdem ist es hilfreich, sich noch einmal vor Augen zu führen, mit welchem Blick Sicherheits- und Strafverfolgungsbehörden auf Informationstechnologien schauen. Diese lassen sich in drei Arten unterteilen:[57]

1. Technologien, die den Behörden Zugang zu Daten erlauben, in der Regel durch Anfrage bei den Unternehmen. Dies sind zum Beispiel Kundendaten bei Telekommunikationsanbietern.
2. Technologien, bei denen die Unternehmen – und daher auch die Behörden – keinen Zugriff haben. Hierunter fallen iPhones mit dem aktuellsten Betriebssystem.
3. Technologien, die Daten gar nicht erst speichern, oder nach kurzer Zeit löschen. Der kanadische Dienst KiK oder Snapchat fallen in diese Kategorie.

Die Diskussion darüber, ob wir uns im «goldenen Zeitalter der Überwachung» befinden, oder ob Behörden mehr und mehr «im Dunkeln» tappen, ist im Endeffekt eine Diskussion darum, ob mehr Technologien in die erste oder die letzten beiden Kategorien fallen. Denn der Trend zur zunehmenden Verschlüsselung ist eindeutig und es leugnet niemand, dass Ermittler hierdurch vor Herausforderungen gestellt werden. Gleichzeitig ist es möglich, dass den Ermittlern durch neue Methoden und Daten in der Summe mehr Anhaltspunkte zur Verfügung stehen als in der Vergangenheit. Bis jetzt ist es staatlichen Behörden jedenfalls nicht gelungen, ihre Position mit relevanten Zahlen zu unterlegen und so abschließend das Argument aufzubauen, dass neue Lösungen notwendig sind.

Wie sollen die Forderungen umgesetzt werden?

Neben der Frage, ob es denn notwendig sei, den Behörden Zugriff zu verschlüsselten Daten zu geben, stellt sich die Frage, *wie* ein solcher Zugriff gestaltet werden könnte. Denn die Bewertung eines Ansatzes erfordert Wissen um die geplante Operationalisierung. In diesem Kontext wird kritisiert, dass Regierungen zwar oft wüssten, was sie gerne als Resultat

hätten – Zugang zu verschlüsselten Daten –, aber nicht ausführen, wie dies umzusetzen sei.[58]

Allerdings lässt sich im Gegensatz zu dem ersten Kryptokrieg in den 1990er Jahren ein klarer Trend zu konkreteren und umsetzbareren Forderungen erkennen. Der damals von der Clinton-Regierung vorgeschlagene «Clipper Chip», der in Geräte eingebaut werden sollte, hatte offensichtliche Umsetzungsprobleme: Wie soll ein System aussehen, dass die Regierung in hunderte von verschiedenen Soft- und Hardware-Lösungen einbauen lässt? Wie geht man mit Produkten aus dem Ausland um? Ist die Regierung überhaupt in der Lage, die entsprechenden technischen Lösungen zu entwickeln und auf dem aktuellen Stand zu halten?[59]

Viele dieser Fragen lassen sich durch die aktuellen Forderungen nach «Vordertüren» einfacher beantworten, denn die Verantwortung zur Umsetzung wird an die einzelnen Unternehmen weitergegeben. Staaten entwickeln die Lösungen nicht mehr selbst, sondern erzwingen die Möglichkeit des Zugriffs von den Unternehmen, die in ihrem Staatsgebiet Geschäfte betreiben wollen. So könnte zum Beispiel die deutsche Bundesregierung theoretisch von allen Smartphone-Herstellern verlangen, dass diese ihre Geräte auf einen Gerichtsbescheid hin auslesen müssen – und ansonsten auf deutschem Boden keine Geräte verkaufen dürfen. Es wäre dann die Entscheidung von Apple, Samsung und anderen Anbietern, ob sie den Markt weiter nutzen möchten, und wenn ja, wie sie die Forderung praktisch umsetzen. Ähnlich könnten Anforderungen für Apps gestellt werden, die in der deutschen Version von Apples App Store und Googles Play Store zum Herunterladen angeboten werden.

Unabhängig von der Frage, ob einzelne Länder so weit gehen würden, gäbe es selbst in einer solchen Situation zwei Herausforderungen: Erstens verschwimmen die Grenzen online sehr stark, sodass das Herunterladen von verschlüsselten Technologien aus dem Ausland für Nutzer, die den Aufwand eingehen wollen, eine Option wäre. Auch Smartphones könnten im Ausland gekauft und im Inland genutzt werden. Zweitens stehen über frei im Internet verfügbare Programme gerade im Bereich der sicheren Kommunikation eine große Zahl an Verschlüsselungsmöglichkeiten bereit, die sich staatlich fast nicht regulieren lassen. Laut dem Sicherheitsforscher Bruce Schneier sind fast 50 Prozent aller Verschlüsselungstechnologien kostenlos online verfügbar.[60] So lassen sich z.B. fast alle vom «Islamischen Staat» an die eigenen Kämpfer empfohlenen Anwendungen hier zuordnen. Der Effekt durch Regulierung wäre in Bezug auf diese Gruppe an Tätern also minimal.[61]

Befürworter von Regulierung erkennen an, dass einige Kriminelle immer Verschlüsselungstechnologien nutzen werden; dagegen sei auch nichts zu machen. Allerdings könnte durch staatliche Regulierung die Zahl derer, die dies tun, dramatisch reduziert werden. Nur wenige Nutzer betreiben den Aufwand, sich gezielt sichere Anwendungen herunterzuladen und diese auch konsequent zu nutzen. Durch eine Veränderung der kommerziell angebotenen Hard- und Software würden sich die Ermittlungen in einem Großteil der Fälle vereinfachen, wodurch wiederum mehr Ressourcen frei wären, um sich auf komplexere Fälle zu konzentrieren.[62]

Welche weiteren Auswirkungen haben die Forderungen?

Selbst wenn Fragen nach der Notwendigkeit und der möglichen Umsetzung der Regulierung von Verschlüsselungstechnologien geklärt sein sollten, wäre immer noch zu beantworten, welche Konsequenzen ein solcher Eingriff hätte. Egal wie die Forderungen nach Zugang umgesetzt würden, sie erforderten einen Eingriff in technische Systeme und Anpassungen des rechtlichen Rahmens. Hieraus ergeben sich drei Argumente, die gegen die Regulierung von Verschlüsselung sprechen: Die Schwächung der Informationssicherheit, wirtschaftliche Folgen der Regulierung und die Konsequenzen auf die Regulierung und Nutzer in anderen Staaten.

Sicherheit gegen Sicherheit

In der Diskussion um Überwachung wird oft auf einen angeblichen Zielkonflikt zwischen Freiheit und öffentlicher Sicherheit hingewiesen. Technologien garantieren die Freiheit der Bürger, aber eben auch die möglicher Krimineller – es müsse daher Einschränkungen geben, um die öffentliche Sicherheit zu stärken. Wenn man genauer hinschaut, handelt es sich bei der vorliegenden Abwägungsentscheidung um einen Zielkonflikt zwischen Informationssicherheit und öffentlicher Sicherheit im Sinne der Ermittlungsmöglichkeiten von Behörden.[63] Denn die diskutierten Technologien leisten einen kritischen Beitrag zur Informationssicherheit und somit in Zeiten, in denen unsere Gesellschaft von digitaler Kommunikation abhängig ist, im weiteren Sinne auch zur nationalen Sicherheit.

Die negativen Konsequenzen eines solchen Eingriffs lassen sich konkretisieren. Informations- und Kommunikationstechnologien sind komplexe Systeme, und schon jetzt gibt es keine (bekannten) perfekten Verschlüsselungssysteme.[64] Soft- und Hardware-Schwachstellen existieren und können ausgenutzt werden, um gegen den Willen der Nutzer an ihre Daten zu gelangen.[65] Sollten Unternehmen nun gezwungen sein, ihre Geräte oder Anwendungen so zu entwickeln, dass sie darauf auch ohne Einwilligung des Nutzers Zugriff haben, müssen sie gezielt Schwachstellen einbauen und erhöhen gleichzeitig die Komplexität der Systeme, was ihre Fehleranfälligkeit steigert.[66] Die Wahrscheinlichkeit, dass auch Kriminelle Zugang zu Geräten erhalten, steigt.[67] Bei über drei Millionen gestohlenen Smartphones im Jahr 2013 allein in den USA können diese Eingriffe schnell ganz reale Konsequenzen für Nutzer haben. Diese Konsequenzen werden vor allem jene (legitimen und illegitimen) Nutzer betreffen, die sich wenig mit der Problematik auseinandersetzen und deren IT-Kenntnisse minimal sind. Fortgeschrittene Nutzer – seien es Geheimdienste, einzelne Individuen oder professionelle kriminelle Netzwerke – werden weiterhin starke Verschlüsselungsmethoden nutzen.[68]

Dieser Blick auf Aspekte der Informationssicherheit und der Konsequenzen eines Eingriffs hilft auch, das unterschiedliche Verhalten verschiedener staatlicher Behörden zu erklären. So unterscheiden sich die Interessen der Geheimdienste (wie der NSA und dem Bundesnachrichtendienst, BND) von denen anderer Sicherheits- und Strafverfolgungsbehörden (wie zum Beispiel dem FBI oder dem Bundeskriminalamt, BKA).[69] Die Behörden bearbeiten unterschiedliche Verbrechen und unterliegen nicht den gleichen Transparenzanforderungen. Darüber hinaus unterscheiden sie sich in Bezug auf technische, finanzielle

und personelle Kapazitäten. In den USA lässt sich dies besonders gut daran erkennen, dass die Geheimdienste, allen voran die NSA, sich in den letzten Jahren nicht hinter das FBI mit seinen Forderungen nach Zugriff auf Verschlüsselung gestellt haben. Ganz im Gegenteil bezeichnete NSA-Chef Mike Rogers Verschlüsselung als «die Grundlage unserer Zukunft» und jede Diskussion um die Nachteile als Zeitverschwendung.[70] Dies lässt sich damit erklären, dass die NSA in den USA auch den Auftrag hat, Informationssysteme, kritische Infrastrukturen und Staatsgeheimnisse zu schützen, und hierbei auf die weite Verbreitung starker Verschlüsselungsmethoden angewiesen ist. Gleichzeitig stehen ihr Mittel und Wege zur Verfügung, um die gewünschten Informationen von Gegnern anderweitig zu erlangen. Nationale und lokale Strafverfolgungsbehörden arbeiten unter anderen Bedingungen. Sie haben weniger finanzielle und technische Mittel zur Verfügung und sie sind häufiger auf «traditionelle» Ermittlungsmethoden angewiesen. Gleichzeitig profitieren sie weniger direkt von sicheren Informationssystemen, denn diese fallen oft nicht in ihren Arbeitsbereich.[71]

Ökonomische Aspekte

Neben der Schwächung von IT-System kann die Regulierung von Verschlüsselungstechnologien auch negative wirtschaftliche Folgen für einzelne Staaten haben. Erstens wären Nutzer und Firmen weniger gut gesichert, was Cyberkriminellen in die Hände spielen würde. In diesem Zusammenhang hält zum Beispiel das BKA fest, dass «mit der weiter zunehmenden Bedeutung der IT im privaten sowie professionellen Bereich [...] sich die Manipulations- und Angriffsmöglichkeiten [...] erhöhen.»[72] Durch die Unterminierung von Verschlüsselungstechnologien würden diese Manipulations- und Angriffsmöglichkeiten weiter zunehmen.

Zweitens würden Regulierungsansätze wahrscheinlich das Vertrauen der Nutzer und Unternehmen in die in dem Land entwickelten Technologien sinken lassen. Vertrauen ist nicht nur notwendig, um Digitalisierungsprozesse voranzutreiben. Vielmehr ist es auch ein Verkaufsargument. Amerikanische Technologiefirmen haben nach 2013 zum Beispiel einen klaren «Snowden-Effekt» verzeichnet, der vor allem durch gesunkenes Vertrauen auf globalen Märkten gekennzeichnet war.[73] Sollten nun die USA oder Deutschland – die zusammen fast 50 Prozent aller Verschlüsselungstechnologien zur Verfügung stellen[74] – entsprechende Gesetze voranbringen, ist es wahrscheinlich, dass Firmen in anderen Nationen besonders sichere Technologien anbieten werden, um die entsprechenden Marktanteile abzugreifen. Siegel wie «IT Security Made in Germany», mit denen Deutschland für die Verlässlichkeit eigener Technologien wirbt, würden national und international ganz klar an Glaubhaftigkeit verlieren.

Die internationale Komponente

Letztlich sollte die Diskussion um Verschlüsselungstechnologien nicht nur in der rein nationalen Dimension gedacht werden. Die hier beschriebenen Technologien leisten in vielen Ländern, in denen es um Grundrechte wie die Meinungs- und Pressefreiheit weniger gut bestellt ist, einen besonders wichtigen Beitrag. Bürgerrechtler und Journalisten in autoritären Staaten sind auf die Vorteile von Verschlüsselungstechnologien angewiesen,

um sicher kommunizieren zu können. Während viele westliche Staaten diese Aktivitäten unterstützen, sind sie in den betroffenen Ländern oft illegal. Sollten nun westliche Staaten von Unternehmen den Zugang zu verschlüsselten Daten einfordern, um gegen kriminelle Machenschaften vorzugehen, werden andere Staaten schnell nachziehen – die Definition von «illegal» wird sich aber nicht zwingend mit der unseren decken, und rechtstaatliches Vorgehen kann hier nicht garantiert werden. Auch aus diesem Grund fordert zum Beispiel die UNESCO, Verschlüsselungstechnologien nicht zu schwächen,[75] und der UN-Sonderberichterstatter für Meinungsfreiheit, David Kaye, warnt Staaten davor, Regulierungen vorschnell voranzutreiben.[76]

Man sollte aber auch nicht vergessen, dass Staaten wie China und Russland nicht darauf warten werden, wie der Westen in dieser Diskussion entscheidet, und dass unser Handeln nicht durch solche Staaten diktiert werden sollte. Nichtsdestotrotz haben westliche Regierungen hier eine Verpflichtung, mit gutem Vorbild voranzugehen, gerade mit Bezug auf Staaten, die weniger extreme Positionen wie China oder Russland einnehmen. Sollten zudem westliche Unternehmen auf Druck der eigenen Regierungen ihre Produkte schwächen, würde dies automatisch Menschen in anderen Regionen betreffen, die diese Produkte nutzen.

Bewertung

Im Vergleich zu den Diskussionen in den 1990er Jahren ist die Debatte um die mögliche Umsetzung von Regulierungsansätzen vorangeschritten. Hier haben es sich staatliche Behörden leichtgemacht und die Entwicklung des Zugangs an die Unternehmen ausgelagert. Diese kennen ihre Produkte am besten und können am ehesten einschätzen, wo Zugangsmöglichkeiten vorhanden sind. Im Gegensatz zu dem Einbau eines Clipper Chips ist es schwieriger, diese Umsetzung direkt von der Hand zu weisen.

Allerdings ist es Befürwortern staatlicher Eingriffe bis heute nicht gelungen, die Notwendigkeit für einen Eingriff in die Informationssicherheit von Millionen Nutzern zu belegen. Ja, Verschlüsselungsmethoden verbreiten sich immer rascher und werden immer nutzerfreundlicher. Durch die Digitalisierung ergeben sich aber auch ganz neue Ermittlungsmöglichkeiten, die diesem Trend entgegenwirken. Behörden mögen im Dunkeln tappen – vielleicht nehmen sie dies aber auch nur so wahr. Selbst wenn dem so sei, ist es unwahrscheinlich, dass die Regulierung von Verschlüsselungstechnologien die Herausforderung grundsätzlich lösen würde. Daher sind die Behörden, die neue Möglichkeiten fordern, eindeutig in der Bringschuld. Denn jeder bisher vorgebrachte Ansatz zur Regulierung von Verschlüsselungstechnologien hätte negative Auswirkungen auf die Art, wie Millionen oder gar Milliarden von Nutzern kommunizieren. Vor dem Hintergrund der oben angeführten Argumente lässt sich eine Einschränkung zu diesem Zeitpunkt daher nicht begründen.

Für Sicherheits- und Strafverfolgungsbehörden wird es jedoch keine Option sein, es so auf sich beruhen zu lassen. Denn sie legen, in der Regel im gesellschaftlichen Interesse, alles daran, Gefahren abzuwehren und Verbrechen zu bestrafen. Gerade in einem aufgeheizten

Klima, zum Beispiel nach Terrorangriffen, in welchem Verschlüsselungstechnologien wieder als wichtiges Mittel von Kriminellen verteufelt werden, wird es Forderungen nach Regulierung immer wieder geben. Es gilt, dieser Politisierung frühzeitig entgegenzutreten. Daher ist es notwendig, sich mit alternativen Ermittlungsmethoden auseinanderzusetzen. Denn wie schon zu Beginn ausgeführt wurde, sind Verschlüsselungstechnologien nur ein Grund, weshalb Behörden «im Dunkeln» tappen. Vor diesem Hintergrund geht der nächste Teil auf Möglichkeiten ein, die Staaten haben, um an Daten zu gelangen, ohne Verschlüsselung regulieren zu müssen.

Teil II
Zum Umgang mit einer verschlüsselten Welt

Eine Folge der Verbreitung von Verschlüsselungstechnologien ist der erschwerte Zugang zu Daten verschiedenster Art. Allerdings sind neue und nutzerfreundlichere Methoden der Verschlüsselung nur eine der Herausforderungen, die diesen Zugang erschweren. Sicherheits- und Strafverfolgungsbehörden müssen zur Zeit einer Reihe anderer technischer Entwicklungen ebenso begegnen. Dazu gehören zum Beispiel auch die zunehmende Verbreitung von Anonymisierungstechnologien, Software zum Löschen von Daten, virtuelle Netzwerke und Cloud-Lösungen zur Sicherung von Daten in anderen Jurisdiktionen.[77] Verschlüsselungstechnologien sind in der öffentlichen Wahrnehmung lediglich die prominenteste Herausforderung.

Wie im ersten Teil gezeigt wurde, gibt es keine einfachen Antworten auf diese Entwicklungen. In der Summe überzeugen die bisher genannten regulatorischen Ansätze nicht. In diesem Abschnitt sollen daher andere Herangehensweisen evaluiert und mögliche Handlungsoptionen erarbeitet werden. Denn Vorder- oder Hintertüren sind nicht die einzigen Ansätze, um Behörden Zugang zu Daten zu verschaffen. Ebenso wie Kriminelle nicht nur Verschlüsselungstechnologien nutzen, um ihre Daten zu sichern, haben Sicherheits- und Strafverfolgungsbehörden[78] verschiedene Möglichkeiten, um in einer sich digitalisierenden Welt Gefahren abzuwehren und Verbrechen aufzuklären. Im Folgenden werden vier konkrete Ansätze skizziert und diskutiert:

- Staatliches Hacking,
- die Sammlung von Metadaten (durch Vorratsdatenspeicherung und Datenlokalisierung),
- Reformansätze für das internationale Rechtshilfesystem, und
- der Ausbau des Personals und des technischen Wissens in den Behörden.

Staatliches Hacking

Eine der prominentesten Alternativen zum Zugang von Daten durch Behörden ist ein staatliches Hacking-Regime. Die Idee dahinter ist simpel: Behörden warten nicht ab, bis Daten durch Nutzer verschlüsselt werden, sondern greifen durch Zugang zu den Endgeräten, also zum Beispiel den Smartphones oder Laptops, auf den Klartext zu, der ja für den Nutzer selbst lesbar ist. Die Umsetzung ist allerdings komplizierter und weiterhin umstritten. Der Zugriff geschieht über Schadsoftware, die auf das Gerät aufgespielt werden muss, zum Beispiel über Phishing E-Mails, korrumpierte Software-Updates, das Ausnutzen von Schwachstellen in der Software des Geräts oder physischen Zugang durch die Behörden. Sobald sie Zugriff haben, können Ermittler, je nach Angriff, auf einzelne Anwendungen oder die gesamten Aktivitäten eines Verdächtigen zugreifen, also zum Beispiel Kommunikation mitlesen, Passwörter einsehen und Kopien von Daten auf dem Gerät anfertigen.[79]

In Deutschland wird bezüglich der Art des Zugriffs zwischen der Quellen-Telekommunikationsüberwachung (dem Zugriff auf einzelne Kommunikationswege oder -anwendungen) und der Online-Durchsuchung (die Durchsuchung von ganzen Endgeräten) unterschieden.[80]

Die Idee des kontrollierten staatlichen Hacking hat aus verschiedenen Gründen eine vergleichsweise breite Reihe an Unterstützern selbst in Zivilgesellschaft und Wissenschaft.[81][82] Ein erstes Argument für ein solches Regime ist, dass keine neuen Schwachstellen geschaffen, sondern existierende ausgenutzt würden. Weiter lässt sich anführen, dass der Ansatz nicht die Geräte einer breiten Masse an Nutzern kompromittiert, wie es eine Regulierung von Verschlüsselungstechnologien tun würde, sondern auf einzelne Individuen ausgerichtet ist. Zudem ist die Anwendung dieser Technik für die Behörden noch vergleichsweise aufwendig, da der Kauf beziehungsweise die Entwicklung solcher Schadsoftware komplex und kostspielig ist und der Einsatz gut koordiniert sein muss. Staatliches Hacken kann also eine Möglichkeit sein, den Behörden in einer begrenzten Anzahl an Fällen, in denen es Ermittler und Richter für angemessen halten, auf unverschlüsselte Daten Zugriff zu gewährleisten.

Allerdings gibt es auch hier eine Reihe an Kritikpunkten und offenen Fragen. Zunächst einmal sind Staatstrojaner ein «außerordentlich eingriffsintensives Instrument,»[83] denn in Smartphones und auf Laptops finden sich eine Vielzahl an Informationen über den jeweiligen Nutzer. Auch aus diesem Grund hat das Bundesverfassungsgerichts mit Blick auf die online-Durchsuchung geurteilt, dass für deren Einsatz «Anhaltspunkte einer konkreten Gefahr für ein überragend wichtiges Rechtsgut»[84] vorliegen müssen. Die jüngst in Deutschland verabschiedete Änderung der Strafprozessordnung mit Bezug zu dem Einsatz von Staatstrojanern verdeutlicht, dass Ermittler schon jetzt versuchen, diesen Rahmen zu sprengen: Laut der Änderung ist es den Behörden nun möglich, diesen Eingriff bei über dreißig Straftaten durchzuführen, unter anderem auch bei Fällen von Geldwäsche oder Bestechung.[85]

In diesem Zusammenhang stellen sich Fragen nach der Transparenz und den Möglichkeiten des Missbrauchs. Während bei einer traditionellen richterlichen Anordnung in der Regel ein Unternehmen zwischen den Ermittlern und den Daten eines Individuums steht, ist die externe Kontrolle im Fall von staatlichem Hacking schwieriger, da direkt auf ein Gerät zugegriffen wird. Auch der betroffene Nutzer wird von der Durchsuchung nichts mitbekommen, hat also keine Möglichkeit, das Vorgehen vor Gericht prüfen zu lassen. Selbstverständlich besteht ein Richtervorbehalt, aber es bleibt unklar, inwiefern das technische Verständnis der Richter ausreicht, um alle Schritte nachvollziehen zu können. Hinzu kommt, dass es schwierig ist, Schadsoftware so zu entwickeln, dass sie ganz genau den rechtlichen Vorgaben entspricht und nicht mehr ausliest, als vorgesehen.

Drittens birgt Hacking von staatlicher Seite große Gefahren für die IT-Sicherheit.[86] Denn um auf Endgeräte zugreifen zu können, werden in der Regel vorhandene Schwachstellen in der Software ausgenutzt, ähnlich wie es auch durch Cyberkriminelle geschieht. Dies schafft Anreize für staatliche Behörden, diese Schwachstellen nicht zu schließen, sondern im Zweifel für sich zu behalten, da sie sonst durch Unternehmen geschlossen würden. Als

Konsequenz bleiben diese Lücken aber auch für andere Angreifer offen.[87] So wurden im Mai 2017 im Rahmen des WannaCry-Angriffs auf Millionen Computer weltweit Schwachstellen verwendet, die ursprünglich durch die NSA genutzt und geheim gehalten wurden.[88] Gefordert wird in dem Zusammenhang daher auch ein «Vulnerabilities Equities Process» (VEP) oder Schwachstellenmanagementsystem, durch welches von den Behörden gefundene Schwachstellen an die Soft- und Hardwarehersteller weitergeleitet werden. Die USA haben hier eine Vorreiterrolle eingenommen und 2014 einen groben Einblick in ihren Prozess gegeben;[89] dieser wurde im Jahr 2017 weiter formalisiert.[90] Allerdings bleibt auch hier die Kritik bestehen, dass Schwachstellen im Zweifel eher für Ermittlungs- und Geheimdiensttätigkeiten genutzt und daher bewusst offengelassen werden.

Die mögliche Effektivität staatlichen Hackings, ebenso aber die Notwendigkeit, dies in einem klaren gesetzlichen Rahmen mit entsprechender Kontrolle durchzuführen, verdeutlicht die «Operation Pacifier» des amerikanischen FBI.[91] Im Rahmen der Operation wurde eine Kinderpornographie-Website durch das FBI übernommen, kurzfristig weiterbetrieben und Schadsoftware auf der Website hinterlegt; gleichzeitig wurde eine Schwachstelle in dem Browsermodell «Tor» ausgenutzt. Hierdurch wurden die Computer von über 8.000 mutmaßlicher Pädophiler in über 120 Ländern infiziert, was dem FBI die Möglichkeit gab, sie zu identifizieren und in einigen Fällen Anklagen zu erheben. All dies geschah auf Grundlage eines einzelnen Gerichtsbescheids und ohne, dass das FBI wusste, wen die Schadsoftware betreffen würde. Zudem wurde eine Schwachstelle in dem genutzten Browser geheim gehalten, was möglicherweise auch legitime Nutzer verwundbar ließ. Gleichzeitig wäre es ohne diesen «Hack» so gut wie unmöglich gewesen, die mutmaßlichen pädophilen Nutzer zu fassen.

Entschlüsselungskapazitäten & Forschungsunterstützung

Im Zusammenhang mit staatlichem Hacking sollten auch Versuche genannt werde, Verschlüsselung durch vorhandene Schwachstellen in der Technologie oder durch «brute force» – also durch hohe Rechenkapazitäten – zu brechen. Sollten Behörden also zum Beispiel ein verschlüsseltes Gerät vorliegen, können sie versuchen, dieses so zu dekryptieren. Für Verbindungsdaten ist dieser Ansatz möglich, falls Schwachstellen in den entsprechenden Anwendungen gefunden werden. Auf diese Art ist es zum Beispiel dem FBI letztendlich gelungen, Zugriff auf das iPhone des Angreifers in San Bernadino zu erlangen. Dieser Ansatz ist allerdings aufwendig und vergleichsweise teuer.[92]

In Deutschland soll die neu geschaffene «Zentrale Stelle für Informationstechnik im Sicherheitsbereich» (ZITiS) in diesem Gebiet aushelfen und andere Behörden als Forschungs- und Entwicklungsstelle beraten. ZITiS selbst wird nicht operativ tätig werden. Neben der Dekryptierung fallen auch Aufgaben aus dem Bereich der digitalen Forensik, der Telekommunikationsüberwachung und der Massendatenauswertung/Big-Data in das Tätigkeitsfeld von ZITiS.[93] Die Behörde könnte also zum Beispiel auch bei der Entwicklung neuer Trojaner unterstützend tätig werden oder versuchen, Schwachstellen in Systemen zu finden.

Der Zugriff auf Metadaten: Vorratsdatenspeicherung und Datenlokalisierung

In der Diskussion um Verschlüsselungstechnologien geht es häufig um Inhaltsdaten. Allerdings sind auch Metadaten ein wichtiger Teil moderner Ermittlungen. Metadaten sind Informationen über Daten, also zum Beispiel Informationen darüber, wer mit wem, wann, wo und wie lange geredet hat. Auch ohne Inhalte verraten diese Daten viel über das Verhalten von Individuen und die Kommunikation in Netzwerken. Metadaten können von Strafverfolgungsbehörden zum Beispiel über die Abfrage bei Mobilfunkkonzernen und Internetanbietern gewonnen werden.

Verschiedene Staaten verpflichten Unternehmen durch gesetzliche Regeln zur Vorratsdatenspeicherung dazu, gewisse Metadaten für einen längeren Zeitraum als für den Geschäftszweck nötig aufzubewahren. Die Idee dahinter ist, dass oft erst nach einer Straftat klar ist, gegen wen ermittelt wird, und daher rückwirkend Zugriff auf diese Daten vorhanden sein muss. Laut dem zur Zeit ausgesetzten[94] deutschen Vorstoß zur Vorratsdatenspeicherung müssen Telefonanbieter die Nummern, Daten und Zeiten von Telefonaten und SMS für mindestens zehn Wochen speichern; Mobilfunkanbieter speichern zudem die Ortungsdaten (für vier Wochen). Internetanbieter sind verpflichtet, die IP-Adressen von Nutzern zu hinterlegen.[95]

Die Vorratsdatenspeicherung kann den Behörden zwar helfen, sie ist aber aus verschiedenen Gründen problematisch. Hervorzuheben ist, dass alle Bürgerinnen und Bürger «anlasslos unter Generalverdacht» gestellt werden,[96] denn ihre Daten werden unabhängig von ihrem Verhalten gespeichert. Dies ist umso fragwürdiger, als dass die Effektivität der Vorratsdatenspeicherung bis heute nicht abschließend nachgewiesen werden konnte. Intuitiv macht es Sinn, dass mehr Daten zu besserer Ermittlung führen, allerdings bleibt die Frage unbeantwortet, wie hoch der tatsächliche Nutzen ist. Weitere Kritikpunkte sind, dass für die Kommunikationsunternehmen durch das zusätzliche Speichern Kosten entstehen, und die gesammelten Daten natürlich auch für Kriminelle ein attraktives Ziel sind.[97]

Vor diesem Hintergrund urteilte Ende 2016 der Europäische Gerichtshof, dass EU-Staaten Vorratsdaten nicht mehr «anlasslos» speichern dürften. Eine solche Sammlung müsse an spezifische Voraussetzungen gebunden sein, «gezielt» stattfinden und sich hinsichtlich erfasster Personen, Speicherfristen und Kommunikationsmittel auf das «absolut Notwendige» beschränken.[98] Die Bundesregierung ist der Meinung, dass das deutsche Gesetz diesen Forderungen entspricht, hat die Umsetzung allerdings im Juni 2017 selbst ausgesetzt.[99] Eine endgültige Entscheidung wird das Bundesverfassungsgericht treffen müssen.

Einige Länder gehen mit Forderungen nach Datenlokalisierung noch einen Schritt weiter. Durch eine Lokalisierung werden das Speichern und Verarbeiten von Daten an nationale Grenzen gebunden.[100] Unternehmen werden zum Beispiel gezwungen, Inhalts- und Metadaten nur im eigenen Land zu verarbeiten, oder zumindest eine Kopie dort zu speichern. Nach den Snowden-Enthüllungen wurde die Angst vor amerikanischer Überwachung oft als Grund für solche Maßnahmen angegeben. Diese Angst mag einer der Beweggründe sein,

in vielen Fällen ist das Ziel aber lediglich, den eigenen Behörden verbesserten Zugang zu den entsprechenden Daten zu geben. Gesetze zur Datenlokalisierung haben in den letzten Jahren zugenommen und eine Reihe an Ländern wie China, Russland, Iran, aber auch Australien und Südkorea, forcieren in unterschiedlichem Ausmaß die Lokalisierung von Daten im eigenen Land.[101] In Deutschland müssten zum Beispiel die im Rahmen der Vorratsdatenspeicherung gewonnenen Daten auf deutschen Servern gespeichert werden. In diesem Fall scheint der Wunsch, die Daten der eigenen Bürger zu schützen, in der Tat im Vordergrund zu stehen. In Fällen wie Russland, wo Unternehmen Kopien aller Nutzerdaten lokal speichern müssen, stehen aber eindeutig die Bemühungen im Vordergrund, die eigenen Ermittlungsmöglichkeiten zu verbessern. Ähnlich wie bei Vorder- oder Hintertüren gehen diese Bemühungen allerdings auf Kosten der breiten Basis an Nutzern: Nicht nur entstehen Risiken des Machtmissbrauchs durch Behörden, das Errichten von nationalen Grenzen und die damit verbundene Fragmentierung gefährdet die grundlegende Idee eines offenen und globalen Internets. Insofern ist der Zugang zu (Meta-)Daten über die Vorratsdatenspeicherung oder Datenlokalisierung kritisch zu sehen.

Reform der internationalen Rechtshilfe

Die Reform des Systems der internationalen Rechtshilfe ist eine weitere Möglichkeit, um den Zugriff von Sicherheits- und Strafverfolgungsbehörden auf Daten von Verdächtigen zu verbessern. Die grundsätzliche Idee hinter Rechtshilfeunterstützungsverträgen (Mutual Legal Assistance Treaties, MLATs) ist es, staatlichen Behörden in Land A Zugang zu Daten bei Unternehmen in Land B zu ermöglichen.

Solche Verträge werden bi- oder multilateral zwischen Staaten abgeschlossen. Sie sind gängiges Instrument bei grenzüberschreitenden Ermittlungen und wurden schon vor der Digitalisierung zur internationalen Beschaffung von Beweismitteln eingesetzt. In Bezug auf digitale Nachweise haben sie an Relevanz gewonnen, gerade für nicht-amerikanische Behörden, denn die meisten Nutzerdaten liegen im Moment bei amerikanischen Technologieunternehmen. Das Kernproblem ist, dass das System der internationalen Rechtshilfe entwickelt wurde, als es Unternehmen wie Google oder Facebook nicht gab und auch die jetzt existierende Asymmetrie – mit einem Großteil der Unternehmenssitze in den USA – nicht vorhanden war. Zur Zeit ist das System für die Vermittlung von Inhaltsdaten extrem komplex:[102] Wenn deutsche Behörden Zugang zu der Kommunikation eines Google-Nutzers wünschen, müssen sie über das Bundesamt für Justiz an das US-amerikanische Justizministerium herantreten, das dann das Büro des Staatsanwalts in Kalifornien kontaktiert, der sich wiederum an Google wendet, falls der Anfrage stattgegeben wurde. Im Schnitt dauert dieser Prozess im Moment zehn Monate pro Anfrage, in vielen Fällen mehrere Jahre.[103] Ziel des aufwendigen Prozesses ist, sicherzuzustellen, dass fremde Staaten nicht mit unrechtmäßigen Anfragen an amerikanische Firmen herantreten können. Dieser Anspruch stellt die amerikanischen Behörden aber vor zunehmende Herausforderungen, denn die Anzahl der Anfragen für Datenträger hat sich im letzten Jahrzehnt verzehnfacht.[104]

Aus europäischer Sicht gibt es verschiedene Möglichkeiten, sich dieser Herausforderung anzunehmen. Zum einen könnte man innerhalb des Systems der Rechtshilfe Prozesse optimieren und Anreize schaffen, um Wartezeiten zu verkürzen. Hier könnten Überlegungen angestrengt werden, ob und wie man für die Kosten des Prozesses auf amerikanischer Seite zumindest teilweise aufkommen könnte. So wäre es dort möglich, Personal entsprechend aufzustocken. Ohne eine solche Kompensation sind die Anreize für die USA schlicht gering.

Zweitens sollte überlegt werden, wie der Prozess digitalisiert und europäische Behörden besser geschult werden können. Formulare, Einsendung der Anfragen, Methoden der gegenseitigen Authentifizierung sowie Statusabfrage könnten online abgewickelt werden.[105] Gleichzeitig müssen die Antragssteller die Rechtshilfeersuchen auch so stellen, dass sie von amerikanischer Seite positiv beantwortet werden können und mit den dortigen rechtlichen Standards übereinstimmen.

Drittens sollte über direkte Zugangsmöglichkeiten europäischer Behörden zu den amerikanischen Staatsanwaltschaften (und andersherum), beziehungsweise direkt zu den amerikanischen Unternehmen, verhandelt werden, ähnlich wie es jetzt schon mit Metadaten funktioniert.[106] Ein solcher bilateraler Vertrag wird im Moment zwischen den USA und Großbritannien diskutiert.[107] Die Vorteile liegen auf der Hand: In den USA werden Ressourcen gespart und für Großbritannien verkürzt sich die Wartezeit auf Informationen drastisch. Dieses Modell lässt sich nicht beliebig übertragen, da auf beiden Seiten des Atlantik weiterhin sichergestellt werden muss, dass die Anfragen den jeweiligen gesetzlichen Anforderungen entsprechen. Es wäre aber möglich, ein solches Modell mit einer Reihe von Staaten, die ihren rechtstaatlichen Prozessen gegenseitig vertrauen, aufzubauen. In diesem Zusammenhang ist vor allem auch die EU gefordert, mit gutem Beispiel voranzugehen; ein EU-weites Instrument und damit eine Harmonisierung der Vorgehensweisen würde für schnellere Prozesse und mehr Transparenz sorgen.[108]

Personal, Ausbildung und Technik

Abschließend ist es wichtig zu betonen, dass die Arbeit der Polizei und anderer Behörden sich im Laufe der letzten Jahrzehnte stetig verändert hat. Ermittler haben in der Vergangenheit immer Möglichkeiten gefunden, sich diesen Anpassungen zu stellen und sich technologischen Herausforderungen anzunehmen. Um dies auch im Rahmen der zunehmenden Digitalisierung zu tun, ist in den Behörden ein entsprechendes Verständnis der technologischen Entwicklungen notwendig. Dieses Wissen gilt es unter anderem durch mehr IT-Spezialisten aufzubauen, entweder durch das Einstellen externer Experten oder durch Ausbildung in den Organisationen. Zudem ist es notwendig, das allgemeine Wissen um den Umgang mit digitalen Beweismitteln sowie neue Methoden und Taktiken in den Behörden, aber auch bei Staatsanwaltschaften und in den Gerichten, gezielt zu fördern. Für alle Beteiligten wird es wichtig sein, neue Ermittlungsansätze – zum Beispiel über das Internet der Dinge – frühzeitig erkennen zu können.

Diese Herausforderung wurde in Deutschland und anderen europäischen Staaten schon erkannt. Allerdings tut man sich aus verschiedenen Gründen bisher schwer damit, das entsprechend gut ausgebildete Personal zu gewinnen.[109] Erstens ist der Staat für IT-Fachkräfte nicht immer ein attraktiver Arbeitgeber, sei es aus Image-Gründen oder aus finanzieller Sicht. In der Privatwirtschaft lockt oft ein Mehrfaches dessen, was der der öffentliche Dienst zahlen kann. Hier ist es notwendig, über alternative Bezahlmodelle nachzudenken. Zweitens stehen Behörden oft im Wettbewerb zueinander. In Deutschland suchen zum Beispiel BND, Bundeswehr, BKA, ZITiS und BSI alle nach IT-Spezialisten. Hier ist es notwendig, sich zentral zu überlegen, wo Prioritäten gesetzt werden sollten, um zu verhindern, dass sich die Behörden untereinander ausbooten.

Die Perspektive für Deutschland

Diese Studie hat sich mit den zunehmenden Problemen staatlicher Behörden hinsichtlich des Zugriffs auf Daten aufgrund von Verschlüsselungstechnologien auseinandergesetzt. Darauf aufbauend lassen sich verschiedene Schlussfolgerungen ziehen, die auch für die Debatte in Deutschland von Nutzen sind.

In Bezug auf die mögliche Regulierung von Verschlüsselungstechnologien sind Politiker und Ermittler, die eine solche fordern, in der Bringschuld. Sie müssen Probleme und Lösungsansätze konkretisieren. Es bleibt unklar, inwiefern Behörden von der Verbreitung der Technologie negativ betroffen sind, und ob andere technische Entwicklungen diesem Trend entgegenwirken. Ohne bessere Daten hierzu ist nicht nur eine informierte Diskussion unmöglich, jedweder Eingriff wäre ohne sie unverantwortlich.

Denn die Argumente gegen Regulierung liegen auf der Hand. Verschlüsselung schützt täglich die Daten von Milliarden von Menschen und Organisationen, inklusive einer Vielzahl an staatlichen Stellen. Gerade vor dem Hintergrund der zunehmenden Abhängigkeit von digitalen Technologien gewinnt dieser Aspekt weiter an Relevanz. Eine mögliche Regulierung durch Vorder- oder Hintertüren würde nicht nur die breite Masse an Nutzern gefährden und Cyberkriminellen die Arbeit vereinfachen. Sie riskiert auch die Reputation der eigenen IT-Wirtschaft und vereinfacht es autoritären Regimes, ähnliche Forderungen zu stellen, was wiederum die Meinungs- und Pressefreiheit weltweit unter Druck setzen würde.

In Deutschland gilt daher aus gutem Grund der Grundsatz «Sicherheit durch Verschlüsselung und Sicherheit trotz Verschlüsselung».[110] Konkret heißt das, dass es «keine gesetzlichen Verpflichtungen zu Schlüsselhinterlegungen oder zur Nutzung von Generalschlüsseln oder gar zu sogenannten ‹backdoors› geben [wird]».[111] An der historisch gewachsenen Absage an einen solchen Eingriff sollte entschieden festgehalten werden. Gleichzeitig ist es notwendig, für ein besseres Verständnis dafür zu sorgen, wie «Sicherheit trotz Verschlüsselung» interpretiert wird.

Dies betrifft zwei Punkte: Zum einen gibt es weiterhin Diskussionen in Deutschland, Over-the-top-Anbieter wie WhatsApp in Zukunft nicht mehr wie aktuell durch das Telemediengesetz zu regulieren, sondern unter das Telekommunikationsgesetz (TKG) zu stellen, welches vorsieht, dass Anbieter «auf eigene Kosten technische Einrichtungen zur Umsetzung gesetzlich vorgesehener Maßnahmen zur Überwachung der Telekommunikation vorzuhalten [haben]».[112] Eine solche Umsetzung könnte je nach Auslegung einer Regulierung einer «Vordertür» wie zu Anfang definiert entsprechen. Die Bundesregierung sollte hier klar Stellung beziehen und ihre Interpretation des TKG öffentlich machen, um Zweifel an der Regulierung der Verschlüsselungsmechanismen von OTT-Anbietern auszuräumen.

Der zweite Punkt betrifft die in Teil 2 vorgestellten Möglichkeiten zum Stärken von Behörden, um sich den Herausforderungen durch Verschlüsselung zu stellen. Denn dass Herausforderungen existieren, lässt sich ebenfalls nicht leugnen. Unter den vorgestellten Optionen sind die der Vorratsdatenspeicherung und der Datenlokalisierung am kritischsten

zu betrachten. Der Vorratsdatenspeicherung wurden aus gutem Grund durch den Europäischen Gerichtshof klare Grenzen gesetzt und die Aussetzung der Umsetzung durch die Bundesnetzagentur ist ein wichtiges Zeichen. Anders als noch vor einigen Jahren gibt es zurzeit auch wenig Bestrebungen, Daten vermehrt in Deutschland zu speichern oder zu verarbeiten.

Der Ausbau von Personal und technischen Kapazitäten sowie die Reform der internationalen Rechtshilfe sind die am wenigsten umstrittenen, allerdings oft auch vernachlässigten Optionen, um die Probleme der Behörden anzugehen. Um das entsprechende Personal zu verpflichten, muss über alternative Gehaltsstrukturen nachgedacht werden und vor allem in die Ausbildung innerhalb der Behörden investiert werden. Um das System der internationalen Rechtshilfe zu verbessern, sollte die Thematik in bilateralen Gesprächen mit den USA und innerhalb der EU verstärkt auf die Agenda gesetzt werden. Insbesondere Möglichkeiten eines direkten Antrags europäischer Behörden bei amerikanischen Unternehmen in Bezug auf Inhaltsdaten sollten auf Umsetzbarkeit geprüft werden.

Am meisten Diskussion ist in Bezug auf staatliches Hacking notwendig. Dieses wird bereits praktiziert und wird den Behörden als Ermittlungsmöglichkeit im 21. Jahrhundert erhalten bleiben. Im Vergleich zur gezielten Schwächung von Verschlüsselungstechnologien stellt das Ausnutzen existierender Schwachstellen ein geringeres Risiko dar. Gleichzeitig stellen offene Schwachstellen immer ein Risiko dar, unabhängig davon, wer sie verheimlicht. Umso notwendiger ist es, offene technische und rechtstaatliche Fragen schnell zu klären. So etwa, welches Handwerkzeug die Behörden nutzen dürfen, und ob sie dieses selbst entwickeln oder einkaufen, und unter welchen Bedingungen die Quellen-Telekommunikationsüberwachung und die online-Durchsuchung durchzuführen sind. Hier hat das Bundesverfassungsgericht aus gutem Grund klare Grenzen gesetzt, und es muss sichergestellt werden, dass die technischen Möglichkeiten sich in diesen bewegen und dass Verfahrensvorkehrungen entsprechend getroffen werden. Vor allem muss die Bundesregierung dringend ein möglichst transparentes Schwachstellenmanagementsystem erarbeiten, um darzulegen, unter welchen Rahmenbedingungen Schwachstellen eingesetzt werden, und um zu garantieren, dass diese auch an die Unternehmen weitergeben werden.

Unabhängig von Regulierungen staatlicher Seite wird der technologische Wandel weiter rapide voranschreiten. Umso wichtiger ist es, Kriminellen langfristig nicht in die Hände zu spielen. Zu diesem Zweck ist es unabdingbar, Technologien wie Verschlüsselung, von der eine Masse an Nutzern profitieren, nicht zu unterminieren. Stattdessen sollte der Fokus darauf liegen, die Kapazitäten der Behörden in einem rechtstaatlichen Rahmen gezielt zu stärken, um ihnen ihre Arbeit zu ermöglichen. So werden letztlich sowohl die Informations- als auch die öffentliche Sicherheit gestärkt.

Der Autor

Mirko Hohmann ist Projektleiter am Global Public Policy Institute (GPPi). Seine Forschungsinteressen liegen im Zusammenspiel zwischen Politik und Technologie. Er leitet die Tätigkeiten des Instituts im Bereich Data and Technology Politics und koordiniert die Transatlantic Digital Debates. Er ist Mitglied bei D64 – Zentrum für Digitalen Fortschritt und war im Jahr 2016 Gastdozent an der Hertie School of Governance.

Danksagung

Der Autor bedankt sich bei Carl Michaelis und Laurenz Derksen für die Forschungsunterstützung, Alexander Pirang und Thorsten Benner für Hilfe bei der Konzeption der Studie, Isabel Skierka für viele Diskussionen zu dem Thema, Oliver Read für die Erstellung der grafischen Aufarbeitungen sowie Aurélie Domisse, Christian Senninger, Sabine Hämmerling und Matteo Schürenberg für inhaltliche Rückmeldungen zu früheren Versionen des Textes.

Impressum

Herausgeberin: Heinrich-Böll-Stiftung e.V., Schumannstraße 8, 10117 Berlin
Kontakt: Dr. Sergey Lagodinsky, Referatsleitung EU/Nordamerika **E** lagodinsky@boell.de

Erscheinungsort: www.boell.de
Erscheinungsdatum: Januar 2018

Weitere E-Books zum Downloaden unter
www.boell.de/publikationen

Endnoten

[1] Ellen Nakashima and Andrea Peterson, «Obama administration opts not to force firms to decrypt data – for now,» *Washington Post*, 8. Oktober 2015, abgerufen am 4. März 2017, www.washingtonpost.com/world/national-security/obama-administration-opts-not-to-force-firms-to-decrypt-data--for-now/2015/10/08/1d6a6012-6dca-11e5-aa5b-f78a98956699_story.html?utm_term=.e85525bf1395.

[2] Jason Shueh, «Obama Asks Tech Industry to Compromise on Encryption,» *Government Technology*, 11. März 2016, abgerufen am 9. März 2017, www.govtech.com/Obama-Asks-Tech-Industry-to-Compromise-on-Encryption.html.

[3] Russell Brandom, «Trump's attorney general pick could restart the encryption fight,» *The Verge*, 18. November 2016, abgerufen am 12. März, 2017, www.theverge.com/2016/11/18/13677798/attorney-general-jeff-sessions-encryption-san-bernardino-trump.

[4] Lindsey J. Smith, «Donald Trump on Apple encryption battle: ‹Who do they think they are?›» *The Verge*, 17. Februar 2016, abgerufen am 6. März 2017, www.theverge.com/2016/2/17/11031910/donald-trump-apple-encryption-backdoor-statement.

[5] Investigatory Powers Bill, part 9, chapter 1 , sections 254–256, 5,c, www.publications.parliament.uk/pa/bills/lbill/2016-2017/0066/17066.pdf

[6] Schweizerische Eidgenossenschaft, *Bundesgesetz über den Nachrichtendienst* (2015), Art. 43, S. 2, www.admin.ch/opc/de/federal-gazette/2015/7211.pdf

[7] Jan Schüßler, «CSU-Innenminister: Polizei muss WhatsApp mitlesen können», *Heise Online*, 4. April 2017, abgerufen am 1. März 2017, www.heise.de/newsticker/meldung/CSU-Innenminister-Polizei-muss-WhatsApp-mitlesen-koennen-3672986.html

[8] New York County District Attorney's Office, «Report on Smartphone Encryption and Public Safety» (2015), abgerufen am 6. März 2017, http://manhattanda.org/sites/default/files/11.18.15%20Report%20on%20Smartphone%20Encryption%20and%20Public%20Safety.pdf.

[9] Bundesamt für Sicherheit in der Informationstechnik, «Glossar und Begriffsdefinitionen», abgerufen 9. März 2017, www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/Glossar/glossar_node.html

[10] Edward W. Felton, «Nuts and Bolts of Encryption: A Primer for Policymakers», (Princeton: Center for Information Technology Policy, 2017), abgerufen am 6. März 2017, www.cs.princeton.edu/~felten/encryption_primer.pdf.

[11] Edward Felten, «Praktische Grundlagen der Verschlüsselung: Ein Leitfaden für Entscheidungsträger,» *Netzpolitik.org*, 27. Februar 2017, abgerufen am 8. März 2017, https://netzpolitik.org/2017/praktische-grundlagen-der-verschluesselung-ein-leitfaden-fuer-entscheidungstraeger

[12] Richard Beary, «Going Dark: Addressing the Challenges of Data, Privacy and Public Safety,» *Police Chief Magazine*, April 2015, abgerufen am 6. März 2017, www.policechiefmagazine.org/magazine/index.cfm?fuseaction=display&article_id=3673&issue_id=42015.

[13] James B. Comey, «Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course?» (speech, Washington, DC, October 16, 2014), Federal Bureau of Investigation, abgerufen am 8. März 2017, www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course; Going *Dark: Encryption, Technology, and the Balances Between Public Safety and Privacy: Hearings Before the Senate Judiciary Committee*, Joint Statement of James B. Comey, Director, Federal Bureau of Investigation, and Sally Quillian Yates, Deputy Attorney General, 8. Juli

2015, abgerufen am 6. März 2017, www.fbi.gov/news/testimony/going-dark-encryption-technology-and-the-balances-between-public-safety-and-privacy.

[14] Wie am Ende dieses Teils ausgeführt wird, betreffen die genannten Entwicklungen nicht alle Behörden gleich. Abhängig von den vorhandenen technischen, finanziellen und personellen Kapazitäten haben sie unterschiedliche Ermittlungsmöglichkeiten und damit auch unterschiedliche Herausforderungen.

[15] International Association of Chiefs of Police, «Data, Privacy, and Public Safety: A Law Enforcement Perspective on the Challenges of Gathering Electronic Evidence» (2015), S. 7., abgerufen am 9. März 2017: www.theiacp.org/portals/0/documents/pdfs/IACPSummitReportGoingDark.pdf

[16] Hintergrundgespräch mit einem Vertreter des US Department of Justice am 13. November 2016.

[17] Wie später noch ausgeführt wird, ist es wichtig, zwischen den Interessen, Problemen und technischen Möglichkeiten von verschiedenen Sicherheitsbehörden zu unterscheiden, da zum Beispiel Strafverfolgungsbehörden eine andere Perspektive auf die Thematik haben als Geheimdienste.

[18] Jeff Desjardins, «What Happens in an Internet Minute in 2016?», *Visual Capitalist*, 25. April 2016, abgerufen am 19. März 2017, www.visualcapitalist.com/what-happens-internet-minute-2016

[19] James A. Lewis, Denise E. Zheng, und William A. Carter, *The Effect of Encryption on Lawful Access to Communications and Data*. CSIS Report. (Washington, D.C.: Center for Strategic and International Studies, 2017): S. 7 ff., www.csis.org/analysis/effect-encryption-lawful-access-communications-and-data.

[20] Wissenschaftlicher Arbeitskreis für Regulierungsfragen bei der Bundesnetzagentur, «Evolution der Regulierung in den Telekommunikations- und Mediensektoren angesichts der Relevanzzunahme von OTT-Anbietern,» Seite 26 ff., abgerufen am 15. Mai 2017, www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Allgemeines/Bundesnetzagentur/WAR/WAR_OTT.pdf?__blob=publicationFile&v=1

[21] European Union Agency for Law Enforcement Cooperation, «Internet Organized Crime Threat Assessment» (2016): S. 11. www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2016

[22] Danny Yandron, «WhatsApp rolls out full encryption to a billion messenger users,» *The Guardian*, 5. April 2016, abgerufen am 6. März 2017, www.theguardian.com/technology/2016/apr/05/whatsapp-rolls-out-full-encryption-to-a-billion-messenger-users

[23] Lewis, Zhang, and Carter, «The Effect of Encryption on Lawful Access to Communications and Data»: 2.

[24] Woodrow Hartzog, «The Feds Are Wrong to Warn of ‹Warrant-Proof› Phones,» *MIT Technology Review*, 17. 17. März 2016, abgerufen am 12. März 2017, www.technologyreview.com/s/601044/the-feds-are-wrong-to-warn-of-warrant-proof-phones/#/set/id/601060

[25] New York County District Attorney's Office, «Report on Smartphone Encryption and Public Safety,» 4.

[26] Apple führte damals an, dass es für den Zugriff erst neue Software entwickeln müsste und weigerte sich gleichzeitig, dies zu tun. Im Endeffekt gelang dem FBI der Zugriff auf das Handy über einen externen Dienstleister, der eine Schwachstelle in der Konfiguration von Apples Software ausnutzte.

[27] Jennifer Daskal, *International Spillover Effects*. Aegis Paper Series. (Stanford, CA: Hoover Institution, 2016): 2, www.hoover.org/sites/default/files/research/docs/daskal_webreadypdf.pdf

[28] Danielle Kehl, Kevin Bankston, and Andi Wilson, «Comments to the UN Special Rapporteur on Freedom of Expression and Opinion Regarding the Relationship Between Free Expression and the Use of Encryption.» New America Open Technology Institute, 10. Februar 2015: 7.

[29] Kehl, Bankston, and Wilson, «Comments to the UN Special Rapporteur on Freedom of Expression and Opinion Regarding the Relationship Between Free Expression and the Use of Encryption»: 4.

[30] Andrew Weissmann, «Apple, Boyd, and Going Dark,» *Just Security*, 20. Oktober, 2014, abgerufen am 8. März 2017, www.justsecurity.org/16592/apple-boyd-dark

[31] Harold Abelson, et. al., *Keys Under Doormats: Mandating insecurity by requiring government access to all data and communications*. DSpace@MIT (Cambridge, MA: Massachusetts Institute of Technology, 2015), https://dspace.mit.edu/bitstream/handle/1721.1/97690/MIT-CSAIL-TR-2015-026.pdf

[32] Steven Levy, «Battle of the Clipper Chip,» *The New York Times*, 12. Juni 1994, abgerufen am 15. März 2017, www.nytimes.com/1994/06/12/magazine/battle-of-the-clipper-chip.html?pagewanted=all

[33] The White House, Office of the Vice President, «Vice President on Clipper 4.», 1. Oktober 1996, abgerufen am 12. März 2017, https://epic.org/crypto/key_escrow/clipper4_statement.html

[34] Für eine breitere Diskussion der Argumente gegen staatlichen Zugang, siehe «Die Kritik: Notwendigkeit, Umsetzung und negative Auswirkungen»

[35] Daniel Weitzner, «The Encryption Debate Enters Phase Two,» *Lawfare*, 6. März 2016, abgerufen am 8. März 2017, www.lawfareblog.com/encryption-debate-enters-phase-two

[36] Daskal, *International Spillover Effects*, S. 4.

[37] Julian Sanchez, «Feinstein-Burr: The Bill That Bans Your Browser.» *Just Security*, 29. April 2016. www.justsecurity.org/30740/feinstein-burr-bill-bans-browser

[38] Rod Rosenstein «Remarks on Encryption at the United States Naval Academy», *US Department of Justice*, 10. Oktober 2017, abgerufen am 10. Dezember 2017 von www.justice.gov/opa/speech/deputy-attorney-general-rod-j-rosenstein-delivers-remarks-encryption-united-states-naval

[39] Investigatory Powers Bill, part 9, chapter 1 , sections 254–256, 5,c, www.publications.parliament.uk/pa/bills/lbill/2016-2017/0066/17066.pdf

[40] Schweizerische Eidgenossenschaft, *Bundesgesetz über den Nachrichtendienst*, Art. 43, S. 2: www.admin.ch/opc/de/federal-gazette/2015/7211.pdf

[41] Lewis, Zhang, and Carter, «The Effect of Encryption on Lawful Access to Communications and Data»: 20.

[42] Stoldt, Till-Reimer, «Bayern verlangt polizeiliche Überwachung von WhatsApp.» *Die Welt*, 1. April 2017. www.welt.de/politik/deutschland/article163317902/Bayern-verlangt-polizeiliche-Ueberwachung-von-WhatsApp.html

[43] Peter Swire and Kenesa Ahmad, «‹Going Dark› Versus a ‹Golden Age for Surveillance›.» (Washington, D.C.: Center for Democracy and Technology, 2011). https://stanford.edu/~jmayer/law696/week8/Going%20Dark%20or%20Golden%20Age.pdf

[44] Hartzog, «The Feds Are Wrong to Warn of ‹Warrant-Proof› Phones.»

[45] Peter Swire, «The Golden Age of Surveillance», *Slate*, 15. Juli 2015, abgerufen am 15 März 2017, www.slate.com/articles/technology/future_tense/2015/07/encryption_back_doors_aren_t_necessary_we_re_already_in_a_golden_age_of.html

[46] Swire and Ahmad, «‹Going Dark› Versus a ‹Golden Age for Surveillance›», S. 4.

[47] Berklett Cybersecurity Project, «Don't Panic: Making Progress on the ‹Going Dark› Debate.» (Cambridge, MA: Berkman Klein Center for Internet and Society, 2016). https://cyber.harvard.edu/pubrelease/dont-panic/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf

[48] David E. Sanger, «New Technologies Give Government Ample Means to Track Suspects, Study Finds.» *The New York Times*, 31. Januar 2016, abgerufen am 12. März 2017, www.nytimes.com/2016/02/01/us/politics/new-technologies-give-government-ample-means-to-track-suspects-study-finds.html?_r=0

[49] U.S. Courts, «Wiretap Report 2016» (2016). www.uscourts.gov/statistics-reports/wiretap-report-2016

[50] Andrea Castillo and Eli Dorado, «Going Dark? Federal Wiretap Data Show Scant Encryption Problems,» (Washington, D.C.: Mercatus Center, 2016). www.mercatus.org/system/files/Going-Dark.pdf

[51] Anne Johnson, Emily Grumbling, and Jon Eisenberg, «Exploring Encryption and Potential Mechanisms for Authorized Government Access to Plaintext: Proceedings of a Workshop.» (Washington, D.C.: National Academy of Sciences, 2016): 8, http://cryptome.org/2016/08/nap-encryption-gov-access.pdf

[52] Lewis, Zhang, and Carter, «The Effect of Encryption on Lawful Access to Communications and Data»: 7.

[53] New York County District Attorney's Office, «Report on Smartphone Encryption and Public Safety»: 4–5.

[54] Der Unterschied lässt sich darauf zurückführen, dass Apple sowohl die Hard- als auch Software zur Verfügung stellt, was bei Android-Geräten in der Regel nicht der Fall ist; der Update-Zyklus verzögert sich daher.

[55] Kevin Bankston, «The Numbers Don't Lie», *Slate*, 18. August 2015, abgerufen am 1. März 2017, www.slate.com/articles/technology/future_tense/2015/08/default_smartphone_encryption_will_stop_more_crimes_than_it_permits.html

[56] Lewis, Zhang, and Carter, «The Effect of Encryption on Lawful Access to Communications and Data»: S. 15

[57] Hartzog, «The Feds Are Wrong to Warn of ‹Warrant-Proof› Phones.»

[58] Edward Felten, «How to Analyze An Encryption Access Proposal», *Freedom to Tinker*, 27. März 2017, abgerufen am 1. April 2017, https://freedom-to-tinker.com/2017/03/27/how-to-analyze-an-encryption-access-proposal

[59] Abelson et al. *Keys Under Doormats*

[60] Bruce Schneier, Kathleen Seidel, and Saranya Vijayakumar, «A Worldwide Survey of Encryption Products» (Cambridge, MA: Berkman Center for Internet and Society, 2016), www.schneier.com/academic/paperfiles/worldwide-survey-of-encryption-products.pdf

[61] Bankston et al. «An Illustrative Inventory of Widely-Available Encryption Applications» (Washington D.C.: New America Open Technology Institute, 2015), https://static.newamerica.org/attachments/12155-the-crypto-cat-is-out-of-the-bag/Crypto_Cat_Jan.0bea192f15424c9fa4859f78f1ad6b12.pdf

[62] Daskal, *International Spillover Effects*, S. 8.

[63] U.S. House Homeland Security Committee, «Going Dark, Going Forward. A Primer on the Encryption Debate» (2016): S.3, abgerufen am 20. März 2017, https://homeland.house.gov/wp-content/uploads/2016/07/Staff-Report-Going-Dark-Going-Forward.pdf

[64] Johnson, Grumbling, and Eisenberg, «Proceedings of a Workshop», 17.

[65] Abelson et al., *Keys under Doormats*, S. 16.

[66] Johnson, Grumbling, and Eisenberg, «Proceedings of a Workshop», 32.

[67] Orin Kerr, «Apple's dangerous game, part 2: The strongest counterargument», *The Washington Post*, 24. September 2014, abgerufen am 20. März 2017, www.washingtonpost.com/news/volokh-conspiracy/wp/2014/09/22/apples-dangerous-game-part-2-the-strongest-counterargument

[68] Daskal, *International Spillover Effects*, S. 13.

[69] Johnson, Grumbling, and Eisenberg, «Proceedings of a Workshop», 23.

[70] Carrie Cordero, «Is There a National Security-Law Enforcement Divide on ‹Going Dark›?», *Lawfare Blog*, 3. Februar 2016, abgerufen am 20. März 2017, www.lawfareblog.com/there-national-security-law-enforcement-divide-going-dark

[71] Ibid.

[72] Bundeskriminalamt, «Bundeslagebild Cybercrime», 27. Juli 2016, S. 19, www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2015.html?nn=28110

[73] John Naughton, «After Edward Snowden's revelations, why trust US cloud providers?», *The Guardian*, 15. September 2013, abgerufen am 25. März 2017, www.theguardian.com/technology/2013/sep/15/edward-snowden-nsa-cloud-computing

[74] Bruce Schneier et al. «A Worldwide Survey of Encryption Products.»

[75] United Nations Educational, Scientific and Cultural Organization, *UNESCO Series on Internet Freedom: Human Rights and Encryption* (Paris: 2016)., S. 61, http://unesdoc.unesco.org/images/0024/002465/246527E.pdf

[76] United Nations Human Rights Office of the High Commissioner, *Report on Encryption, Anonymity, and the Human Rights Framework*, A/HRC/29/32, 22. Mai, 2015. www.ohchr.org/EN/Issues/FreedomOpinion/Pages/CallForSubmission.aspx

[77] European Union Agency for Law Enforcement Cooperation, «Serious and Organised Crime Threat Assessment: Crime in the Age of Technology» (2017), S. 26, www.europol.europa.eu/activities-services/main-reports/european-union-serious-andorganised-crime-threat-assessment-2017

[78] Es ist wichtig, darauf hinzuweisen, dass im Folgenden die Arbeit der Geheimdienste weitestgehend ausgeklammert wird, da diese in einem anderen technischen und legalen Umfeld agieren.

[79] Adam Segal and Alex Grigsby, «How to break the deadlock over data encryption», *The Washington Post*, 13. März 2016, abgerufen am 25. März 2017, www.washingtonpost.com/opinions/how-to-break-the-deadlock-over-data-encryption/2016/03/13/e677fb78-d110-11e5-88cd-753e80cd29ad_story.html

[80] Bundesverfassungsgericht, Urteil des Ersten Senats vom 20. April 2016 – 1 BvR 966/09 – Rn. (1–29). Abgerufen am 5. April 2017, www.bverfg.de/e/rs20160420_1bvr096609.html

[81] Siehe unter anderem M. Bellovin, Matt Blaze, Sandy Clark, and Susan Landau. «Lawful hacking: Using existing vulnerabilities for wiretapping on the Internet» (Northwestern Journal of Technology

and Intellectual Property, 2014), http://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=1209&context=njtip; www.brookings.edu/research/lawful-hacking-and-the-case-for-a-strategic-approach-to-going-dark

[82] Kevin Bankston, «Ending The Endless Crypto Debate», Lawfare, 14. Juni 2017, abgerufen am 16. Juni 2017, https://lawfareblog.com/ending-endless-crypto-debate-three-things-we-should-be-arguing-about-instead-encryption-backdoors

[83] Ulf Buermeyer, «Gutachterliche Stellungnahme», Deutscher Bundestag, 31. Mai 2017, abgerufen am 16. Juni 2017, www.bundestag.de/blob/508848/bdf7512e32578b699819a5aa33dde93c/buermeyer-data.pdf

[84] Bundesverfassungsgericht, «Vorschriften im Verfassungsschutzgesetz NRW zur Online-Durchsuchung und zur Aufklärung des Internet nichtig, Pressemitteilung Nr. 22/2008 vom 27. Februar 2008», abgerufen am 7. Juni 2017, www.bundesverfassungsgericht.de/SharedDocs/Pressemitteilungen/DE/2008/bvg08-022.html

[85] Patrick Beuth und Kai Biermann, «Dein trojanischer Freund und Helfer», *ZEIT Online*, 22. Juni 2016, abgerufen am 25. Juni 2017, www.zeit.de/digital/datenschutz/2017-06/staatstrojaner-gesetz-bundestag-beschluss/komplettansicht

[86] Axel Anbank, «9 Problems of Government Hacking: Why IT-Systems Deserve Constitutional Protection», *Freedom to Tinker*, 20. Februar 2014, abgerufen am 25. März 2017, https://freedom-to-tinker.com/blog/axel/9-problems-of-governments-hacking-why-it-systems-deserve-constitutional-protection; Marshall Erwin, «Lawful Hacking After the Encryption Debate», *Just Security*, 15. Oktober 2015, abgerufen am 25. März 2017, www.justsecurity.org/26849/lawful-hacking-encryption-debate; Larry Greenemeier, «Wiretaps through Software Hacks to Get Legal Scrutiny», *The Scientific American*, 6. Juni 2013, abgerufen am 27. März 2017, www.scientificamerican.com/article/web-wiretap-legal-scrutiny-for-privacy

[87] Sven Herpig, «Government Hacking: Computer Security vs. Investigative Powers», *Stiftung Neue Verantwortung*, Juni 2017, S. 6.

[88] Alasdair Allan, «Don't Draw The Wrong Conclusions From The Wannacry Ransomware Outbreak», *motherboard*, 15. Mai 2017, abgerufen am 15. Juni 2017, https://motherboard.vice.com/en_us/article/vv5x4d/dont-draw-the-wrong-conclusions-from-the-wannacry-ransomware-outbreak

[89] Michael Daniel, «Heartbleed: Understanding When We Disclose Cyber Vulnerabilities», The Obama White House Archives, 28. April 2014, abgerufen am 15. April 2017, https://obamawhitehouse.archives.gov/blog/2014/04/28/heartbleed-understanding-when-we-disclose-cyber-vulnerabilities

[90] Rob Joyce, «Improving and Making the Vulnerability Equities Process Transparent is the Right Thing to Do», The White House, 15. November 2017, abgerufen am 10. Dezember 2017 von www.whitehouse.gov/blog/2017/11/15/improving-and-making-vulnerability-equities-process-transparent-right-thing-do

[91] Sven Herpig, «Government Hacking: Computer Security vs. Investigative Powers», *Stiftung Neue Verantwortung*, Juni 2017, S. 12ff.

[92] Lewis, Zhang, and Carter, «The Effect of Encryption on Lawful Access to Communications and Data», 31.

[93] Bundesministerium des Inneren, «Startschuss für ZITiS», abgerufen am 27. März 2017, www.bmi.bund.de/SharedDocs/Pressemitteilungen/DE/2017/01/zitis-vorstellung.html

[94] Friedhelm Greis, «Bundesnetzagentur setzt Vorratsdatenspeicherung aus», ZEIT Online, 28. Juni 2017, abgerufen am 07. Juli 2017, www.zeit.de/digital/datenschutz/2017-06/gerichtsurteil-vorratsdatenspeicherung-bundesnetzagentur

[95] Mirko Hohmann, «German Bundestag Passes New Data Retention Law», *Lawfare Blog*, 16. Oktober 2015, abgerufen am 27. März 2017, www.lawfareblog.com/german-bundestag-passes-new-data-retention-law

[96] Wolfgang Janisch, «Das Privatleben bleibt geschützt», *Süddeutsche Zeitung*, 21. Dezember 2016, abgerufen am 29. März 2017, www.sueddeutsche.de/politik/vorratsdatenspeicherung-das-privatleben-bleibt-geschuetzt-1.3304988

[97] Caroline Goemans and Jos Dumortier, «Enforcement issues – Mandatory retention of traffic data in the EU: Possible impact on privacy and on-line anonymity» (Leuven: Interdisciplinary Centre for Law and Information, 2003): 6. www.law.kuleuven.be/citip/en/docs/publications/440retention-of-traffic-data-dumortier-goemans2f90.pdf

[98] Wolfgang Janisch, «Das Privatleben bleibt geschützt».

[99] Friedhelm Greis, «Bundesnetzagentur setzt Vorratsdatenspeicherung aus», *ZEIT Online*, 28. Juni 2017, abgerufen am 07. Juli 2017, www.zeit.de/digital/datenschutz/2017-06/gerichtsurteil-vorratsdatenspeicherung-bundesnetzagentur

[100] Jonah Force Hill, «The Growth of Data Localization Post-Snowden: Analysis and Recommendations for U.S. Policymakers and Industrial Leaders», *Lawfare Paper Research Series*, vol. 2, no. 3 (2014): S.3, https://lawfare.s3-us-west-2.amazonaws.com/staging/Lawfare-Research-Paper-Series-Vol2No3.pdf

[101] Anupam Chander and Uyen P. Le, «Breaking the Web: Data Localization vs. the Global Internet», (Davis, CA: University of California Davis Legal Studies Research Paper Series, 2014), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2407858%20

[102] Um Zugriff auf *Metadaten* zu erhalten, können deutsche Ermittler schon jetzt bei den Vertretungen in Deutschland oder sogar den ausländischen Service Providern anfragen. Für Inhaltsdaten ist allerdings der Weg über das offizielle Rechtshilfeverfahren notwendig.

[103] Jonah Force Hill, «Problematic Alternatives: MLAT Reform for the Digital Age,» *Harvard Law School National Security Journal*, 28. Januar 2015, abgerufen am 28. März 2017, http://harvardnsj.org/2015/01/problematic-alternatives-mlat-reform-for-the-digital-age

[104] U.S. Department of Justice, «FY 2015 Budget Request: Mutual Legal Assistance Treaty Process Form» (2015), S.1 abgerufen am 15. März 2017, www.justice.gov/sites/default/files/jmd/legacy/2014/07/13/mut-legal-assist.pdf

[105] Alan and McQuinn and Daniel Castro, «How Law Enforcement Should Access Data Across Borders,» Information Technology & Innovation Foundation, Juli 2017, abgerufen am 15. August 2017 von https://itif.org/publications/2017/07/24/how-law-enforcement-should-access-data-across-borders

[106] U.S. Homeland Security Committee, «Going Dark, Going Forward,» 13.

[107] Jennifer Daskal and Andrew K. Woods, «A New US-UK Data Sharing Treaty?», *Just Security*, 23. Juni 2015, abgerufen am 28. März 2017, www.justsecurity.org/24145/u-s-u-k-data-sharing-treaty

[108] Europäische Kommission, «Improving cross-border access to electronic evidence: findings from the expert process and suggested way forward,» Non-paper from the Commission service, 22. Mai 2017, abgerufen am 1. August 2017, https://ec.europa.eu/home-affairs/sites/homeaffairs/files/docs/pages/20170522_non-paper_electronic_evidence_en.pdf

[109] Georg Mascolo, Reiko Pinkert, Ronen Steinke, and Hakan Tanriverdi, «Kaum ein Hacker will zum BND,» *Süddeutsche Zeitung*, www.sueddeutsche.de/digital/geheimdienst-kaum-ein-hacker-will-zum-bnd-1.3446843

[110] Deutscher Bundestag, Drucksache 18/7721, S. 18. Abgerufen am 5. April 2017, http://dipbt.bundestag.de/doc/btd/18/077/1807721.pdf

[111] Markus Reuter, «Innenminister fordern Hintertüren gegen Verschlüsselung – in der französischen Version der gemeinsamen Erklärung (Update),» *netzpolitik.org*. Abgerufen am 5. April 2017, https://netzpolitik.org/2016/innenminister-fordern-hintertueren-gegen-verschluesselung-in-der-franzoesischen-version-der-gemeinsamen-erklaerung

[112] Telekommunikationsgesetz, §110, abgerufen am 5. April 2017, www.gesetze-im-internet.de/tkg_2004/__110.html