



CH-3086 Zimmerwald

Robert Flück, Chef Cyber und elektromagnetische Aktionen, Kdo Cy

**Per Kurier/
persönlich**

Bundesverwaltungsgericht
Abteilung I
Herr Instruktionsrichter
Alexander Misic
Postfach
CH-9023 St. Gallen

Referenz/Aktenzeichen: A-6444/2020
Ihr Zeichen: mia/kob
Unser Zeichen: -
Sachbearbeiter/in: PUNI, TIFF
Zimmerwald, 8. März 2024

Stellungnahme

in der Sache

Digitale Gesellschaft, 4000 Basel

**Beschwerdefüh-
rende 1**

Beschwerdeführer 2

Beschwerdeführer 3

**Beschwerdefüh-
rende 4**

**Beschwerdefüh-
rende 5**

Beschwerdeführer 6

Beschwerdeführer 7

alle zusammen **Beschwerdeführende**

alle vertreten durch lic. iur. Viktor Györfy, Rechtsanwalt, Peyrot, Schlegel und Györfy Rechtsanwälte, Beethovenstrasse 47, 8002 Zürich

gegen

den **Nachrichtendienst des Bundes NDB**, Papiermühlestrasse 20, 3003 Bern

NDB oder Vorinstanz

betreffend

Funk- und Kabelaufklärung

Sehr geehrter Herr Instruktionsrichter Misić

Sehr geehrte Damen Bundesverwaltungsrichterinnen und Herren Bundesverwaltungsrichter

In rubrizierte Angelegenheit bedankt sich der Dienst Cyber und elektromagnetische Aktionen für die Möglichkeit zur Stellungnahme zur Verfügung vom 8. Februar 2024.

I. Formelles

A. Frist (ad Ziff. 2)

1. Mit Verfügung vom 8. Februar 2024 hat das Bundesverwaltungsgericht dem CEA Frist erteilt bis am 12. März 2024 eine Stellungnahme zur Stellungnahme der Beschwerdeführenden vom 20. September 2023 einzureichen.
2. Die vorliegende Eingabe erfolgt daher frist- und formgerecht.

B. Klassifikation der Eingaben (ad Ziff. 3)

3. Die nachfolgende CEA Stellungnahme zur Stellungnahme der Beschwerdeführenden vom 20. September 2023 ist parteiöffentlich.
4. An das Gericht richtet der CEA sämtliche zusätzlichen Unterlagen wie interne Richtlinien vollständig, wobei es sich um als VERTRAULICH klassifizierte Dokumente gem. Art. 4 ff. der Verordnung vom 4. Juli 2017 über den Schutz von Informationen des Bundes (Informationsschutzverordnung, ISchV; SR 510.411) handelt (Beilagen 1-4). Diese Beilagen sind nicht parteiöffentlich.

II. Materielles

Die nachfolgenden Ausführungen beziehen sich auf der Stellungnahme der Beschwerdeführenden 20. September 2023 in der Sache A-6444/2020.

Der CEA wurde aufgefordert im Rahmen seiner Stellungnahme einlässlich und unter Angabe technischer Gegebenheiten zu dem Vorbringen der Beschwerdeführenden insbesondere gemäss den Ziffn. 25, 28, 40, 42f., 62-69, 75 und 78 der Stellungnahme vom 20. September 2023 zu äussern. Dabei soll der CEA insbesondere auf die Funktionsweise und die Eigenheiten des Internets sowie der Übertragung von Signalen über leitungsgebundenen Netzen (zwischen den verschiedenen Anbietern von Telekommunikationsdienstleistungen, nachfolgend FDA) eingehen.

Mit der nachfolgenden Stellungnahme kommt der CEA gerne dieser Aufforderung nach. Es werden zuerst grundlegende Element wie IP-Protokoll, Routing, optische Signale und OSI Layer vorgestellt.

- IP-Protokoll: Internet Protokoll. Vorherrschendes Transportprotokoll für Daten im Internet.
- Routing: Wegfindungsprozess der IP-Protokolle.
- Optische Signale: Signale, die mit Laser über Glasfasern übertragen werden.
- OSI Layer: Open System Interconnection Layer. Eine schematische Darstellung von Kommunikationsprotokollen.

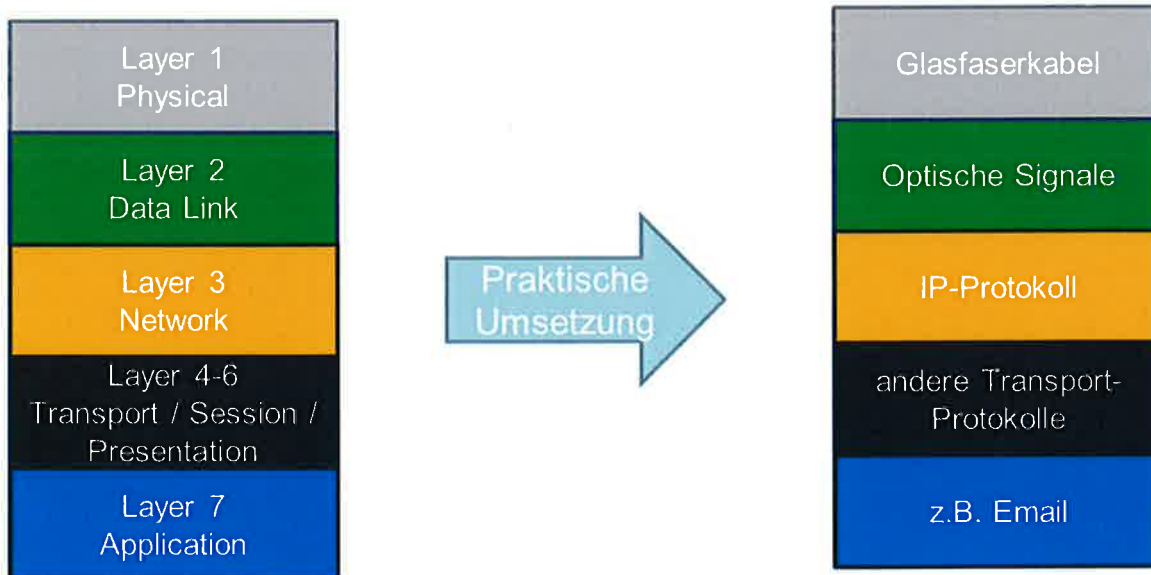


Abbildung 1: OSI Protokoll Stack und praktische Umsetzung

1. Zu Ziff. 25:

Der Dienst CEA definiert die Via-Kommunikation wie folgt: Eine Kommunikation zwischen zwei Schweizer Parteien über einen ausländischen Server, die aus zwei Kommunikationen besteht:

1. Die Senderpartei¹ sendet eine Kommunikation an einen Server im Ausland.
2. Der Server im Ausland sendet die Kommunikation an den Empfänger in der Schweiz.

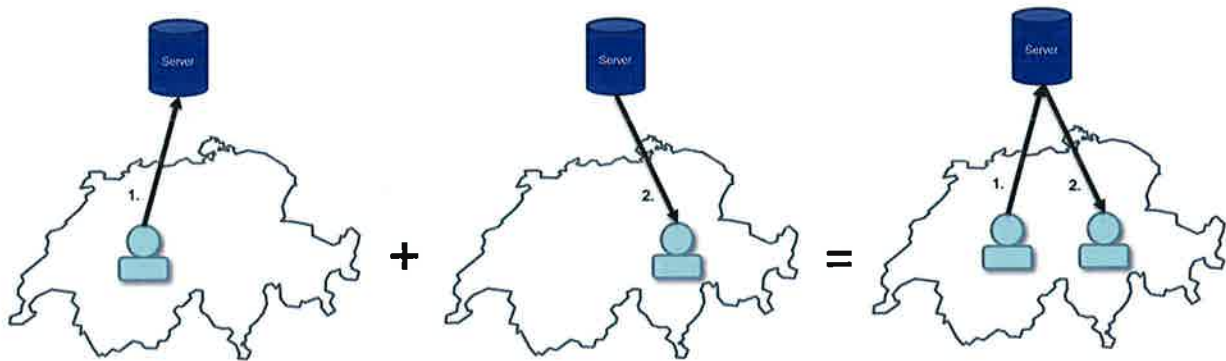


Abbildung 2: Via-Kommunikation.

Zu beachten ist, dass beide Kommunikationen grenzüberschreitend sind, auch wenn der Sender und der Empfänger sich in der Schweiz befinden. Die Erfassung der Signale erfolgt in diesem Fall aufgrund eines Auftrags des NDB², der durch das BVGer bewilligt und von der C VBS freigegeben wurde. Die Kommunikationen finden auf einer grenzüberschreitenden Verbindung statt, die wir berechtigterweise in der Erfassung haben.

Der CEA sieht im Fall der ersten Kommunikation eine komplette Nachricht von der Schweiz ins Ausland (sprich: Schweizer IP-Adresse zu ausländischer IP-Adresse), und im zweiten Fall eine Kommunikation mit kompletter Nachricht vom Ausland in die Schweiz (sprich: ausländische IP-Adresse zu Schweizer IP-Adresse). Auf IP-Ebene (Layer 3 OSI-Modell) sind diese Kommunikationen demzufolge grenzüberschreitend. Zu erkennen, dass es sich bei dieser Kommunikation um eine CH-CH Kommunikation handelt, ist bei einer Erfassung auf IP-Ebene (Layer 3 im OSI-Modell) technisch nicht möglich.

Bei der ersten technischen Analyse der Nachricht (Layer 7 OSI-Modell) wird aufgrund von weiteren Merkmalen (z.B. «ch»-Endung, Schweizer Telefonnummer, Schweizer IBAN, Schweizer Adresse., etc.) erkannt, dass es sich hier um eine Kommunikation zwischen zwei schweizerischen Telekommunikationsteilnehmern handelt. Sie wird im Auswertesystem entsprechend markiert und für eine weitere Analyse gesperrt.

Auch wenn die Beschwerdeführerin dieses Beispiel der Via-Kommunikation als «kein Sonderfall» aufführt, entspricht es nicht den Beobachtungen des CEA. Solche Via-Kommunikationen kommen zwar vor, sind aber weit seltener als von der Beschwerdeführerin behauptet.

¹ Der Absender der E-Mail keine Kontrolle darüber, wie die E-Mail geroutet wird. Die technische Infrastruktur seines Providers (nachfolgend FDA) entscheidet hierüber.

² Aber nicht, weil der Absender oder der Empfänger Suchbegriffe des NDB wären. Schweizerische Suchbegriffe sind gem. Art. 39 Abs. 3 NDG nicht zulässig.

2. Zu Ziff. 28:

Eine Via-Kommunikation kann erkannt werden, sobald diese einmal die Schweizer Grenze überschreitet.

Auch wenn der CEA nur eine Richtung der Kommunikation erfasst hat, ist durch die Erkennung auf Layer 7 des OSI-Modells eine Klassifizierung der Kommunikation als «schweizerisch» möglich. Es müssen somit nicht beide Kommunikationsvorgänge erfasst werden, um einen Schweizbezug auf OSI Layer 7 festzustellen. Eine «überwiegende Anzahl» von Via-Kommunikationen konnte der CEA bei den erfassten Signalen bislang nicht feststellen, da diese im modernen Internet seltener sind, als von der Beschwerdeführerin behauptet wird. Wir verweisen hier explizit auf unseren Schlussbemerkungen zum Internet-Caching und CDNs.

Die Schweiz hat nicht eine unendliche Anzahl von FDA, die wiederum nicht über eine unendliche Anzahl von grenzüberschreitenden Verbindungen verfügen. Die Vorstellung, dass ein IP-Paket «viele Wege» ins Ausland nehmen kann, steht im Gegensatz zu den wirtschaftlichen Zielen der FDA (Peering), der technischen Machbarkeit (verfügbare Dark Fibers), der Latenz der Kommunikation (Geschwindigkeit) und dem Routingverhalten des Internets (BGP/OSPF).

Aus diesen Gründen entspricht es nicht der Erfahrung des CEA, dass es «viele Wege» gibt, die grenzüberschreitend sind. Der grenzüberschreitende Verkehr konzentriert sich auf eine überschaubare Anzahl nationaler und internationaler FDA.

3. Zu Ziff. 40:

Wie unter Punkt 2. beschrieben, wird der grenzüberschreitende Verkehr über eine endliche Anzahl nationaler und internationaler Provider geführt. Jeder dieser FDA/ Provider hat aufgrund von logischen und physikalischen Gegebenheiten eine bestimmte Anzahl Leitungen, die klar grenzüberschreitend sind (z.B. von Zürich nach Frankfurt). Diese können beispielweise Peerings mit ausländischen Providern (z.B. Deutsche Telecom) oder Mietleitungen sein, die beispielsweise den Schweizer Provider an den grössten Internet-Exchange der Welt anbinden (DE-CIX Frankfurt).

Solche Leitungen haben ihr logisches Ziel im Ausland und sind somit grenzüberschreitend und gut identifizierbar. Diese Leitungen ins Ausland sind zielgerichtet auswählbar. Die bisher gemachten Erfahrungen des CEA bestätigen dies.

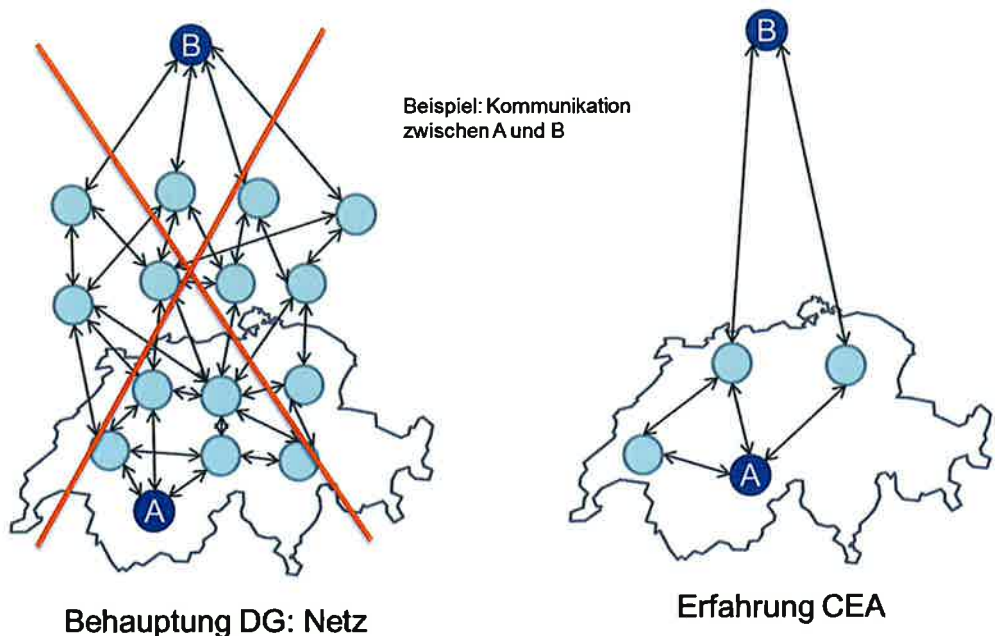


Abbildung 3: Erfahrung CEA

Die Beschwerdeführerin zeichnet ein Bild von unendlich vielen möglichen Leitungen, undurchschaubaren Verbindungen, Ineffizienz und Unklarheit. Aufgrund der gemachten Erfahrungen und der gelebten Praxis kann der CEA diese Behauptung nicht bestätigen.

4. Zu Ziff. 42 und 43:

Grenzüberschreitende Verbindungen enthalten mehr oder weniger Informationen, die für einen bestimmten Kabelauflösungsauftrag relevant sein können. In der Praxis gelingt es dem CEA die Verbindungen mit höherer Relevanz auszuwählen. Die Auswahl wird aufgrund verschiedener Kriterien getroffen. Die wichtigsten Kriterien sind insbesondere die geographische Lage des Endpunkts des Kabels, die dort vorhandenen weitergehenden Verbindungen oder die Art der Dienstleistung des FDA. Es gibt selbstverständlich keine 100% Garantie, dass ein IP-Paket einen bestimmten Weg wählt, aber aus Effizienz- und wirtschaftlichen Gründen werden gewisse Verbindungen mit sehr hoher Wahrscheinlichkeit ausgewählt. Zum Beispiel: Ein Paket von Europa nach Asien nimmt in der Regel den Weg über Tiefseeverbindungen via Ägypten-Indien-Hongkong, anstatt einen Umweg über die USA zu machen. Es gibt deshalb eine Effizienz und Zielgerichtetheit bei dem Weg, der die Datenpakete wählen und dadurch auch eine Effizienz und Zielgerichtetheit bei der Auswahl der Signale und Leitungen.

Aufgrund der gemachten Erfahrungen des CEA nimmt ein IP-Paket immer den «kürzesten Weg». Damit ist nicht unbedingt die physikalische Distanz gemeint, sondern auch die logische Distanz zwischen zwei Netzwerken. Der «kürzeste Weg» wird durch wirtschaftliche Überlegungen der FDA (Peering), die technische Machbarkeit (verfügbare Dark Fibers), die Latenz der Kommunikation (Geschwindigkeit) und dem Routingverhalten des Internets (BGP/OSPF) bestimmt. Der Behauptung der Beschwerdeführerin, es gäbe eine unklare Vernetzung zwischen dem «Schweizer Internet» und dem Rest des Internets, muss der CEA klar widersprechen.

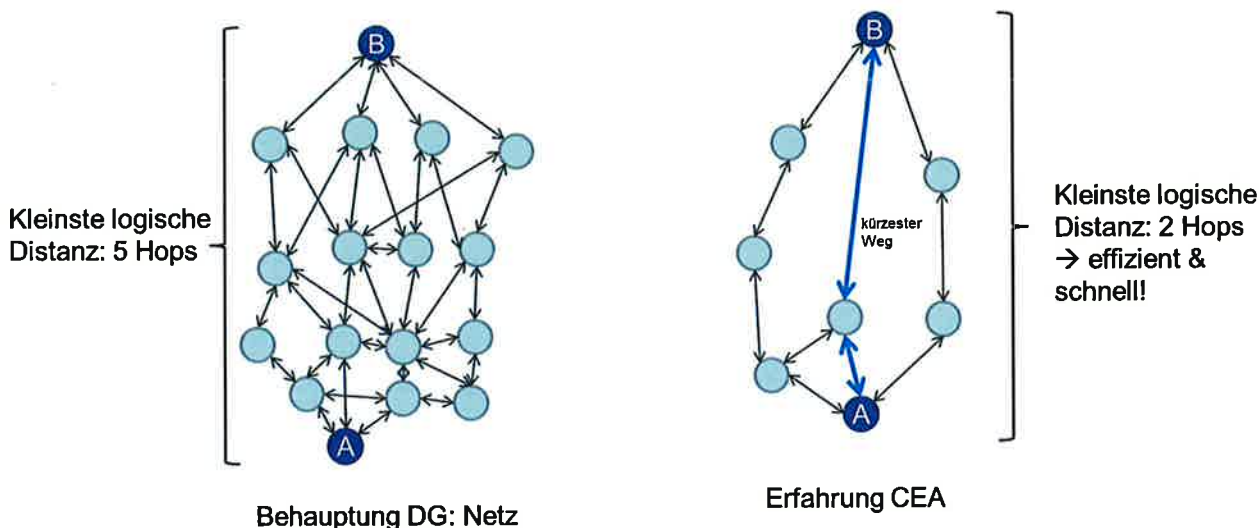


Abbildung 4: Netzeffizienz

Wie schon unter Punkt 3. erläutert, gibt es eine endliche Anzahl an grenzüberschreitenden Signalen, die die Schweiz mit dem Ausland verbinden. Es ist aus wirtschaftlichen und technischen Gründen beschwerlich, eine Glasfaser z.B. von Zürich nach Frankfurt zu legen. Erstens ist die Infrastruktur für Langstreckenübertragungen sehr teuer und zweitens müssen viele bauliche Schritte getätigt werden, um eine Glasfaser über eine derart grosse Distanz zu legen.

Aus diesem Grund greifen nationale und internationale FDA auf grosse bestehende und etablierte internationale Transportdienstleister zurück, die dann in ihrem Auftrag die Signale grenzüberschreitend transportieren. Auf diesen internationalen Glasfasern befindet sich der Verkehr zwischen dem Schweizer Internet und dem Rest der Welt. Eine Ausleitung der grenzüberschreitenden Signale kann somit effizient und zielgerichtet erfolgen.

Ein IP-Paket mit dem Ziel im Ausland (z.B. Frankfurt) hat also aus technischen und wirtschaftlichen Gründen nicht eine «unendliche» Anzahl möglicher Wege, um das Ziel zu erreichen, sondern wird früher oder später über eine Leitung eines internationalen FDA den Weg ins Ausland finden. Dabei ist es nicht relevant, ob das IP-Paket in Zürich, Genf oder anderswo in der Schweiz an den internationalen Dienstleister nach Frankfurt übergeben wurde – auf der Kabelfaser zwischen der Schweiz und Frankfurt wird es vorkommen.

Das Netzchaos mit unendlich vielen grenzüberschreitenden Leitungen, wie die Beschwerdeführerin regelmässig in ihren Aussagen wiederholt behauptet, findet der CEA in der Praxis auf dem Internet nicht wieder.

Unsere Erfahrungen aus der Praxis zeigen:

- die grenzüberschreitenden Signale sind klar auffindbar und beschränkt in der Anzahl.
- die IP-Pakete nehmen - aus wirtschaftlichen und technischen Gründen - den logisch kürzesten Weg. Die einzige Ausnahme hierzu bildet ein Ausfall im Netz, der durch eine kurzfristige Umleitung der Signale umgangen wird. Diese Art von grossen Ausfällen beobachtet der CEA aber sehr selten; sie werden oft innert Minuten wieder behoben.

Der CEA beobachtet in diesem Zusammenhang kein derart dynamisches Netz, wie die Beschwerdeführerin es behauptet. Es ist möglich, dass das «Schweizer Internet» mit mehr Ausfällen zu kämpfen hat, aber auf den internationalen Leitungen ist das in der Praxis nicht beobachtbar.

5. Zu Ziff. 62:

Betreffend Effektivität und Zielgerichtetheit der Massnahme verweisen wir auf die obigen Ausführungen der Signalwege und Signalselektion.

6. Zu Ziff. 63:

Die Ausleitung findet auf OSI Layer 2 statt. Durch Taps wird eine optische Signalkopie erstellt und zum CEA weitergeleitet.

7. Zu Ziff. 64:

Die Ausleitung der Signale findet auf Layer 2 statt. Diese werden dann an den CEA weitergeleitet. Diese Signale auf Layer 2 sind grenzüberschreitend (s. Ausführungen oben); der FDA nimmt weder eine Prüfung noch eine Filterung vor.

8. Zu Ziff. 65:

Die FDA sind gem. Art 43 NDG verpflichtet, technische Angaben zu machen (Abs. 1). Diese Angaben werden beim CEA ausgewertet, um die grenzüberschreitenden Verbindungen zu identifizieren und gegebenenfalls die Ausleitung der entsprechenden Signale zu veranlassen. Zusätzlich hat die FDA die gesetzliche Pflicht, die Daten auszuleiten (Abs. 2) und die Kabelaufträge geheim zu halten (Abs. 3). Weitere technische Aufgaben wie Filterung oder Selektion fallen den FDA nicht zu.

Aus sicherheits- und technischen Gründen findet keine Datenverarbeitung oder Filterung am Ort der Ausleitung statt.

9. Zu Ziff. 66:

Mit den technischen Angaben der FDA (gem. Art. 43 Abs. 1 NDG) können grenzüberschreitende Leitungen klar identifiziert werden. Diese sind Leitungen, die einen logischen oder physischen Endpunkt im Ausland haben. Oft handelt es sich um Mietleitungen ins Ausland oder um einen Übergabepunkt an internationale Transportdienstleister. Logisch im Sinne von: mindestens ein Adressierungselement (z.B. IP-Adresse) befindet sich im Ausland. Und physisch: eine Mietleitung nach z.B. Frankfurt oder ein Upstream-Peering mit einem internationalen Provider.

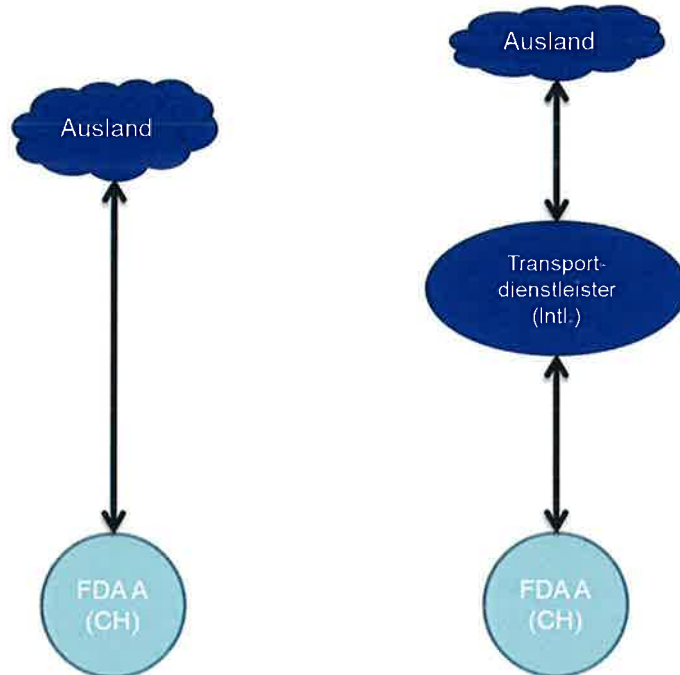


Abbildung 5: Transport über internationale Dienstleister

10. Zu Ziff. 67:

Der CEA definiert grenzüberschreitende Signale wie folgt: Grenzüberschreitende Signale sind Signale, deren Start- oder Zielort im Ausland ist. Dieser Start- resp. Zielort kann physisch (z.B. Frankfurt) oder logisch (IP-Adresse im Ausland) sein.

Der Ausleitungspunkt der Signale kann durchaus an Standorten innerhalb der Schweiz sein (bspw. Zürich) und nicht nur an einem Grenzzort (bspw. Basel). Die Signale sind an diesen Standorten bereits für das Ausland adressiert und ausgesondert und werden dort in für das Ausland bestimmte Leitungen eingespielen.

11. Zu Ziff. 68:

Siehe Stellungnahme unter Punkt 2. zu Ziff. 28.

12. Zu Ziff. 69:

Der CEA kann aufgrund der technischen Angaben der FDA die grenzüberschreitenden Verbindungen identifizieren. Falls es sich um eine Via-Kommunikation handelt, kann das wie schon unter Punkt 2. beschrieben, auf Layer 7 identifiziert werden.

13. Zu Ziff. 75:

Der CEA definiert Transitleitungen wie folgt: Transitsignale sind Signale, die logisch oder physisch den Ursprung und das Ziel im Ausland haben.

Es handelt sich hier um optische Verbindungen, die nur auf Layer 2 durch die Schweiz transportiert werden, und auf dem Weg durch die Schweiz regeneriert³ oder verstärkt⁴ werden. Es gibt mehrere FDA die Transitleitungen in der Schweiz betreiben. Die Behauptung der Beschwerdeführerin ist entspricht nicht der Realität.

14. Zu Ziff. 78:

Das von der Beschwerdeführerin erwähnte Beispiel mit einer gmail.com E-Mail-Absenderadresse ist insofern falsch, als dass diese Kommunikation von einer schweizerische IP-Adresse ausgeht, die als solche vom CEA erkannt werden.

Falls die organisatorischen und technischen Massnahmen des CEA zur Identifizierung und Aussonderung von Schweizer Verkehr keine eindeutigen Zuweisungen erlauben, so wird eine inhaltliche Kontextanalyse den Bezug zur Schweiz ergeben. Diese Daten werden dann durch den Analysten für die weitere Bearbeitung entsprechend markiert. Obwohl die Beschwerdeführerin behauptet, dass dieser Umstand oft vorkommt, kann der CEA aufgrund der gemachten Erfahrungen und der gelebten Praxis diese Aussage nicht bestätigen⁵.

15. Schlussbemerkungen:

Ogleich das Internet stetig wächst, ist die Anzahl der grenzüberschreitenden Verbindungen auch heute immer noch überschaubar und die transportierten Signale identifizierbar. Wird ein neues Glasfaserkabel gebaut, so wird es mit grösster Wahrscheinlichkeit an den bekannten Orten durchgeführt und an bestehende Internetknoten der Schweiz angeschlossen. Effizienz, Effektivität und Wirtschaftlichkeit sind wichtige Beweggründe für die FDA und sie orientieren sich beim Ausbau Ihrer Netze durchaus an diesen Grundsätzen.

Des Weiteren wurde vom CEA beobachtet, dass ein IP-Paket immer den kürzesten logischen Weg zwischen zwei Netzen nimmt (die Ausnahme bleibt weiterhin der Verbindungsausfall). Die Behauptung, dass es nicht möglich sei, den Weg eines IP-Pakets vorauszusagen, entspricht nicht den Erfahrungen des CEA. Es ist in der Tat möglich, grenzüberschreitende Kabelverbindungen zu identifizieren und diese zielgerichtet auszuleiten.

Darüber hinaus ignoriert die Beschwerdeführerin die Existenz und den Gebrauch von Caches (Zwischenspeicher) bzw. Content Distribution Networks (CDN). Populäre und etablierte Seiten oder Dienste werden an verschiedenen Orten im Internet zwischengespeichert, um nahe am Konsumenten des jeweiligen Internet-Dienstes zu sein. Oft befindet sich dieser Cache-Server direkt im Netz der FDA um die Last auf internationalen Leitungen zu vermindern. Diese Nähe verbessert das Endnutzererlebnis und die Netznutzung enorm. Eine Abfrage auf z.B. Netflix.com geht nicht zum Netflix Hauptquartier in Amerika, sondern wird lokal in der Schweiz von einem Cache-Server beantwortet. Das Gleiche trifft auf weitere populäre Seiten wie z.B. nytimes.com oder facebook.com zu.

³ Regeneration: das optische Signal wird kurzfristig in ein elektrisches Signal umgewandelt um es danach wieder optisch synchron weiterzuleiten.

⁴ Verstärkung: Der Transportverlust eines Lichtsignals wird durch einen Verstärker wieder ausgeglichen.

⁵ Es handelt es sich hier um Datensätze im einfachen Prozentbereich.

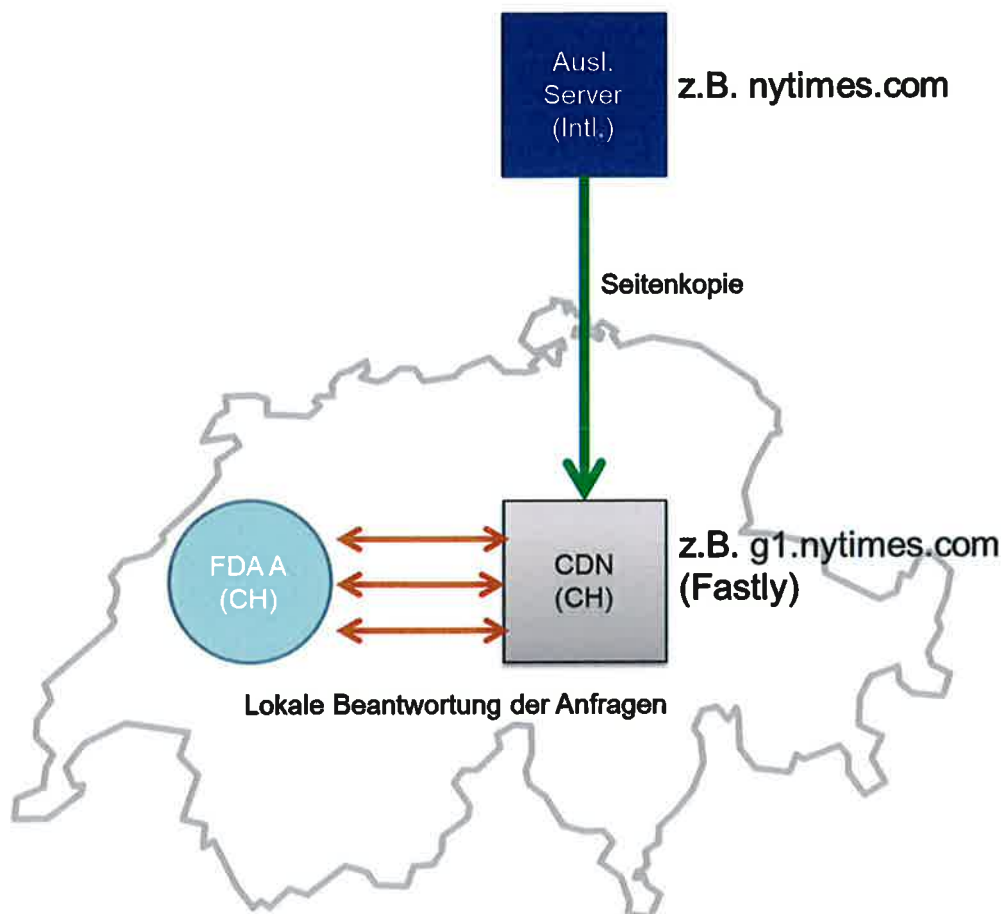


Abbildung 6: Content Distribution Networks

Anbieter solcher Cache Dienste werden CDN (Content Distribution Networks) genannt und die meisten Anfragen werden in der Regel in der Schweiz beantwortet; sie sind dadurch nicht grenzüberschreitend und werden somit nicht durch die Kabelauflklärung erfasst. Ohne diese Cache-Servers wären viele internationale Leitungen oder populäre Dienste völlig überlastet. Bekannte Anbieter von CDN sind beispielweise Akamai, Fastly oder Cloudflare⁶. Diese Anbieter sind für die Endbenutzer unsichtbar, verringern aber die Last auf den internationalen Verbindungen um ein Vielfaches und machen das moderne Internet überhaupt möglich, da nicht jede Kommunikation mit dem Endkunden über den Ursprungsserver stattfindet.

Diese Lastverteilung wird auch im E-Mail-Bereich wie z.B. bei Gmail eingesetzt. Ein E-Mail an @gmail.com geht also nicht über das Google Hauptquartier in Amerika, sondern wird in lokalen Servern beantwortet.

Die Behauptungen der Beschwerdeführerin über die Funktionsweise des Internets entsprechen mehrfach nicht den gemachten Erfahrungen des CEA.

* * * * *

⁶ Quelle: [CDN Finder - CDN Planet.](#)

Höflichst ersuche ich Sie um eine wohlwollende Prüfung der eingereichten Stellungnahme und der dazugehörigen Unterlagen.

Freundliche Grüsse

Kommando Cyber Kdo Cy



Robert Flück
Chef Dienst Cyber und elektromagnetische Aktionen

- *vierfach*