Chaos Computer Club

Stellungnahme an das Bundesverfassungsgericht zum BND-Gesetz und zur Ausland-Ausland-Fernmeldeaufklärung

1 BvR 2835/17

Constanze Kurz,
Dirk Engling, Rainer Rehak

27. November 2019

Gegenstand der Stellungnahme

Gegen das BND-Gesetz wurden verschiedene verfassungsrechtliche Bedenken aufgeworfen. Diese Stellungnahme widmet sich den technischen Fragen beim Mitschneiden von Telekommunikation und bei der Filterung und Analyse der Inhalts- und Metadaten. Behandelt sind die technischen Gegebenheiten bei der paketvermittelten Kommunikation und die Möglichkeiten der Überwachung von Ausland-Ausland-Kommunikation sowie der staatlichen Infiltration, mit welcher der BND auch ohne Mitwirkung von Telekommunikationsanbietern Datenverkehr ausleiten könnte.

Heutige technische Gegebenheiten: Netzstruktur

Kommunikation im Netz ist heute gekennzeichnet durch dynamische und komplexe Systeme, die ineinander greifen, um technische Standards und vertragliche Vereinbarungen zwischen Netzbetreibern und Diensteanbietern unterschiedlicher Leistungsfähigkeit und Größe umzusetzen. Datenströme werden typischerweise dynamisch über verschiedenste Routen und Medien durch das Netz geschickt. Auch die direkten Peering-Verbindungen zwischen darauf spezialisierten Anbietern werden in zunehmendem Maße dynamischer.[1] Bei Unterbrechungen von Verbindungen oder hohem Datenaufkommen greifen heute in der Regel automatische Mechanismen, die den Datenverkehr über alternative Routen leiten.

Die im BNDG unterschiedenen inländischen, ausländischen und internationalen Datenverkehre spiegeln nicht die heutige Netzstruktur wider, wenn es um das Überwachen und Filtern der Telekommunikation geht. Vielmehr wird der Weg bei paketvermittelter Kommunikation zwischen zwei Teilnehmern regelmäßig ad hoc und dynamisch bestimmt, ist auch innerhalb eines Kommunikationsprozesses veränderlich und überschreitet dabei oft mehrfach Landesgrenzen. Das erschwert die Analyse, wenn aus rechtlichen Gründen zwischen inländischen, ausländischen und internationalen Datenverkehren unterschieden werden muss.

In der Regel ist diese Differenzierung der Datenverkehre nicht vollständig möglich. Die Gründe liegen nicht nur in der Dynamik der Netzstruktur, sondern auch am verbreiteten Einsatz von Tunneltechnologien und sog. Virtuellen Privaten Netzen (VPN).[2]

Dass eine Kommunikationsbeziehung die gleichen Hin- und Rückwege nimmt, ist zudem nicht immer gegeben und erschwert die Zuordnung nach Inland oder Ausland weiter. Beispielsweise können Messenger oder Videotelefonie-Verbindungen einen

---

[1] Peering ist durch eine feste Verbindung gekennzeichnet, bei der zwei Netzanbieter eine direkte Verbindung zwischen ihren Netzen schalten. Internet Service Provider, Netzbetreiber oder Content Delivery Networks tauschen dabei kostenneutral Datenverkehr aus. Vgl. zur Peering-Praxis und zu Netzknoten: NSA-Untersuchungsausschuss des Bundestags, Gutachten Rechthien MAT A SV-13/3, S. 7.

[2] Vgl. NSA-Untersuchungsausschuss des Bundestags, Gutachten Rodosek MAT A SV-13/3, S. 14f.

Kommunikationskanal nutzen, dessen Hinweg über London und dessen Rückweg über Frankfurt läuft, oder auch mehrere Verbindungen in verschiedene Rechenzentren an unterschiedlichen Orten aufbauen.

Während bei Fax und Telefon die Anschlussinhaber und Benutzer zuverlässig zuzuordnen sind, ist dies bei IP-Paketen im Internet nicht möglich. Die Zuordnung eines Datenstroms zu einer Person und damit auch die Kategorisierung ob inländisch, ausländisch oder international ist nur gesichert möglich, wenn Einblick in die übertragenen Daten genommen wird.

Die Daten, die zur Leitung des Paketes verwendet werden, sogenannte IP-Adressen, sagen lediglich aus, wo sich der Benutzer netztopologisch, nicht aber physikalisch befindet und mit welchem Server er kommuniziert. Dies sind die Source- und Destination-Felder im Paket. Um nun eine Person und ihren genauen Ort eindeutig zu identifizieren, muss man tiefer in die Pakete hineinschauen und zum Beispiel die Anmelde-Phase an einem Server mitlesen oder den Inhalt der übertragenen Nachricht analysieren. Da aber ein Großteil der Daten, die das Paket transportiert, verschlüsselt sind, kann man hier nicht ohne weiteres hineinschauen.

Beispielhaft kann eine typische heutige Nutzung öffentlicher Hotspots aus Sicht des Überwachers betrachtet werden: An einem beliebigen Tag kommt ein normaler Benutzer an dutzenden öffentlichen Hotspots vorbei. Sie werden betrieben vom öffentlichen Nah- und Fernverkehr, von Supermärkten, Restaurants, Bibliotheken, Hotels und Bürgernetzen. Die Verbindungen von Teilnehmern in diesen Netzwerken werden dabei nicht selten erst über einen Tunnel in ein entferntes, oft auch im Ausland befindliches Rechenzentrum umgeleitet, teils weil der Betreiber seine Kunden-Wifis global verwaltet, teils weil der Dienstleister aus dem Ausland kommt oder Netz von dort mietet, teils weil rechtliche Probleme vermieden werden sollen.

Wer nun die Telekommunikation mitschneidet, kann zwar sehen, dass ein Nutzer hinter einem öffentlichen Hotspot beispielsweise die Website von web.de aufruft. Wer der Nutzer ist, ob er dort seine E-Mails abruft oder nur die dort angebotenen tagesaktuellen Nachrichten auf der Startseite liest, ob er deutscher Staatsbürger ist, lässt sich nicht feststellen beim bloßen Anblick des IP-Pakets und ohne die Verschlüsselung der Verbindung (https) zu brechen. Dass die Person web.de aufgerufen hat, ist nur noch an der IP-Adresse erkennbar, wenn der Verbindungsaufbau schon verschlüsselt ist. Dieses Beispiel lässt sich genauso auf viele weitere Dienste im Internet übertragen.

Wirksame technische Filter, die im Rahmen der Ausland-Ausland-Aufklärung eine Überwachung der Telekommunikation deutscher Bürger oder besonders geschützter Berufsgeheimnisträger vollständig und zuverlässig automatisiert verhindern können, sind nicht vorstellbar. Es ist in der heutigen Netzstruktur regelmäßig bei Beginn einer Kommunikation nicht vorab absehbar, welchen Weg die Datenpakete nehmen werden. Entsprechend ist es unvermeidbar, dass der BND auch beispielsweise E-Mails und Telefonate von journalistischen Informanten oder von EU-Einrichtungen und EU-Bürgern aufzeichnet.

Datenerfassung

Art und Umfang des Zugriffs auf Netze

Ein Telekommunikationsnetz ist definiert als die Gesamtheit von Übertragungssystemen und gegebenenfalls Vermittlungs- und Leitwegeinrichtungen sowie anderweitigen Ressourcen, einschließlich der nicht aktiven Netzbestandteile, die die Übertragung von Signalen über Kabel, Funk, optische und andere elektromagnetische Einrichtungen ermöglichen, einschließlich Satellitennetzen, festen, leitungs- und paketvermittelten Netzen, einschließlich des Internets, und mobilen terrestrischen Netzen, Stromleitungssystemen, soweit sie zur Signalübertragung genutzt werden, Netzen für Hör- und Fernsehfunk sowie Kabelfernsehnetzen, unabhängig von der Art der übertragenen Information. Durch diese weite Definition sind dem BND zunächst keine Schranken gesetzt, welche Teile der Netze er anzapfen kann.

Doch das geheimdienstliche Ausleiten hat wegen der heutigen hochbandbreitigen Verbindungen Kapazitätsgrenzen. Daher wird in der Regel nicht der gesamte Verkehr etwa eines großen Internet Exchanges überwacht, sondern werden Teile der Netzwerk-Struktur gespiegelt. Typisch ist beispielsweise die Spiegelung von einzelnen Kunden-Ports (in der Regel 10-GBit/s oder 100-GBit/s-Ports) auf den Routern in Internet Exchanges oder die Ausleitung der Daten einzelner Transit-Kunden unter Zuarbeit des jeweiligen Internet Service Providers.

Da sich § 8 BNDG auf das Erbringen von Telekommunikationsdiensten bezieht, können davon alle Unternehmen betroffen sein, die direkt oder indirekt in Deutschland eine Telekommunikationsinfrastruktur betreiben. Dies sind primär große Unternehmen wie die Deutsche Telekom, Vodafone oder O2/Telefónica, die eigene Kommunikationsnetze besitzen, auch im Mobilfunk- oder Satellitenbereich. Betroffen sind aber auch Firmen, die fremde Netze mieten, um Internetzugänge anzubieten, in Deutschland beispielsweise das Unternehmen 1&1.

Da § 8 BNDG jedoch auch diejenigen Akteure mit einbezieht, die nicht direkt Telekommunikationsdienste anbieten, aber die an deren Erbringung mitwirken, fallen darunter zusätzlich Betreiber von Internet-Übergabepunkten bzw. Peering-Punkten wie beispielsweise DECIX oder BCIX sowie ebenfalls internationale Internet-diensteanbieter (Tier 1/2), die in Deutschland aktiv sind, wie etwa Level 3 Communications/CenturyLink. Praktisch geschah eine solche Überwachung beispielsweise schon in den geheimen BND-Operationen Eikonal[3] und Glotaic[4].

[3] Betroffen war die Deutsche Telekom, https://netzpolitik.org/2016/frank-walter-steinmeier-vor-dem-geheimdienst-untersuchungsausschuss/ vom 18. März 2016. Der BND-Telekom-Vertrag „Transit“ ist öffentlich: https://cdn.netzpolitik.org/wp-upload/2004-03-01_BND-Telekom-Transit-Vertrag.pdf

[4] Betroffen war der US-Anbieter MCI, https://www.spiegel.de/netzwelt/netzpolitik/cia-hatte-direkten-zugriff-auf-deutsche-telekommunikation-a-1051407.html vom 4. September 2015.

Anteil an weltweiter Kommunikation

Da in paketvermittelten Netzwerken die Verkehrswege schwer vorhersagbar sind, ist der Anteil an der weltweiten Kommunikation, auf den der BND mit seinen Befugnissen zugreifen darf, nicht eindeutig zu beziffern. Es kann beispielsweise passieren, dass Internetverkehr von den Vereinigten Staaten nach Marokko durch den weltgrößten Internetknoten DECIX in Frankfurt am Main geleitet wird.

Betrachtet man die Transferraten[5], kann nicht sinnvoll auf den globalen Anteil geschlossen werden, da einige Internetknoten, etwa in China, Iran oder den Vereinigten Staaten, keine Zahlen zur Verfügung stellen. Es kann allerdings anhand der Größe und strategischen Position deutscher Netz- und Netzknotenbetreiber davon ausgegangen werden, dass ein größerer Teil des Internetverkehrs der westlichen Welt durch deutsche Infrastrukturen fließt.

Anlasslose Massenüberwachung

Der BND hat in den letzten Jahren internationale Telekommunikationsverkehre jeweils unter Einsatz von tausenden Selektoren abgehört. Die Anzahl der eingesetzten Selektoren stieg zuletzt erneut.[6] Schon aufgrund der Menge der Datensätze sind Verfahren zur Filterung und Analyse automatisiert.

BND-Mitarbeiter sichten nach eigenen Angaben die erfassten Daten auch manuell auf Hinweise, ob Deutsche überwacht wurden, und „bereinigen“ in Folge den Bestand. Dabei soll zudem eine Prüfung stattfinden, ob der Kernbereich der privaten Lebensgestaltung der Kommunizierenden betroffen ist. Dazu muss der Inhalt der Kommunikation betrachtet werden, eine Kennzeichnung der Daten soll in einem solchen Falle erfolgen.

Dieses Vorgehen suggeriert, dass die Datenmenge gewissermaßen überschaubar wäre. Davon kann praktisch für alle davon betroffenen Grundrechtsträger aber keine Rede mehr sein. Zudem haben sich die BND-Angaben, dass jeweils alle Datensätze vor einer Weiterverarbeitung oder Weitergabe gefiltert und geprüft oder solche Weitergaben auch nur dokumentiert werden, als eine falsche Darstellung erwiesen.[7]

Auch in Ländern der Europäischen Union wurde seitens des BND abgehört und mit zahlreichen Selektoren hantiert, wie aus dem Abschlussbericht des NSA-BND-Untersuchungsausschusses des Bundestags hervorgeht. Betroffen waren laut dem Bericht ausländische, darunter auch europäische Amtsträger, Journalisten sowie

---

[5] Im September 2019 lag etwa der Spitzenwert bei 7,1 Tbit/s, vgl. https://www.de-cix.net/de/about-de-cix/media-center/press-releases/7-terabits-per-second-cracked vom 20. September 2019.

[6] Vgl. BT-Drucksache 19/10459: Unterrichtung durch das Parlamentarische Kontrollgremium, https://dip21.bundestag.de/dip21/btd/19/104/1910459.pdf vom 24. Mai 2019.

[7] Im Rahmen der geheimen BND-Operation „Glotaic“ wurden Telekommunikationsverkehre einschließlich Audiodaten abgehörter Gespräche ohne Prüfung „direkt nach USA geroutet“. https://www.spiegel.de/netzwelt/netzpolitik/cia-hatte-direkten-zugriff-auf-deutsche-telekommunikation-a-1051407.html vom 4. September 2015.

Mitarbeiter der UNO und von Hilfsorganisationen, Banken und ausländischen Unternehmen.

Um den gesamten Verkehr etwa an einer Glasfaserleitung zu überwachen und zu analysieren, wird der Datenstrom typischerweise gespiegelt und danach vorgefiltert, um die dabei selektierten Daten auszuwerten. Praktisch wird aber wegen des enormen Aufwands nicht die gesamte Glasfaserleitung in zweistelliger Terabit-Größenordnung gespiegelt, sondern Bruchteile davon im Bereich von 100 Gbit/s pro Schnittstelle.

Ob solche erheblichen Datenmengen tatsächlich durch BND-Mitarbeiter nach der Vorfilterung noch manuell gesichtet werden können, um Grundrechtsträger zu schützen, ist fraglich. Eine echte „datensatzspezifische" Prüfung ist in der Praxis illusorisch. Das gilt zugleich für eine sinnvolle nachgelagerte Prüfung durch die Kontrollinstanzen.

Das Vorgehen des BND lässt sich in zwei Stufen einteilen: zunächst Sammlung und Vorfilterung großer Datenmengen, danach Analyse und Auswertung selektierter Informationen. Technisch kann diese Analyse vielfältige Formen haben, etwa Datenabgleiche mit vorhandenen Informationen, Mustererkennung oder Spracherkennung. Dies stößt bei vollständiger Verschlüsselung auf unauflösbare Probleme.

Die technische Leistungsfähigkeit bei der heimlichen anlasslosen Massenüberwachung von großen Datenmengen bei Telekommunikationsverkehren durch Geheimdienste ist durch die Veröffentlichungen von Edward Snowden greifbarer geworden. Das von ihm enthüllte Programm „Tempora" ist die umfangreichste der bisher bekanntgewordenen Abhöroperationen.

„Tempora" ist der Codename für das Überwachungsprogramm des britischen Geheimdienstes GCHQ in Kooperation mit der US-amerikanischen NSA, dessen Existenz heute nicht mehr bestritten wird. Das Ziel des Programms ist es, den internationalen Internetverkehr anzuzapfen und zur Analyse zwischenzuspeichern. Das gelang auf technischem Wege an den Glasfaserknotenpunkten im Süden Großbritanniens und am Überseekabel TAT-14 ab dem Jahr 2011 als sog. „full take", also als vollständige Aufzeichnung aller darüber laufenden Verbindungen. Nach dem Bericht des Guardian[8] werden Inhaltsdaten der Kommunikation drei Tage und Metadaten der Telekommunikation für dreißig Tage zur Auswertung gespeichert.

Die Befugnis des § 6, Abs. 1 BNDG erlaubt eine solche Massenüberwachung, da sie zum einen weitgehend und zum anderen vage formuliert ist. Auch falls der BND heute technisch nicht in der Lage sein sollte,[9] diese Befugnis praktisch umzusetzen, steht gesetzlich einer massenhaften Erfassung nichts entgegen. Das bedeutet zugleich massenhafte Einblicke nicht nur in Kommunikation, sondern beispielsweise auch in Mobilitätsdaten. Letztlich sind immer mehr Aspekte des alltäglichen Lebens eines Großteils der Grundrechtsträger nicht nur digitalisiert, sondern werden auch online

---

[8] Vgl. https://www.theguardian.com/uk-news/2013/oct/25/leaked-memos-gchq-mass-surveillance-secret-snowden vom 25. Oktober 2013.

[9] Die Zentrale Stelle für Informationstechnik im Sicherheitsbereich (ZITiS) befindet sich im Aufbau. Die zu bildenden Fähigkeiten bei der Telekommunikationsüberwachung, Kryptoanalyse und Big-Data-Auswertung sollen auch dem BND dienen: ZITiS hat die Aufgabe, Bundes-Behörden mit Sicherheitsaufgaben bei informationstechnischen Fähigkeiten zu unterstützen. 13 der 62 Mitarbeiter waren zuvor hauptberuflich für den BND tätig bzw. sind entsandt oder dafür freigestellt, vgl. BT-Drucksache 19/6246, https://dip21.bundestag.de/dip21/btd/19/104/1910459.pdf vom 4. Dezember 2018.

verteilt und verarbeitet. Die Erfassung der Telekommunikation wandelt sich mehr und mehr in eine Erfassung von Lebensabläufen, Transaktionen (etwa Finanzen, Konsum) und Verhalten und Bewegungen von Menschen. Die massenhafte technisierte Überwachung von solchen persönlichen und höchstpersönlichen Daten durch Geheimdienste in Europa wurde im Zuge der Veröffentlichungen von Edward Snowden in großem Detail bekannt.[10] Zudem wächst mit dem Digitalisierung all dieser alltäglichen Handlungen auch die Wahrscheinlichkeit, dass immer mehr Zufallserkenntnisse gewonnen werden.

Zugriff ohne Mitwirkung Dritter

Wenn eine Datenerfassung ohne Hilfe der Netzbetreiber stattfinden soll, gibt es im wesentlichen zwei weitere Wege der Datenerlangung: Einerseits könnte sich der BND durch Überwindung von vorhandenen Schutzmechanismen direkten Zugriff auf die Software der Netzinfrastruktursysteme verschaffen (Infiltration); andererseits könnten die technischen Eigenschaften funkbasierter Übertragungstechniken ausgenutzt werden, bei denen Signale auch in der Nähe der Funkstationen abgefangen werden können. Damit kann Datenverkehr quasi passiv ohne physischen Zugriff mitgeschnitten werden (Funk- und Satellitenüberwachung).

Die Infiltration informationstechnischer Systeme erfolgt in der Regel in drei Schritten: das verdeckte Aufbringen der Spionagesoftware, die Datenausleitung und die (Selbst-)Entfernung der Spionagesoftware vom System. Bei der verdeckten Aufbringung werden Sicherheitslücken der Telekommunikationssysteme ausgenutzt und dadurch infiltriert. Ziel ist es, die Systeme ohne Wissen der Betreiber verdeckt zu steuern und umzukonfigurieren. Nach dem erfolgreichen Aufbringen der Software können nicht nur beliebige Daten ausgeleitet, sondern auch andere damit verbundene Systeme manipuliert werden.

Die dauerhafte und unbemerkte Infiltration von gut gesicherten Systemen ist technisch jedoch sehr aufwendig und riskant, da ständig Detektion und Deaktivierung verhindert werden müssen und zudem die Systeme im laufenden Betrieb durch die Betreiber selbst verändert werden könnten, etwa durch nötige Updates oder sonstige Anpassungen.

Das Aufbringen einer Schadsoftware zur Spionage kann nicht nur direkt in den Telekommunikationssystemen erfolgen, sondern auch über Zwischenstationen und die Geräte von Mittelspersonen, indem etwa zunächst der Computer einer Mitarbeiterin der Betreiberfirma infiltriert und von diesem aus auf die Netzsysteme zugegriffen wird, sobald sich die Mitarbeiterin an der Arbeitsstelle zum internen Betreibernetz verbindet.[11]

---

[10] Ein Beispiel ist die automatische Überwachung von Webcams mitsamt dem Versuch der Gesichtserkennung im Rahmen der Operation „Optic Nerve“, vgl. https://www.theguardian.com/world/2014/feb/27/gchq-nsa-webcam-images-internet-yahoo vom 28. Februar 2014.

[11] So geschehen beispielsweise bei der geheimdienstlichen Spionage mit der Schadsoftware „Regin“ beim belgischen Provider Belgacom, vgl. https://theintercept.com/2014/11/24/secret-regin-malware-belgacom-nsa-gchq/ vom 24. November 2014.

Bei derartigen Eingriffen kann es allerdings zu Funktionsstörungen in den infiltrierten Systemen kommen, was die Betreiber auf die Spionagesoftware aufmerksam machen kann. Falls es ein geplantes Enddatum für die geheimdienstliche Maßnahme gibt, muss die Spionagesoftware nach Ablauf der Frist wieder deaktiviert und vom Betreibersystem gelöscht werden, was wiederum technisch nicht trivial durchführbar ist.[12]

Die Beschaffung der für die Infiltration nötigen Sicherheitslücken ist mit weitreichenden technischen und nicht-technischen Implikationen verbunden. Da der internationale Softwaremarkt zunehmend homogener wird (Microsofts Windows, Apples iOS, Googles Android), funktionieren Sicherheitslücken eben nicht nur bei den Zielsystemen, sondern in der Regel auch bei vielen oder allen anderen Systemen ähnlicher Konfiguration. Das Finden, Kaufen oder Anmieten solcher Sicherheitslücken gefährdet somit die Allgemeinheit, wenn sie nicht direkt an die betroffenen Hersteller gemeldet werden und ihnen damit die Möglichkeiten gegeben wird, die Lücken zu schließen. Beteiligt sich der BND an der fragwürdigen Praxis des staatlichen Hackens, gefährdet er zugleich die innere Sicherheit Deutschlands, da Parlamente und Behörden, öffentliche Stellen und die Verwaltung hierzulande mit derselben Software arbeiten, deren Sicherheitslücken gehandelt und ausgenutzt werden, anstatt diese Fehler schnellstmöglich zu beheben.

Zusätzlich zu dieser Gefährdung der inneren Sicherheit Deutschlands werden auf diese Weise auch Menschen und Institutionen in anderen Teilen der Welt erheblich gefährdet. Zudem erzeugt der Kauf von Software-Schwachstellen einen steigenden Bedarf in einem grauen globalen Markt, der schon aus Sicherheitsgründen nicht unterstützt werden sollte.

Ohne die Mitwirkung eines Netzbetreibers ist neben einer Manipulation durch eine Infiltration auch noch die Variante bekannt, in das Routing von Netzwerken einzugreifen. Ein Beispiel sind Eingriffe in das BGP-Routing[13], in deren Folge sich der Weg von Datenströmen durch die Netze verändert. Da Manipulationen wie sog. Hijacks und Spoofings im BGP-Protokoll in großem Stil von Netzbetreibern schnell erkannt werden, finden solche manipulativen Operationen oft in sehr kleinem Rahmen statt. Ziel kann dabei beispielsweise sein, das Routing derart zu manipulieren, dass bestimmte Datenströme danach bereits überwachte Routen nehmen.

Praktisch besteht eine Möglichkeit darin, an einem Internet Exchange einen Port für eine Manipulation des Routings zu nutzen: Zunächst wird eine BGP-Session zu dem Netzwerk aufgebaut, welches ausspioniert werden soll. Hier bestehen nur wenig Hürden, da die meisten Netzwerke offen peeren. Über das BGP-Protokoll können dann manipulative Routen annonciert werden. Sofern keine strikten Filter im Einsatz sind, kann eine solche Manipulation erfolgreich sein.

Große Internet Exchanges haben typischerweise mehrere 10.000 BGP-Sessions aus aller Welt mit sehr vielen Providern, die gut überwacht werden, um dadurch

---

[12] Vgl. Rainer Rehak: „Angezapft – Technische Möglichkeiten einer heimlichen Online-Durchsuchung und der Versuch ihrer rechtlichen Bändigung“, MV-Verlag Edition Wissenschaft, 2013, Seite 29ff.

[13] Das Border Gateway Protocol (BGP) ist ein international verbreitetes Routing-Protokoll im Internet.

temporäre absichtliche oder auch unabsichtliche Fehlkonfigurationen zu entdecken. Das führt dazu, dass BGP-Hijacks in großem Rahmen schnell erkannt werden und es daher schwierig ist, damit unentdeckt zu bleiben.

Satellitenüberwachung

In der näheren Zukunft wird die Satellitenkommunikation weiter an Bedeutung gewinnen. Eine rein passive Beobachtung von Teilnehmern und eine Erfassung von Verkehrsdaten ist bei Kommunikation über Satelliten technisch möglich. Die Inhaltsdaten werden nur teilweise verschlüsselt sein, da die dafür nötigen Ressourcen wie Elektrizität und verfügbarer Raum auf Satelliten knapp sind.

Allerdings sind bei der Satellitenkommunikation längst nicht alle Inhalte unverschlüsselt. Die Verschlüsselung der Inhalte wird meistens von den Nutzern selbst erledigt, etwa mit Hilfe von IPSec oder anderen Verschlüsselungslösungen.

Es ist technisch vergleichsweise einfach, die nicht verschlüsselten Inhalte mitzulesen: Benötigt wird lediglich eine Antenne im Umfeld der Bodenstation. Mit „Umfeld“ ist hier nicht unbedingt der Nahbereich gemeint: Es genügen wegen der Breite des Strahlenkegels (Beam-Größe und Ground Footprint) oft 100 bis 1.000 Kilometer. Alternativ ist es technisch möglich, den Datenverkehr im Weltraum mitzulesen, wie es beispielsweise der russische Geheimdienst FSB vollzogen hat.[14]

Neben dem Abgreifen der Inhalte ist bei Satellitenkommunikation auch die Identifikation von Verkehren durch Zeit-Signaturen möglich und heute bereits im Einsatz.

Datenfilterung und -auswertung

Nicht nur wegen der internationalen Struktur der Netze und ihres dynamischen Routings, sondern vor allem wegen des stetig ansteigenden Ausmaßes von Kommunikationsdaten über unsere Lebensgewohnheiten, gewinnt die Vorfilterung für den Grundrechtsschutz der Kommunizierenden an Bedeutung. Die Befugnisse des BND übersteigen alle Arten von anlasslosen massenhaften Datenerfassungen, die bisher gesetzlich erlaubt waren. Auch dass die Metadaten der Telekommunikation nicht nur ohne beschränkende Voraussetzungen erhoben, sondern sechs Monate gespeichert werden dürfen, degradiert diese aussagekräftigen Daten über Personen und ihr Verhalten zu bloßen Nützlichkeiten. Daher sollen die Suchkriterien für das Analysieren von Datenströmen ein entscheidender Faktor zur nachgelagerten Begrenzung der Grundrechtseingriffe sein.

Ein Internet Exchange wie etwa DECIX transportiert immer Mischverkehr, also ist immer auch Ausland-Ausland-Verkehr zu erwarten. Das Problem besteht darin, den Verkehr mit Auslandsbezug zu lokalisieren und dann auszufiltern, um ihn

[14] Mit dem Satellit Olimp-K, vgl. https://space.skyrocket.de/doc_sdat/olimp-k.htm, 27. November 2019.

durchsuchen und speichern zu können. Dies ist eine technisch anspruchsvolle Aufgabe.

Die Suchkriterien für Inhaltsfilter entscheiden darüber, welche Kommunikation festgehalten wird und welche nicht. Dabei arbeiten diese Filter syntaktisch. Um solche Inhalte herausfiltern zu können, die Ausland-Ausland-Kommunikation sind, müssten die Kriterien dafür in der Software abschließend definiert sein. Das muss man jedoch als technisch unlösbar bezeichnen.

Die sichere Filterung nach solchen Kommunikationsverkehren ist fehlerbehaftet und praktisch schlicht nicht hinreichend brauchbar. Gerade Aktivisten und investigativ arbeitende Journalisten und andere Berufsgeheimnisträger nutzen in hohem Maße technologische Hilfsmittel, um ihren Aufenthaltsort zu verschleiern. Sie wären gerade durch den Versuch des Selbstschutzes wesentlich anfälliger für eine fälschliche örtliche Attributierung durch den BND.

Bei der großen Menge an Rohdaten nutzt der BND in der Praxis das sog. Datenfilter-System (DAFIS) mit dem Ziel, damit die ausschließlich ausländische Telekommunikation zu markieren. Auch dieser Versuch der Filterung ist notwendigerweise fehlerbehaftet. Das DAFIS des BND besteht aus einer Kombination von IP-Geolokations-, Typ-, Metadaten- und Inhaltsfilter. Diese Methoden sind jedoch nicht mehr sinnvoll, wenn bei der Kommunikation Verschlüsselung verwendet wird. An einem einfachen Beispiel für die heute gebräuchlichen Messenger wird deutlich, warum die Filter bei verschlüsselten Daten fehlschlagen: Hier sieht der Überwachende lediglich, dass eine Person beispielsweise den Messenger Skype benutzt, jedoch nicht, wer mit wem und wieviel kommuniziert.

Dass ein solcher Filter nicht einwandfrei funktionieren kann, wird auch ersichtlich durch die Tatsache, dass beispielsweise eine E-Mailadresse mit der Domain-Endung „gmail.com“ nicht zweifelsfrei auf eine US-Bürgerin schließen lässt. Auch IP-Adressen lassen sich schwer auf ausreichend genaue Ortsdaten der Kommunikationspartnern abbilden. (Verweis auf unten) Dennoch sind die Filter nicht gänzlich ineffektiv.

Einem Gutachten des Verbands der Internetwirtschaft eco zufolge erreicht die Qualität des Systems DAFIS geschätzte 98,5–99 % korrekte Filterung.[15] Was auf den ersten Blick akzeptabel wirken mag, erweist sich bei den hohen Datenmengen als keineswegs hinreichend: Im Jahr 2016 gab es am DECIX ca. 500.000.000.000 Verbindungen pro Tag. Bei einer Filterqualität von 99,9 % ergeben sich also täglich 500 Millionen falsch zugeordnete Verbindungen. Bei einer Filterqualität von 99,5 % werden sich 2,5 Mrd. Verbindungen pro Tag falsch zugeordnet. Und bei einer Filterqualität von 99,0 % ergeben sich täglich 5,0 Mrd. falsch zugeordnete Verbindungen. Zusätzlich zu diesen immensen Fehlerzahlen und damit Eingriffen in die Grundrechte von Deutschen und Nicht-Deutschen, müssten die Betroffenen darüber informiert werden. Wie jedoch eine Einzelfallprüfung bei potentiell Millionen täglichen Fällen aussehen sollte, bleibt offen.

Bei einer automatisierten Erhebung ist die technische Unmöglichkeit einer brauchbaren Vorfilterung auch deswegen problematisch, da erst eine weitere Datenverwertung und damit eine Durchsicht der Daten die Wahrscheinlichkeit erhöht, die tatsächlich gewünschte (und erlaubte) Kommunikation herauszufiltern.

---

[15] Vgl. Landefeld, Klaus: Die neue Globalisierung – wenn das Inland zum Ausland wird, in: FIfF-Kommunikation 1/2017, Seite 47-50.

Der Spagat, den der Geheimdienst dabei zu leisten hat, besteht darin, dass er ausländische Datenpakete nur dann sicher von inländischen Kommunikationen unterscheiden kann, wenn er sie einer tiefgehenden inhaltlichen Analyse unterzieht. Der Schutz der Grundrechte der Kommunikationsteilnehmer kann also erst dadurch besser sichergestellt werden, dass Inhalte der Kommunikation betrachtet werden. Das jedoch ist bereits der Grundrechtseingriff, der zu vermeiden gewesen wäre.

Der Zugriff auf die Telekommunikationsverkehre ist vor der Filterung potentiell vollständig. Die im Gesetz formulierten Einhegungen (Nennung von Netzen, Filtertechnologien, Suchbegriffe) sind technisch ineffektiv und entfalten daher praktisch kaum eine Schutzwirkung.

IP-Adressen als Filter

Es existieren einige Verfahren, um eine IP-Adresse geographisch zu lokalisieren, also einen zugehörigen Ort zu bestimmen. Verwendung finden dabei beispielsweise kommerzielle Datenbanken, die für eine angegebene IP-Adresse ein sog. Location Mapping anbieten. Geliefert wird eine Geolokation zu einer angegebenen IP-Adresse. Vollständig sind solche Datenbanken aber bei weitem nicht, oft auch nicht ausreichend aktuell, entsprechend fehleranfällig ist das Verfahren. Häufig kommt es nach dem Verkauf von IP-Adressen vor, dass es Wochen oder Monate dauert, bis Geolokations-Datenbanken aktualisiert werden und die Neu-Lokation der IP-Adressen korrekt ausweisen.

Auch die öffentlich verfügbaren Informationen bei sog. whois-Einträgen von Providern oder durch Traceroutes können Anhaltspunkte zur geographischen Position einer IP-Adresse liefern. Keines der Verfahren ist aber ausreichend genau, um in jedem Fall sicher festzustellen, wo sich ein informationstechnisches Gerät mit einer bestimmten IP-Adresse tatsächlich befindet. Oft kann nur eine grobe geographische Region ermittelt werden. Als Geolokator ist eine IP-Adresse daher insgesamt wenig geeignet.

Schutzwirkung von Suchbegriffen

Betrachtet man den § 6 BNDG (Voraussetzungen für die Verarbeitung von Daten) aus dem technischen Blickwinkel, erweist er sich als wenig zielführend: Zur Suche nach relevanten Inhalten sollen danach nur bestimmte Suchbegriffe verwendet werden. Dies hat nach (2) den Zweck, die mit der Datenerhebung in Kommunikationsnetzen einhergehenden Eingriffsmöglichkeiten etwas einzuhegen. So heißt es dazu in (3): „Suchbegriffe, die zur gezielten Erfassung von Einrichtungen der Europäischen Union, von öffentlichen Stellen ihrer Mitgliedstaaten oder von Unionsbürgerinnen oder Unionsbürgern führen, dürfen nur verwendet werden, wenn dies erforderlich ist [...]“.

Bei der Verwendung von jeglichen Suchbegriffen fallen regelmäßig sehr viele Datensätze an, die nicht direkt im Zusammenhang mit der Zielfragestellung stehen, also sogenannter „Beifang“ sind. Besonders die Informationen aus (3) sollten einem erhöhten Schutz unterliegen. Trotz der prinzipiellen immensen Unschärfe von

Suchbegriffen werden jedoch nur jene Suchbegriffe begrenzt, die zur „gezielten Erfassung“ führen. Sind die Daten als „Beifang“ und gerade nicht gezielt erfasst worden, wäre ihre Erfassung unproblematisch. Eine Einschränkung der Suchbegriffe ist bei nicht-gezielter Erfassung völlig unpraktikabel. Ein effektiver Schutz der in (2) genannten Akteure während einer Datenerhebung in Telekommunikationsnetzen ist auf diesem Wege grundsätzlich nicht möglich.

Dies verweist auf das prinzipielle Problem, die Eingriffsintensität solcher Maßnahmen durch Begrenzung von Suchbegriffen zu beschränken. Die Schutzwirkung der Suchbegriffe wird insbesondere dadurch neutralisiert, dass jegliche Filter (inklusive der Suchbegriffe selbst) prinzipbedingt für die Eignungsprüfung nach § 12 BNDG zunächst deaktiviert werden müssen. Oder anders gesagt: Um geeignete Suchbegriffe oder geeignete Telekommunikationsnetze zu bestimmen, ist ein Vollzugriff auf alle Datenströme notwendig.

Ob die zuständigen Stellen die Güte der technischen Filterung mit Selektoren überprüfen könnten, bleibt offen, auch weil die technischen Details der Filterung durch den BND nicht offenliegen. Da der BND potentiell zumindest alle kabelbasierten Kommunikationsverkehre auf deutschem Gebiet anzapfen könnte, entsteht schon aufgrund der potentiellen Menge ein Kontrollengpass.

Besonders vielversprechend aus der Perspektive des BND ist das Überwachen der Anlandungspunkte von Unterseekabeln und von Zugangsleitungen von Internet Service Providern zu Internet Exchanges oder Carrier Neutral Datacenters sowie das Anzapfen grenzüberschreitender Fasern.

Diese Fälle stellen wegen der großen Datenmengen auch jedes Kontrollregime auf eine harte Probe. In Anbetracht der personellen Ausstattung und der Arbeitsweise der Kontrollorgane ist nicht einmal von sinnvollen Stichprobennahmen auszugehen. Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) hat zudem im Rahmen seines 27. Tätigkeitsberichts[16] auf die Schaffung von Sanktionsbefugnissen gegenüber dem BND gedrungen, die bisher nicht bestehen. Denn in der Vergangenheit stellte bei Vorliegen eines Dissenses zwischen dem BfDI und dem BND der Dienst die rechtswidrige Datenverarbeitung in der Regel nicht ein.

Datenweitergabe ins Ausland

Bedenklich sind zudem die Regelungen für die Datenweitergabe an ausländische Geheimdienste. Diese Zusammenarbeit des BND mit ausländischen Diensten bindet sich nach § 14 Abs. 3 BNDG an die Ausland-Ausland-Aufklärung vom Inland aus. Der BND kann ohne faktische Prüfung überwachte Telekommunikation weiterreichen und muss sich nicht um einen angemessenen Grundrechtsschutz nach der Weitergabe kümmern. Auch ob die übergebenen Informationen danach noch an weitere Geheimdienste oder wiederum andere Stellen weitergereicht werden, braucht den BND nicht zu interessieren. Dass etwa auch Geheimdienste in nicht-demokratischen Staaten am Datenkarussell beteiligt sind, wird damit in Kauf genommen.

---

[16] Vgl. 27. Tätigkeitsbericht zum Datenschutz 2017-2018, https://www.bfdi.bund.de/SharedDocs/Publikationen/Taetigkeitsberichte/TB_BfDI/27TB_17_18.html?nn=5217016 vom 8. Mai 2019.

Über den Umfang dieses Datenkarussells ist öffentlich wenig bekannt. Auch das Kanzleramt räumt ein, keinen Überblick über die Kooperationen des BND mit ausländischen Diensten zu haben.[17] Einige Angaben der Bundesregierung machen aber deutlich, dass allein an die NSA Millionen Datensätze pro Monat weitergereicht werden:

> „Die Bundesregierung geht davon aus, dass die in den Medien behauptete Erfassung von ca. 500 Millionen Telekommunikationsdaten pro Monat durch die USA in Deutschland sich durch eine Kooperation zwischen dem Bundesnachrichtendienst (BND) und der NSA erklären lässt."[18]

Da die „Kooperationen mit ausländischen öffentlichen Stellen künftig weiter ausgebaut werden" sollen,[19] wachsen auch die Datenmengen und verschärft sich dieses Problem in Zukunft noch. Nicht durch klare Regeln begrenzte Datenweitergaben und jede Art von automatisiertem Massenaustausch von Inhalts- oder Metadaten mit ausländischen Geheimdiensten ist daher ein künftiges Scheunentor.

Bei gemeinsam mit ausländischen Diensten verwendeten Dateien ist von keiner adäquaten Kontrolle oder von Begrenzungen im Sinne der Grundrechte auszugehen. In § 26 BNDG heißt es dazu: „In die Absichtserklärung ist […] aufzunehmen, dass […] der Bundesnachrichtendienst sich vorbehält, um Auskunft […] zu bitten." In einer nicht-bindenden Absichtserklärung die Möglichkeit einer Bitte aufzunehmen, macht die Unkontrollierbarkeit der übergebenen Informationen augenscheinlich.

Fazit

Der weitaus überwiegende Teil aller Kommunikation ist heute paketvermittelt. Eine sichere Differenzierung in Inländer oder Ausländer dieser paketvermittelten Telekommunikation nach den Endpunkten der informationstechnischen Geräte oder nach den Merkmalen der Kommunikation kann technisch nicht sicher gewährleistet werden. Um mit Hilfe der Inhalte der Kommunikation zu differenzieren, muss daher tief in den Verkehr hineingeschaut werden. Die dafür typischerweise verwendeten Methoden[20] können Details der Kommunikation nur liefern, wenn die Daten nicht verschlüsselt sind.

Es ist zu konstatieren, dass alle rechtlichen und technischen Konstrukte zum Schutz der Grundrechtsträger im Inland (also Filter, Suchworte, Netzdefinitionen) technisch bedingt nur wenig tatsächliche Schutzwirkung entfalten. Die Unterscheidung kann praktisch nicht ausreichend sichergestellt werden. Der Gesetzgeber hat dem BND aus technischer Sicht somit keine echte Einhegung seiner Möglichkeiten vorgeschrieben.

---

[17] Vgl. Antwort der Bundesregierung, BT-Drucksache 18/13518, http://dip21.bundestag.de/dip21/btd/18/135/1813518.pdf vom 6. September 2017.

[18] Antwort der Bundesregierung, BT-Drucksache 17/14560, https://dipbt.bundestag.de/doc/btd/17/145/1714560.pdf vom 14. August 2013, S. 2.

[19] BT-Drucksache 18/904118, https://dip21.bundestag.de/dip21/btd/18/090/1809041.pdf vom 5. Juli 2016, S. 3.

[20] Bei einer sog. Deep Packet Inspection (DPI) werden in Datenpaketen nicht nur Absender- und Empfängeradressen ausgewertet, sondern auch der Inhalt selbst.