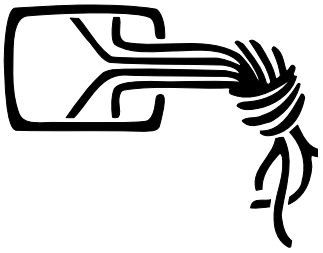


Sachverständigen-Gutachten gemäß Beweisbeschluss SV-13

1. Untersuchungsausschuss (NSA-UA) der 18. Wahlperiode des Deutschen Bundestags

Kay Rechthien

Mitarbeit: Frank Rieger, Constanze Kurz
Freitag, 30. September 2016

Dieses Gutachten behandelt die Darstellung der technischen Gegebenheiten bei der paketvermittelten Übertragung von Telekommunikationsdaten auf der Ebene sogenannter „Autonomer Systeme“ (AS), die in einem globalen „Internet Exchange Point“ (IXP) verbunden sind, einschließlich der technischen Hintergründe und der technischen Entwicklung der IP-Übertragungsverfahren sowie der Darstellung der technischen Beschaffenheit der gemäß § 27 Abs. 2 TKÜV bzw. zur strategischen Überwachung von Ausland-Ausland-Telekommunikationsverkehren auszuleitenden Daten und der Möglichkeiten der regionalen Zuordnung dieser ausgeleiteten Kommunikationsdaten.

Einleitung

Das Internet ist einerseits die Grundlage für moderne Gesellschaften und andererseits das größte Ziel der Abhöranstrengungen von Geheimdiensten. Seine tatsächliche technische Struktur ist von größter Bedeutung für alle Versuche, Internet-Überwachung zu verstehen und gesetzlich zu regulieren. Die noch aus dem längst vergangenen Zeitalter der Leitungsvermittlung stammende Denkweise, die den heutigen Gesetzen und Gepflogenheiten zugrundeliegt, ist mit den tatsächlichen Gegebenheiten weitgehend unvereinbar. In der Praxis ist das Internet ein vielschichtiges, hochdynamisches und komplexes System aus technischen Notwendigkeiten, kommerziellen Vereinbarungen und informellen Übereinkünften, in dem Netzbetreiber verschiedenster Größenordnungen, Internet Exchanges, Diensteanbieter aller Art und Endkunden interagieren. Eine einfache Unterscheidung zwischen inländischem und ausländischem Datenverkehr ist durch die Komplexität der Netzstruktur, die Vielfalt der Dienstemodelle – Stichwort Cloud-Services – und die schnellen Veränderungen von Routing-Pfaden, Netzbelegungen, die enormen Bandbreiten und die vielfache Schachtelung der Datenverkehre auf den Glasfaserleitungen nicht mehr möglich.

Physische Struktur des Netzes – Glasfaserkabel

Das wesentliche Transportmedium für große Mengen Daten, Telefongespräche und Videoströme sind heutzutage Glasfaserkabel. Nur noch auf den letzten Metern zum DSL-Kunden kommen Kupferleitungen zum Einsatz, wie man sie aus der traditionellen Telefonie kennt.

Die Glasfaserkabel im Boden sind in der Regel Bündel von mehreren einzelnen Glasfasern. Während in der Stadt mehrere hundert Paare Glasfaser in einem Kabel laufen, sind es bei Unterseekabeln nur wenige (4 bis 12) Adern. Da Glasfasern vergraben und nicht immer einfach auszutauschen sind und der konstant wachsende Bandbreitenbedarf versorgt werden muss, werden die auf dem Kabel transportierten Dienste auf verschiedenen Ebenen geschachtelt. Dadurch wird das Kabel so effizient wie möglich genutzt.

Auf der untersten Ebene wird diese Schachtelung durch verschiedene Wellenlängen erreicht, die zum Datentransport genutzt werden. Licht wird in der Glasfaser in einem Bereich von 1200 nm und 1700 nm durchgeleitet, also im Bereich des nicht sichtbaren Lichts. Dieser Bereich des Lichtspektrums wird in schmale Wellenlängenbereiche aufgeteilt. Dazu wird das Licht von Dutzenden Lasern, die jeweils auf einer dieser Wellenlängen arbeiten, mit einem Prisma auf einer Faser gebündelt und am anderen Ende mit einem Prisma wieder voneinander getrennt. Das funktioniert genau wie bei einem Strahl Sonnenlicht, der durch ein Prisma zu einem Regenbogen aufgefächert wird. Mit dieser Technik kann man mehrere hundert Kanäle mit jeweils mehreren 100 Gbit/s auf einer Glasfaser bündeln.

Diese Kanäle werden dann an Dritte weitervermietet oder vom Netzbetreiber selbst für eigene Daten genutzt. Auf einer üblichen Glasfaser-Leitung fließen mehrere Terabit an Daten. Aktuell installiert werden Leitungen, auf denen 19,2 TBit/s (das sind 19200 GBit/s) pro Faserpaar transportiert werden. Typischerweise werden einzelne Wellenlängen oder Bündel von Wellenlängen vermietet. Die Mieter dieser Kapazitäten auf der Faser sind typischerweise große Netzwerkanbieter, die diese dann wiederum an ihre Kunden verkaufen.

Auf diesen Leitungen wiederum können hochbandbreitige Dienste wie Internetverkehr laufen oder auch sehr sensible Standleitungen zwischen Industriefirmen, Banken oder Forschungsnetzen. Bis auf diese Ebene schaltet man Verbindungen auf Leitungsbasis mit Punkt-zu-Punkt-Verbindungen, das heißt, das Licht, das an einem Ende der Faser eingeleitet wird, kommt auch am anderen Ende wieder heraus. Diese einzelnen Glasfaser-Leitungen werden dann aber auf Routern, Switchen und anderen Systemen terminiert, die Paketinformationen auf weitere Leitungen zum nächsten Knotenpunkt schicken.

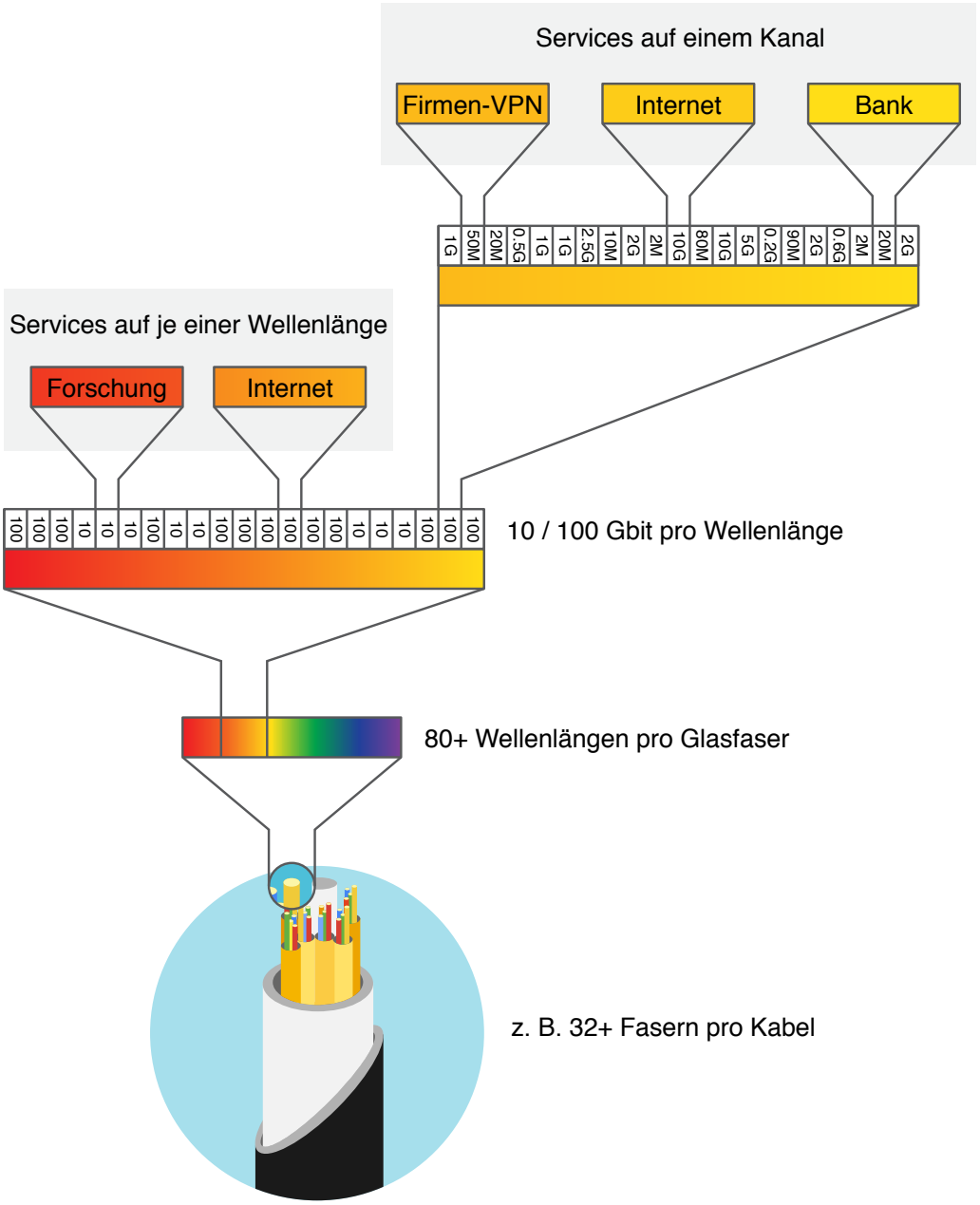


Abbildung 1: Schachtelung verschiedener Dienste auf einer Glasfaser

Da nur wenige Abnehmer – wiederum kleinere Netzwerkanbieter oder große Unternehmen – Kapazitäten in der Größenordnung einer ganzen Wellenlänge benötigen, wird üblicherweise der Verkehr vieler Kunden gebündelt. Von dem eigentlichen

Eigentümer der Glasfaser bis zum Endkunden, etwa einer Firma, die darüber ihre Standorte verbindet, liegen heute etwa zwischen vier und acht Mittelsmänner, die jeweils den Verkehr mehrerer ihrer Kunden auf die von ihnen angemietete Transportkapazität zusammenbündeln.

Dieser Verkehr kann dann beispielweise aus einzelnen verschlüsselten Kanälen zur Vernetzung von Rechenzentren oder Firmenstandorten bis hin zu hochbandbreitigen Verbindungen mit Internetverkehr bestehen. Ebenso können dort auch Verbindungen von Mobilfunkmasten, Energieversorgern und Handelsfirmen laufen. Diese Datenströme werden mit speziellen Kennungen und dem Eingangs- und Ausgangspunkt versehen, um dann über verschiedenste Wege und Medien durch das Netz geschickt zu werden. Diese Verschachtelung kann erneut mehrfach auf verschiedenen Ebenen mit verschiedenen Protokollen geschehen, so dass man auf der obersten Ebene nicht mehr sieht, was auf den darunterliegenden stattfindet.

Das heißt: Hört man eine Glasfaser ab, kann man den Verkehr von vielen Hundert verschiedenen Diensten, Tausenden von Firmen und Millionen Endkunden mitlesen. Um jedoch die Inhalte zu differenzieren, muss man sehr tief in den Verkehr hineinschauen.

Paketvermittlung, Unterschied zu Leitungsvermittlung

Der Verkehr auf den Glasfasern ist heutzutage grundsätzlich paketorientiert. Früher wurden Telefon- und Datenverbindungen als direkte Leitungen zwischen den Kommunikationspartnern realisiert. Vom Telefon des Kunden führte eine Leitung zu einer Vermittlungsstelle, zwischen den Vermittlungsstellen gab es dicke Bündel von Leitungen. Wenn Teilnehmer A einen Anruf zum Teilnehmer B führen wollte, schaltete die Vermittlungsstelle, zu der die Leitung des Anschlusses von A führte, über dieses Leitungsbündel eine Verbindung zur Vermittlungsstelle, die für den Anschluss von B zuständig war, die dann den Anruf zu B durchstellte. Während des Gespräches gab es eine durchgehende elektrische Verbindung zwischen den beiden Teilnehmern.

Bei internationalen Gesprächen waren mehrere Vermittlungsstellen beteiligt. Es gab feste Kabelbündel zwischen Ländern. Wenn ein solches Kabel angezapft wurde, waren darauf die Gespräche zu finden, die zwischen diesen beiden Ländern geführt wurden. Diese Epoche ist allerdings lange vorbei.

Heute ist der weit überwiegende Teil der Kommunikation paketvermittelt. Die Kommunikation aus Nutzersicht, also zwischen zwei Endgeräten, beruht immer auf Paketvermittlung. Dabei werden die Daten – egal ob Internet-Inhalte oder Telefongespräche – in kleine Pakete aufgeteilt.

Die Paketvermittlung im Netz kann man sich etwa vorstellen wie den Päckchentransport bei der Post. Vom Absender werden die Päckchen zum lokalen Paketverteilzentrum transportiert. Dort landen sie auf einem Fließbandsystem. Dieses scannt die Postleitzahl und sortiert die Päckchen in Container für die richtige Transportrichtung. Fängt die Postleitzahl des Empfängers etwa mit einer 8 an, landet das Päckchen in dem Container, der Richtung Bayern geht. Ist die erste Zahl eine 1, geht es Richtung Berlin.

Welchen Weg der Container dann zum nächsten Frachtzentrum nimmt, hängt von einer Reihe von Kriterien ab. Sind viele Pakete in eine Richtung unterwegs, landen die

entsprechenden Container vielleicht auf einem Zug, einem großen Sattelschlepper oder in einem Flugzeug. Welcher Weg eingeschlagen wird, hängt wiederum von der Stau-Lage auf der Straße ab, vom Fahrplan der Bahnstrecke, der Auslastung der Frachtflugzeuge und der einzelnen Verteilzentren und davon, ob es sich um Eilsendungen oder normale Päckchen handelt.

Ist ein Paketzentrum etwa besonders stark ausgelastet, kann auch eine andere Anlage für die weitere Sortierung und den Weitertransport genutzt werden. Durch eine Reihe dieser Paketzentren – man kennt die Namen aus der Sendungsverfolgung von DHL oder UPS – gelangt das Päckchen schließlich zum Ziel. Der Weg der Sendung kann dabei sehr verschieden sein. Ob ein Päckchen von Berlin nach San Francisco den Weg
Berlin - Frankfurt - London - New York - Atlanta - San Francisco
nimmt oder vielleicht die Route
Berlin - Köln - Amsterdam - London - Memphis - Los Angeles - San Francisco
gewählt wird, ist dem Absender und Empfänger letztlich egal, solange es ankommt.

Das Internet funktioniert nach dem gleichen Prinzip. Die Verteilzentren heißen hier „Router“. Sie sind untereinander verbunden und leiten die Datenpakete weiter zu einem Router, der eine kürzere Route zum Ziel verspricht und damit das Paket näher an sein Ziel bringt. Auch hier spielen eine Vielzahl von Kriterien eine Rolle. Die Verbindungen zwischen den Routern können verschieden stark ausgelastet, der Verkehr über einzelne Strecken besonders teuer oder preiswert sein, Strecken oder Router ausfallen.

Diese Faktoren können sich auch noch je nach Richtung des Datenverkehrs unterscheiden, so dass Hin- und Rückrichtung eines Videotelefonats unterschiedliche Wege durch das Netz nehmen. Auch wenn es für die Nutzer nicht bemerkbar ist, werden einzelne Datenübertragungen – etwa ein Film-Stream – nicht selten über verschiedene Wege gleichzeitig transportiert. Dabei können die einzelnen Datenpakete einer Übertragung auch in vom Absenden abweichender Reihenfolge ankommen, weil die verschiedenen Wege, die sie nehmen, unterschiedlich lange dauern. Auf dem Computer des Empfängers werden die Pakete dann wieder in die richtige Reihenfolge gebracht.

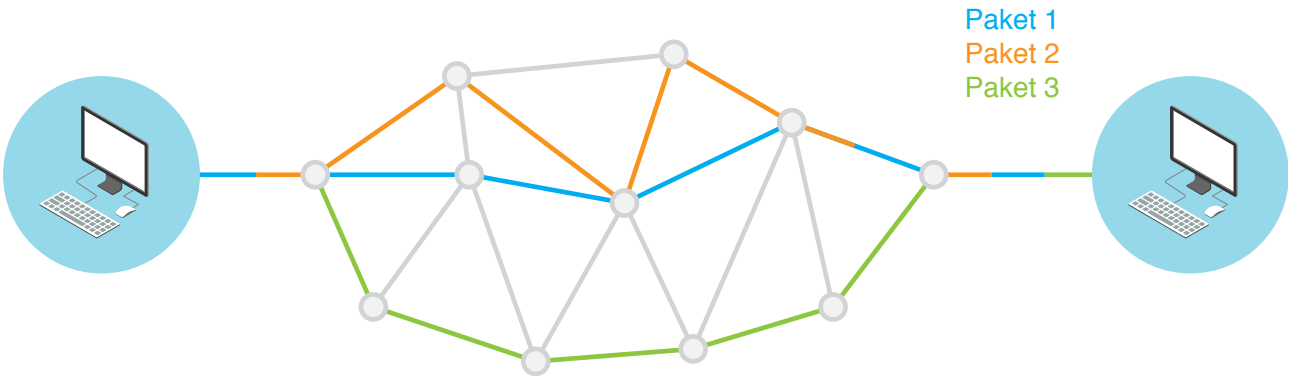


Abbildung 2: Schema Paketvermittlung

Bedingt durch diese Eigenschaften des paketorientierten Datenverkehrs ist es nicht möglich, mit der oben beschriebenen Denkweise der Leitungsvermittlung an das Internet heranzugehen. Welche Datenverkehre sich auf einer bestimmten Leitung zwischen zwei Routern befinden, lässt sich kaum zuverlässig vorhersagen. Der Weg der Pakete zwischen zwei Teilnehmern wird ad hoc und dynamisch bestimmt und kann sich von einem Augenblick zum anderen verändern.

Peering, Transit und Exchanges

Einen wesentlichen Einfluss auf den konkreten Weg eines Datenpaketes hat das sogenannte Peering. Dabei handelt es sich um ein komplexes Netzwerk von Vereinbarungen zwischen den großen Internet-Firmen, über das geregelt wird, wer mit wem an welchem Ort Datenströme austauscht. Das Internet ist – wie der Name schon sagt – ein Netz, das aus der Zusammenschaltung von vielen einzelnen Netzen (Autonomen Systemen, AS) besteht, die jeweils unter der Kontrolle eines einzelnen Anbieters oder eines Anbieterverbundes stehen.

Jedes einzelne Netz und Autonome System trifft die Routing-Entscheidungen eigenständig auf Basis der von seinem Betreiber vorgegebenen Kriterien. An den Punkten, an denen Daten vom Netz eines Anbieters – zum Beispiel der Telekom – in das Netz eines anderen Anbieters – zum Beispiel von Vodafone Kabel Deutschland gelangen, gibt es drei grundsätzliche Arten der Zusammenschaltung: Peering, Transit und Exchanges.

Das sogenannte Peering ist eine feste Verbindung, bei der die beiden Netzanbieter eine direkte Verbindung zwischen ihren Netzen schalten. Diese wird entweder direkt in einem Rechenzentrum geschaltet oder über eine angemietete Verbindung über eine Faser realisiert, auf der sich in der Regel noch eine Fülle anderer Verbindungen (siehe Seite 4, Abbildung 1) befinden. Dieser Weg wird meist gewählt, wenn eine große, relativ absehbare Menge Verkehr zwischen den beiden Anbietern hin- und herfließt.

Dabei setzt sich zunehmend das Konzept durch, dass die Peering-Verbindungen über spezialisierte Anbieter realisiert werden, die keine Endkunden bedienen oder Daten vorhalten, sondern ihrerseits globale Hochbandbreiten-Netze betreiben, auf denen Peering-Kapazität zwischen Providern in ausreichenden Mengen vorhanden sind oder geschaltet werden. Das Netzwerk der Peering-Verbindungen wird dadurch in zunehmendem Maße sehr dynamisch.

Wenn es keine direkte Verbindung zwischen den beiden Netzen gibt oder aus geschäftlichen Gründen nicht erwünscht ist, wird der Datenverkehr oft über sogenannte Transit-Verbindungen geleitet. Dabei mietet meist ein kleinerer Anbieter, der etwa ein Rechenzentrum mit Webservern betreibt, eine bestimmte Transportkapazität über das Netz eines großen Anbieters zu allen anderen Netzen, mit denen der große Anbieter Verbindungen hat – zum Beispiel den verschiedenen Netzen von DSL-Anbietern, deren Kunden auf die Webserver in dem Rechenzentrum zugreifen wollen.

Wie der Transit-Anbieter den Verkehr zwischen dem Rechenzentrum und dem Netzknoten eines DSL-Anbieters routet, also welchen Weg die Daten dann konkret nehmen, darauf haben beide Seiten in der Regel keinen Einfluss. Der Transit-Anbieter optimiert die Datenflüsse anhand eigener Kriterien – meist der Auslastung seiner Leitungen und Router.

Die dritte Möglichkeit der Verbindung zweier Netze sind die sogenannten Internet Exchanges. Die Exchanges sind Anbieter mit neutralen technischen Plattformen, auf denen die Netzanbieter flexibel Verbindungen nach Bedarf zwischen ihren Netzen schalten können. Der Vorteil für den Anbieter ist die Möglichkeit, je nach Bedarf schnell und ohne großen Aufwand neue Verbindungen zu schalten. Der bekannteste Exchange in Deutschland ist das DE-CIX, es gibt aber mehr als ein Dutzend weitere solcher Knotenpunkte.

In der Praxis benutzen die Internet-Anbieter eine Mischung aus allen drei Netz-Zusammenschaltungsformen, wobei der Verkehr je nach Auslastung von Routern und Leitungen, Preisgestaltung der einzelnen Anbieter, technischen Kriterien und geschäftspolitischen Erwägungen optimiert wird. Durch die oben erläuterten Eigenschaften der Paketvermittlung bekommt der Nutzer davon nur in Ausnahmefällen etwas mit – etwa wenn eine Netz-Zusammenschaltung überlastet ist. Welchen Weg sein Film-Stream am Ende genommen hat, ist für ihn schließlich auch irrelevant. Für alle drei Arten der Zusammenschaltung ist nicht vorab absehbar, welchen Weg ein Datenpaket nehmen wird.

Funktionsweise des Routings im Netz

Untereinander kommunizieren die Autonomen Systeme (AS) mit dem Border Gateway Protocol (BGP). Dieses Protokoll wird benutzt, um Routineinformationen auszutauschen. Wenn nun ein Kunde im Netz der Deutschen Telekom, beispielsweise 212.184.123.0/25, zu finden ist, sieht der Eintrag in der Routingtabelle, die alle Möglichkeiten beinhaltet, über welche Router ein Weg eines Datenpaketes von diesem Kunden beispielsweise zum Server des Deutschen Bundestages verlaufen kann, in etwa so aus:

```
BGP routing table entry for 46.243.122.0/24
Best Path: 2914 198913
Other Path: 24989 198913
Community: 2914:410 2914:1201 2914:2202 2914:3200 3320:1276 3320:2010
3320:9020 64512:200 64900:36001 64900:36301
```

Routingtabelleneintrag für den Netzblock in dem www.bundestag.de betrieben wird

Hinter der IP-Adresse 46.243.122.58 im Beispiel ist der Webserver von www.bundestag.de zu finden.

„Best Path“ beschreibt den Pfad, der aktuell genutzt wird. Die Deutsche Telekom (AS3320) gibt die Pakete an den Netzwerk-Anbieter NTT (AS 2914) und NTT leitet diese weiter an Babiel (AS198913), den Hoster von www.bundestag.de.

„Other Path“ ist der alternative, aber derzeit nicht genutzte Pfad, der aus Sicht des Routingprotokolls genauso lang ist, aber aus verschiedensten Gründen als unattraktiver gesehen wird als der Best Path.

„Community“ beschreibt sogenannte BGP Communities. Dies sind Kennzeichnungen an einem Routingtabelleneintrag, um weitere Informationen zu übermitteln oder den Verkehr zu leiten. 2914:410 bedeutet, dass der ISP Babiel, bei dem der Bundestags-Server steht, ein Kunde von NTT ist. 2914:2202 bedeutet, dass Babiel an NTT in Deutschland angeschlossen ist. 3320:9020 bedeutet, dass die Deutsche Telekom die Route von NTT durch ein Peering geschickt bekommt, und 3320:2010 sagt aus, dass es in Europa zusammengeschaltet ist. Die Informationen zur Interpretation dieser Communities sind allerdings nicht zwingend öffentlich.

BGP, das Protokoll, das Netzwerkbetreiber untereinander sprechen, ist ein vektorbasiertes Routingprotokoll, daher zeigt der Pfad „Path“ in der Routingtabelle lediglich die Provider auf, über die das Netz erreichbar ist. Es wird nur festgelegt, dass die Deutsche Telekom das Paket an NTT gibt und NTT es dann an Babiel weiterleitet. Ob NTT das Paket in

Deutschland transportiert oder netzintern die Daten beispielsweise erst nach Amsterdam schickt und dort an die Deutsche Telekom übergibt, lässt sich aus der Routingtabelle nicht ersehen.

Ebensowenig ist es ersichtlich, ob das Paket zwei Router oder zwanzig Router auf dem Weg zwischen Telekom und Babiel passiert. Wieviele Router das Paket tatsächlich passiert, kann man unter bestimmten Umständen anhand von Analyse-Tools wie Traceroute feststellen, allerdings ist hier nur eine Ebene zu sehen. Ob das Paket dedizierte Glasfasern, geteilte Punkt-zu-Punkt-Verbindungen oder Tunnelprotokolle genutzt hat, kann man nicht feststellen. Ebenso ist es nahezu unmöglich, von außen den genauen Weg zu erkennen und zu beschreiben, etwa ob das Paket eine Glasfaser an der Bahntrasse nimmt, vielleicht die Faser neben einer Pipeline zum Transport verwendet wird oder eine angemietete Leitung eines anderen Carriers nimmt.

Ein Internet Exchange wie der DE-CIX ist lediglich eine neutrale Austauschplattform, um mehrere Netzwerkbetreiber zu erreichen. Der Internet Exchange bietet die gemeinsame technische Basis, greift aber nicht in das Routinggeschehen ein und kann es auch nicht beeinflussen. Die Entscheidung, ob und wo Daten ausgetauscht werden, liegt ausschließlich bei den Providern, Carrier und Akteuren, die im globalen Internetverbund BGP miteinander sprechen. Internet Exchanges sind nur eine Möglichkeit dafür, neben direkten Verbindungen und Transit-Carriern.

Methoden der Netzüberwachung

Es gibt eine Reihe von Methoden, den Datenverkehr zu überwachen und herauszufinden, woraus er besteht. Dabei ist die Bandbreite der zu analysierenden Verbindungen der ausschlaggebende Kostenfaktor. Um den gesamten Verkehr zu analysieren, muss man den Datenstrom spiegeln und mit für die entsprechenden Bandbreiten ausgelegten Geräten vorfiltern und dann in der gewünschten Detailtiefe auswerten.

Um tiefere Protokollschichten – wie etwa Absender und Empfänger einer E-Mail – und den Inhalt von Kommunikation zu analysieren und herauszufiltern, nutzt man die sogenannte Deep Packet Inspection (DPI). Da dies eine technisch sehr aufwendige Methode ist und die DPI-Geräte mit derzeit 100 GBit/s pro Port im Vergleich zu den anfallenden Gesamtbandbreiten (bis zu 19200 Gbit/s pro Faserpaar) nur begrenzte Mengen des Verkehr analysieren können, gibt es effizientere Methoden, um zumindest statistisch auszuwerten, was in dem Netz eines Providers transportiert wird.

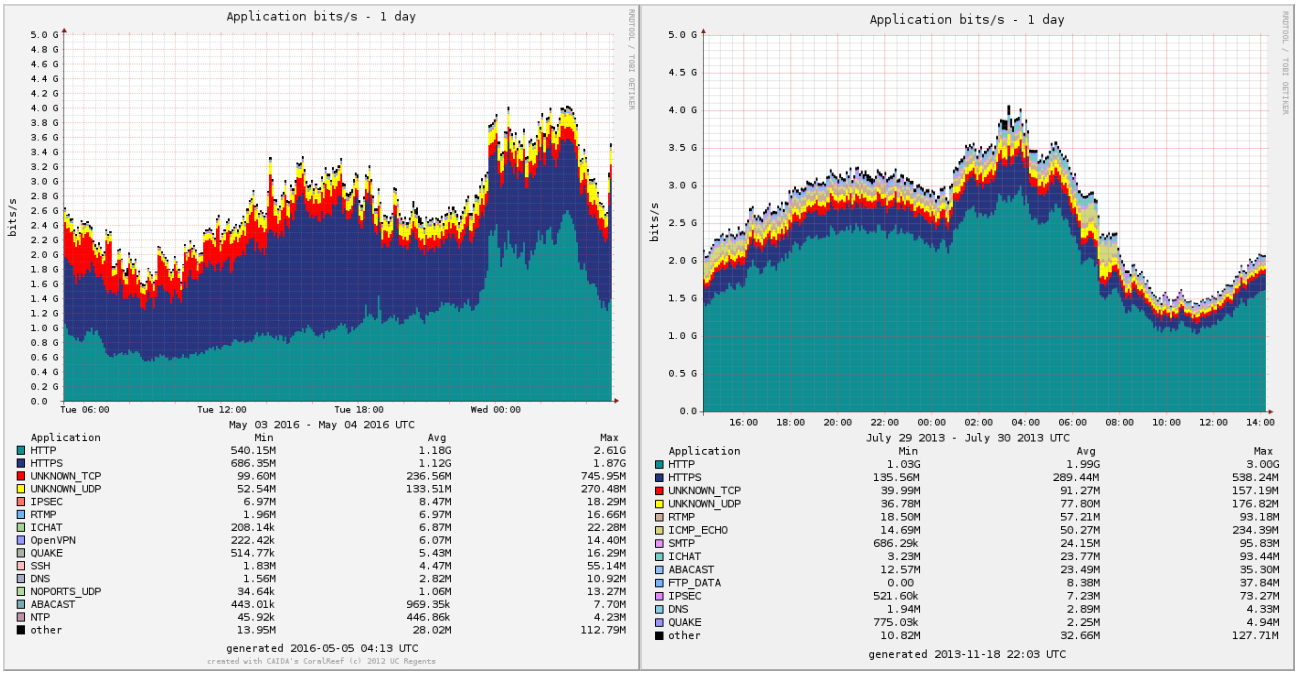
Internet Exchange Points, Carrier, Transit Provider und andere große Netzwerke nutzen zum Betrieb ihres Netzes Techniken wie sFlow, NetFlow oder IPFIX, die man auch unter dem Begriff „Sampling“ kennt. Auch hier werden nicht etwa mehrere Terabit des Verkehrs vollständig analysiert, sondern nur ein Bruchteil der Informationen ausgeleitet. So wird beispielsweise bei sFlow jedes 16.000ste Paket ausgeleitet und davon lediglich der Header. Aus dem Header lässt sich lediglich zuverlässig ersehen, was Absender- und Zieladresse eines Paketes sind und zu welchem Internet-Protokoll es gehört (also etwa https für verschlüsselte Webseiten-Aufrufe).

Auf diese Weise bekommt man einen groben Durchschnitt der Arten des Verkehrs im Backbone, mit Hilfe dessen vor allem Verkehrsoptimierung betrieben wird. Wenn aus der statistischen Durchschnittsanalyse etwa ersichtlich wird, dass auf einer bestimmten

Verbindung viel Verkehr anfällt, der über diesen Routingweg unnötig hohe Kosten verursacht, kann das Routing angepasst werden. Der genaue Inhalt der Pakete wird nicht ausgeleitet, da die Datenmengen dafür zu groß sind. Die Genauigkeit der Analysen hängt von der Sampling-Frequenz ab, aber bildet immer nur einen groben Durchschnitt ab. Verlässliche Aussagen über die An- oder Abwesenheit von bestimmten Quell- oder Zieladressen lassen sich auf diese Weise nur für hochvolumigen Verkehr treffen, da genügend Pakete aus solchen Verbindungen in der Probennahme enthalten sein müssen.

So kann eine Analyse nach bestimmten Mustern durchgeführt werden: Wenn beispielsweise der Datenverkehr auf Port 443 hoch ist, große Pakete enthält und eine der IPs zu einem Hoster gehört, handelt es sich um einen voluminösen Download. Ein anderes Beispiel: Wenn die Quell-IPs einem Access-Netzwerk zugeordnet sind, die Ziel-Adressen Port 1194 enthalten und die IP einem Firmenstandort zugehörig sind, dann kann man daraus interpretieren, dass es sich hierbei um eine OpenVPN-Verbindung eines Mitarbeiters in die Firmenzentrale handelt.

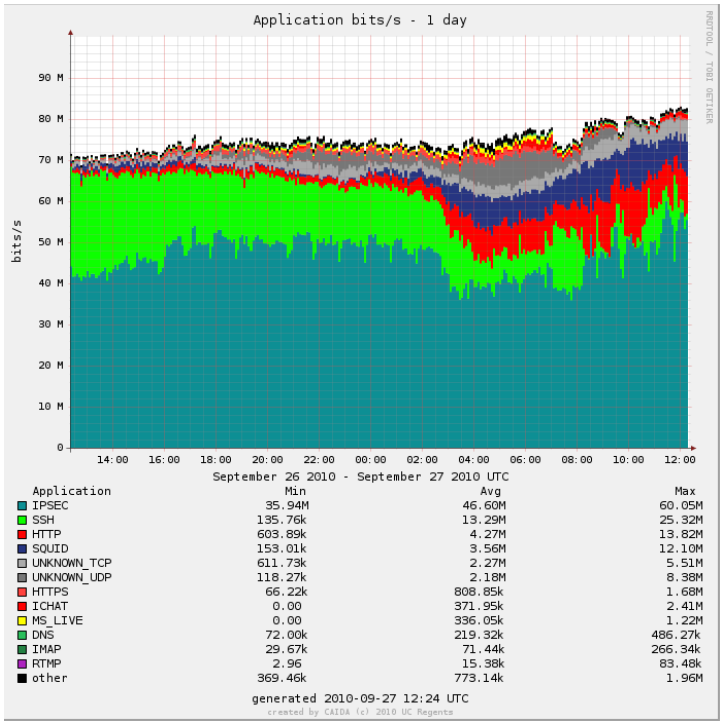
Sowohl durch Sampling als auch durch Deep Packet Inspection kann man Statistiken erstellen, wieviel Verkehr zu welchen Netzwerken fließt oder welche Applikationen genutzt werden. Die Zusammensetzung des Verkehrs ist stark abhängig davon, was für Kunden auf der jeweiligen Verbindung zusammengefasst sind. Sehr gut lässt sich dies aus nach häufigsten Verkehrsarten sortierten Graphen von verschiedenen kleineren Internet Exchanges in den Vereinigten Staaten ersehen:



Die Graphen stammen aus dem öffentlichen Internet-Statistik-Projekt Center for Applied Internet Data Analysis (caida.org).

Wie sich gut ersehen lässt, weist jeder der kleinen Internet Exchanges (die jeweils nur einen Bruchteil der auf einem Faserpaar geschalteten Kapazität vermitteln) eine sehr unterschiedliche Charakteristik auf, die aus den darauf aggregierten Kundenverbindungen resultiert. Diese schwankt auch im Tagesverlauf. Wie sich schon anhand dieses begrenzten Beispiels ersehen lässt, ist es kaum möglich, globale Aussagen über die Zusammensetzung des Internetverkehrs zu machen. Dementsprechend liegen die

öffentlich auffindbaren Statistiken über die Anteile der verschiedenen Verkehre sehr weit auseinander und sind mit größter Vorsicht zu betrachten. Je nachdem, ob die Daten bei Endkunden-ISP, bei kleinen oder großen Internet Exchanges, auf den Backbones von großen Telekommunikationsanbietern oder an anderen Stellen gewonnen wurden, werden sie sehr unterschiedlich ausfallen.



Grundsätzlich lässt sich jedoch feststellen, dass Video-Streams aller Art (z. B. Netflix, Amazon Video, Youtube) und File-Sharing (z. B. Bittorrent) einen signifikanten Teil des Verkehrs im öffentlich sichtbaren Internet ausmachen. Hieraus folgt auch, dass eine Regelung, die die strategische Fernmeldeüberwachung für einen pauschalen prozentualen Anteil des Auslandsverkehrs gestattet, erhebliche Rechtsprobleme aufwirft.

Um feststellen zu können, dass zum Beispiel ein Nutzer eine bestimmte Anzahl Nachrichten mit einem bestimmten Dienst verschickt hat, muss man Deep Packet Inspection verwenden, um die Verkehrsvorgänge im Detail anzuschauen – sofern die Datenströme nicht verschlüsselt sind.

Sampling wird in fast jedem Netzwerk eingesetzt, da es essentiell ist zum Vermeiden von Verstopfungen auf Leitungen. Deep Packet Inspection ist wiederum eher selten, da es eine sehr kostenintensive und zudem rechtlich fragwürdige Technologie ist, um die heutigen Datenmengen auch nur ansatzweise zu analysieren.

Mit aktueller marktüblicher Technik lassen sich pro Faserpaar 19,2 Terabit transportieren. Die Faserbündel, die heute in Europa grenzüberschreitend installiert sind, enthalten üblicherweise mehrere dutzend Faserpaare. Derzeit werden an den beiden größten Exchanges DE-CIX in Frankfurt und AMSIX in Amsterdam etwa jeweils fünf Terabit durchgesetzt. Schon aus dieser Relation lässt sich ableiten, dass der weitaus größte Teil des Datenverkehrs nicht durch die Exchanges fließt, sondern über direkte Peerings zwischen den Netzanbietern abgewickelt wird. In der Tendenz wird zukünftig der Anteil der Exchanges am Datenverkehrsaufkommen weiterhin abnehmen.

Die gezielte Ausleitung einer bestimmten Netz-Verbindung aus Datenströmen in Terabit-Größenordnung ist sehr aufwendig und nur in einem mehrstufigen Verfahren möglich. Heute verfügbare Hardware für die tiefere Analyse ist in der Regel für Bandbreiten von 100 Gbit pro Schnittstelle ausgelegt, also etwa einem Zweihundertstel der auf einem Faserpaar transportierbaren Bandbreite. Um eine 19,2-Tbit/s-Faser vollständig zu überwachen, müssten etwa zweihundert dieser Systeme installiert werden.

Hinzu kommt, dass es nicht garantiert ist, das eine Kommunikationsbeziehung die gleichen Hin- und Rückwege nimmt. Aus Routing- und Netzwerksicht ist jede dieser Kommunikationsbeziehungen eine Kombination aus Quell- und Ziel-IP bzw. -Port. So können z. B. Messenger einen Kommunikationskanal aufbauen, dessen Hinweg über Frankfurt und der Rückweg über Amsterdam läuft, aber auch mehrere Verbindungen zur besseren Verteilung der Datenmengen auf verschiedenen Verbindungen in verschiedene Rechenzentren aufbauen. Somit ist es aufwendig, komplette Kommunikationsvorgänge auszuwerten, wenn man nicht direkt an der Quelle analysiert.

Es ist aufgrund dieser technischen Komplexitäten davon auszugehen, dass sich geheimdienstliche Anzapfung nicht auf den gesamten Verkehr eines Exchanges bezieht oder nur in Ausnahmefällen versucht, hochbandbreitige Verbindungen auf dem Festland anzuzapfen, sondern sich typischerweise auf folgende Aspekte in der Netzwerk-Struktur konzentriert:

1. Anlandestationen von Unterseekabeln,
2. andere grenzüberschreitende Fasern mit vergleichsweise geringer Bandbreite,
3. Zugangsleitungen von Internet Service Providern zu Exchanges bzw. Carrier Neutral Datacenters,
4. Spiegelung von einzelnen Kunden-Ports auf den Routern in Exchanges,
5. Ausleitung der Verkehre einzelner (Transit-)Kunden unter Mithilfe des Internet Service Providers,
6. Ausleitung des Verkehrs nahe am Ziel (Endkunde, Firma etc.),
7. Manipulation des Routings für das Ziel-Netzsegment.

Manipulation von Routingwegen

Durch die sehr dynamische Natur der Aushandlung und Festlegung des Datenroutings ergeben sich für einen Angreifer diverse Möglichkeiten der Manipulation. Auf der Ebene der physischen Infrastruktur – also der Fasern und des Routings – ist es bei genauer Kenntnis der Redundanz-Vorkehrungen der Provider möglich, durch gezielte Sabotage eine Änderung des Weges zu erzwingen, den der Datenverkehr zwischen zwei Endpunkten nimmt. Wird etwa eine Faser unterbrochen, greifen automatische Mechanismen, die den Verkehr über eine alternative Strecke leiten.

Dabei kommen verschiedene Strategien zum Einsatz, typischerweise entweder redundante Leitungen über zwei geographisch verschiedene Strecken oder Umleitungen auf Routing-Ebene, die etwa beim Ausfall der Strecke Hamburg-Frankfurt die Daten via Hamburg-Düsseldorf-Frankfurt leiten. Auf diese Weise kann ein Angreifer zumindest kurzfristig erreichen, dass Daten über Leitungen oder Router fließen, die er angezapft hat. Gleiches gilt für die Sabotage von Router-Standorten, etwa durch einen gezielten Stromausfall.

Auf logischer Ebene kann ein Angreifer das Routing einzelner Netze durch Annoncieren von Routen manipulieren, die über von ihm kontrollierte Infrastruktur gehen. Der einfachste Weg dazu ist es, eine spezifischere Route für das anzugreifende Netz zu publizieren. Dazu gibt der Angreifer für das anzugreifende Teilstück eines Netzes eine genauere Routing-Regel vor. Diese Regel wird dann bevorzugt und der Verkehr von und zu diesem Netzsegment über ihn geleitet. Solange es sich dabei um relativ kleine, nicht besonders aktiv gemanagte Netzsegmente handelt und darüber nicht auffällig große Mengen Verkehr gehen, können solche manipulativen Umleitungen durchaus lange unbemerkt bleiben. Auffällig werden manipulative oder auch durch Fehler verursachte Routinganomalien in der Regel erst dann, wenn darüber größere Mengen Verkehr gehen oder es zu Funktionseinschränkungen kommt.

Die Filter gegen BGP-Redirection bzw. -Hijacking sind zwar vorhanden, aber nicht weitverbreitet. Die größten Provider im Netz annoncieren weit über 100.000 Routen. Korrekt verwaltete Filterlisten, die sicherstellen, dass Veränderungen an diesen Routen nur von dazu Berechtigten – also den wirklich zuständigen Systemen – vorgenommen werden, haben das vier- bis fünffache Volumen der eigentlichen Routing-Tabelle. Dadurch überschreiten diese Filterlisten oftmals das Verarbeitungsvermögen der Router.

Geolokationstechniken

Es gibt mehrere Methoden, eine IP-Adresse zu lokalisieren, also eine zugehörige geographische Position zu bestimmen. Es gibt kommerzielle Datenbanken, die für eine IP-Adresse ein sogenanntes Location Mapping anbieten. Man kann die geographische Position aber auch selbst durch Triangulierung berechnen oder sich auf die öffentlich verfügbaren Informationen wie whois-Einträge von Providern oder Hostnamen im Traceroute verlassen. Keine der Methoden ist aber genau genug, um sicher festzustellen, wo sich eine IP-Adresse wirklich befindet.

Kommerzielle Datenbanken sind oft veraltet und ungenau. So kann eine IP-Adresse, die seit Monaten in Berlin genutzt wird, immer noch einem anderen Provider zugeordnet sein, der sich beispielsweise im Ausland befindet.

Eine Triangulierung auf Latenzbasis kann in Echtzeit durchgeführt werden, ist aber sehr anfällig für äußere Einflüsse. So können beispielsweise Verkehrsbelastungen in Weitverkehrsnetzen dazu führen, dass Abweichungen oder Ungenauigkeiten entstehen. Diese Ungenauigkeiten können dazu führen, dass eine geographische Abweichung von mehreren hundert Kilometern entsteht. Eine genaue Geolokation durch Latenz-Triangulierung ist lediglich unter Laborbedingungen möglich, um den gewollten Detailgrad zu erreichen.

Anhand der Einträge in der Routingtabelle, Registrierungs-Datenbanken (RIPE etc.) und Traceroutes kann man auslesen, wo ein Netz genutzt wird, sofern der Verwalter das Netzes es transparent dokumentiert. Wenn nun aber – was nicht selten vorkommt – ein multinationaler Konzern mit Tochterunternehmen in mehreren Ländern IP-Adress-Blöcke tauscht, dann können diese Einträge schnell irreführend werden.

Über Traceroutes kann man ebenso das Ziel einer groben Region zuordnen, wenn beispielsweise im Eintrag ein Stadtname auftaucht. Da diese Methoden auch für die Fehlerbehebung von den Netz-Betreibern verwendet wird, sind diese Daten oft am aktuellsten. Das folgende Beispiel illustriert einen solchen Traceroute, der zumindest eine Städte-genaue Routingpfadverfolgung ermöglicht:

```
 1  M-EA1.M.DE.net.DTAG.DE (194.25.0.209)  2.460 ms  2.455 ms  2.451 ms
 2  d-ed1-i.D.DE.NET.DTAG.DE (62.154.15.198)  11.702ms  11.701ms 10.853 ms
 3  80.150.171.254 (80.150.171.254)  11.717 ms  11.951 ms  11.952 ms
 4  xe0-0-0.irt1.dus53.de.as13237.net (217.71.96.30)  11.085 ms  11.085 ms  11.083 ms
 5  xe0-2-0.irt1.han87.de.as13237.net (217.71.96.77)  15.428 ms  15.433 ms  15.431 ms
 6  xe0-2-0.irt1.ber02.de.as13237.net (217.71.96.153)  20.585 ms  20.587 ms  20.566 ms
```

Traceroute von der Deutschen Telekom in München zu euNetworks in Berlin

Das Beispiel zweigt den Weg München - Düsseldorf - Hannover - Berlin, wo die Übergabe von der Deutschen Telekom an euNetworks in Düsseldorf stattfindet.

All diese Methoden funktionieren aber nur, wenn es sich dabei um öffentlich erreichbare IP-Netzwerke handelt, die Hostnamen aussagefähig sind und keine Filter implementiert wurden. Wenn innerhalb des ISPs Methoden zur Verkehrsleitung wie Multiprotocol Label Switching (MPLS) implementiert sind und die Hostnamen keine aussagekräftigen Beschreibungen enthalten, lassen sich praktisch keine verwertbaren Aussagen mehr über den Routingpfad oder die Geolokation von Start- und Zieladresssen treffen.

```
 2  ip5886cb20.dynamic.kabel-deutschland.de (88.134.203.32) 32.419 ms 23.373 ms 23.654 ms
 3  ip5886caee.dynamic.kabel-deutschland.de (88.134.202.238) 22.671ms 23.468ms 27.019 ms
 4  ip5886ca2b.dynamic.kabel-deutschland.de (88.134.202.43)  23.100ms 23.926 ms 22.787 ms
 5  72.14.209.54 (72.14.209.54)  30.410 ms  39.694 ms  30.432 ms
 6  216.239.56.186 (216.239.56.186)  22.874 ms  22.488 ms  23.827 ms
 7  216.239.57.188 (216.239.57.188)  60.904 ms 23.662 ms  22.548 ms
     MPLS Label=576043 CoS=4 TTL=1 S=1
 8  209.85.253.216 (209.85.253.216)  26.281 ms 34.933 ms 40.362 ms
     MPLS Label=358763 CoS=4 TTL=1 S=1
 9  108.170.234.127 (108.170.234.127)  30.083 ms 30.858 ms 31.829 ms
     MPLS Label=564796 CoS=4 TTL=1 S=1
10  209.85.243.65 (209.85.243.65)  28.100 ms 34.083 ms 29.716 ms
```

Traceroute von einem Kabel-Deutschland-Anschluss in Berlin zum Google-DNS-Server (8.8.8.8)

Wenn man nun versucht, einen Rechner in einem privaten Firmennetzwerk mit internationalen Standorten zu lokalisieren, braucht man direkten Zugang zu diesen Netzen. Um genau festzustellen, wo eine IP-Adresse benutzt wird, benötigt man Zugriff auf aktuelle, vollständige Dokumentation und die Daten aus dem Netzbetrieb von den jeweiligen Netzwerken, beispielsweise Roaming-Informationen vom Mobilfunk, IP-Zuteilungen und Endkundenzuordnung in Access-Netzen.

Alle oben erläuterten Mechanismen und Methoden gelten im Grundsatz auch für IPv6. Es ergeben sich durch die zukünftige Umstellung auf IPv6 keine gravierenden Besonderheiten oder Erleichterungen für einen Abhörenden.