

„AUSSPÄHEN UNTER FREUNDEN“

Der NSA/BND-Angriff auf Belgacom und KPN Netherlands

„Ausspähen unter Freunden – das geht gar nicht.“

Als sie Opfer des amerikanischen Lauschangriffs wurde, hatte die deutsche Kanzlerin alle unsere Sympathien. Jetzt, wo es um das Ausspähen der österreichischen und der luxemburgischen Telekommunikation geht, ist sie nicht Opfer, sondern Chefin der Tatverdächtigen. Jetzt erwarten wir in Österreich, in Belgien und in den Niederlanden von ihr vor allem eines: Aufklärung.

DIE „GROSSE UMSCHALTAKTION“

Wie die NSA Transitleitungen auf die Prioritätenliste setzte

Helfrich, Harald

Von: Helfrich, Harald
Gesendet: Donnerstag, 3. Februar 2005 10:42
An: ‘telcom@bundesnachrichtendienst.de‘
Cc: Alster, Wolfgang
Betreff: Transit STM1 – Zuschaltung (Ffm 21 - Luxembourg 757/1)
Wichtigkeit: Hoch

Verlauf:

Empfänger	Übermittlung
‘telcom@bundesnachrichtendienst.de‘	
Alster, Wolfgang	Übermittelt: 03.02.2005 10:42

Hallo Hr. Siegert, Hr. Knau hat heute wieder eine STM 1 zugeschaltet. in dieser befindet sich nun kein nationaler Verkehr mehr (aus diesem Grunde fand auch die große Umschaltaktion statt). Die

Verbindung Ffm 21 - Luxembourg 757/1 wurde auf die Punkte 71 / 00/ 002 / 03 / 19 + 39 zugeschaltet. Vier der darin befindlichen 2MBit-Strecken befinden sich auf ihrer ersten Prioritätenliste, diese sind zu finden auf: Kanal 2: Luxembourg/VG - Wien/000
750/3Kanal 6: Luxembourg//CLUX - Moscow/CROS 750/1Kanal 14:
Ankara/CTÜR - Luxembourg/CLUX 750/1Kanal 50: Luxembourg/VG

-
Prague/000 750/1.Bitte um eine kurze Rückmeldung, wenn alles o.k. ist. Ende nächste

Woche folgt eine weitere STM1.Mit freundlichen Grüßen Harald Helfrich!“§§ComDeutsche Telekom AG ReSA Frankfurt Dipl. Ing. Harald Helfrich, RA 434-1Oeserstraße 11165934 Frankfurt*

(0 69) 6 64 29-1 01* (069) 6 64 29-1 50mailto:Harald.Helfrich@t-com.net

Dieses Mail der Deutschen Telekom AG an den BND haben wir vor kurzem in Wien veröffentlicht.

Darin meldet der ReSa¹-Mitarbeiter Helfrich dem BND-Mann Siegert den Vollzug eines NSA-Wunschs: den Zugriff auf vier weitere Transitleitungen.

Zu diesem Zeitpunkt lief die „Große Umschaltaktion“ – von deutschen Zielen auf Ziele von „Freunden“ wie Österreich, Belgien und den Niederlanden.

Im Jahr 2002 vereinbarten BND und NSA in einem Memorandum of Agreement (MoA) das gemeinsame Absaugen von Telekom-Leitungen. Dazu schloss der BND am 1. März 2004 den „Geschäftsbesorgungsvertrag Transit“ mit der Deutschen Telekom ab.

Darin wurde vereinbart:

„§ 1 Vertragsgegenstand

1. Der Auftraggeber beabsichtigt im Rahmen seiner Aufgabenstellung nach §§ 1 Abs. 2, 2 Abs. 1 Nr. 4 des Gesetzes über den Bundesnachrichtendienst vom 20.12.1990 kabelgestützte leitungs- und paketvermittelte Fernmeldeverkehre, die ihren Ursprung und ihr Ziel nicht in der Bundesrepublik Deutschland haben („Transit“), aufzuklären.“

Die „Zuschaltungen“ der Deutschen Telekom AG an BND und NSA fanden auf Basis dieses Vertrags statt.

Der BND erhielt Räumlichkeiten bei der Deutschen Telekom AG in Frankfurt. Dort wurden mittels Splitter die Daten ausgesuchter Transitleitungen nach Pullach abgeleitet. Von dort gingen die Daten an die Joint Signal Activity JSA in Bad Aibling, wo die NSA direkten Zugriff auf alle abgeleiteten Daten hatte.

DIE PRIORITÄTENLISTE

Der BND wählte die Leitungen anhand der Prioritätenliste der NSA.

In einer Prioritätenliste aus dem Jahr 2005 finden sich 255 Transitleitungen. Sie verteilen sich auf 31 europäische und 33 nichteuropäische Staaten.

INTERNATIONAL		EUROPA	
Abu Dhabi	1	Belgien	15
Ägypten	3	Bosnien- Herzegowina	6
Argentinien	1	Bulgarien	3
Australien	5	Dänemark	22
Bahrein	2	Finnland	6
Brasilien	2	Frankreich	46
Chile	1	Griechenland	2
China	9	Irland	2
Dubai	10	Italien	7

¹ Regionalstelle für staatliche Sonderaufträge – Verbindungsstelle der Deutschen Telekom AG zum BND

Elfenbeinküste	1	Kroatien	4
Gabun	1	Lettland	1
Guinea	1	Luxemburg	11
Indien	3	Niederlande	71
Indonesien	2	Norwegen	19
Israel	5	Österreich	11
Japan	10	Polen	26
Komoren	1	Portugal	3
Libanon	1	Rumänien	6
Malaysia	4	Russland	10
Mauritius	1	Schweden	25
Nigeria	1	Schweiz	9
Pakistan	1	Serbien	3
Philippinen	1	Slowakei	7
Saudi Arabien	13	Slowenien	2
Singapur	7	Spanien	5
Südkorea	1	Tschechien	15
Taiwan	4	Türkei	5
Thailand	2	Ukraine	2
Tschad	2	Ungarn	7
VAR	1	Weißrussland	2
Vietnam	2	Zypern	3
Zentralafrika	1		
Zimbabwe	1	31 Staaten Europa	134
		23 EU	80
		7 nicht EU	54
		33 nicht Europa	120
		64 insgesamt	254

Wichtige Staaten fehlen auf der Prioritätenliste: die USA, Kanada und Großbritannien. Allein in Großbritannien standen NSA und BND 156 Transitleitungen zur Auswahl. Keine einzige von ihnen wurde in die Prioritätenliste aufgenommen. Offensichtlich telefonieren Terroristen nicht mit London.

GROSSBRITANNIEN

London	93
Thameside, Vauxhall, Madley, Whitehill u.a.	63
gesamt	156

15 Transitleitungen auf der Prioritätenliste haben einen Endpunkt in Belgien, 71 einen in den Niederlanden. Die Niederlande liegen damit bei den Zielen der NSA mit Abstand an erster Stelle.

BELGIEN

LSZ	ENDSTELLE A	CARRIER	ENDSTELLE B	CARRIER
750	Bruxelles	Belgacom	Ljubljana	Telecom Slovenje
750	Banska Bystrica	Slovak Telecom	Bruxelles	Belgacom
750	Amsterdam	Getronics	Zaventem	GPS Belgium
750	Albertslund	Tele Danmark	Bruxelles	Belgacom
750	Bruxelles	Belgacom	Warszawa	Telekom Polska
750	Bruxelles	Belgacom	Yokohama/IDC	C&W IDC Tokyo
750	Beograd	Telekom Srbija	Bruxelles	Belgacom
750	Bruxelles	Belgacom	Zagreb	HT (Croatia)
750	Bruxelles	Belgacom	Prague	Czech Telecom
750	Bruxelles	Belgacom	Chiba	Kodi
750	Bruxelles	Belgacom	Sarajewo	BH Telecom
750	Bruxelles	Belgacom	Copenhagen	Tele Danmark
703	Paris	France Telekom	Bruxelles	Belgacom
703	Bruxelles	Belgacom	Paris	France Telekom
750	Bruxelles	Belgacom	Moscow	Rostelekom

NIEDERLANDE

LSZ	ENDSTELLE A	CARRIER	ENDSTELLE B	CARRIER
750	Amsterdam	KPN Netherlands	Minsk	BELTELCOM
750	Amsterdam	KPN Netherlands	Dharhan	Saudi Telecom Co.
750	Amsterdam	KPN Netherlands	Warszawa	Telekom Polska
750	Amsterdam	Getronics	Zaventem	GPS Belgium
750	Amsterdam	KPN Netherlands	Cairo	Telecom Egypt
712	Karachi	Paktelecom	Rotterdam	KPN Netherlands
750	Karachi	Paktelecom	Rotterdam	KPN Netherlands
750	Amsterdam	KPN Netherlands	Jeddah	Saudi Telecom Co.
712	Amsterdam	KPN Netherlands	Jeddah	Saudi Telecom Co.
750	Rotterdam	KPN Netherlands	Sarajewo	BH Telecom
750	Amsterdam	KPN Netherlands	Warszawa	Telekom Polska
750	Rotterdam	KPN Netherlands	Zagreb	HT (Croatia)
750	Amsterdam	KPN Netherlands	Luxemburg	P & T Luxemburg
712	Rotterdam	KPN Netherlands	Warszawa	Telekom Polska
750	Rotterdam	KPN Netherlands	Warszawa	Telekom Polska
750	Rotterdam	KPN Netherlands	Sofia	BTC
750	Albertslund	Tele Danmark	Rotterdam	KPN Netherlands
712	Copenhagen	Tele Danmark	Rotterdam	KPN Netherlands
750	Amsterdam	KPN Netherlands	Copenhagen	Tele Danmark
750	Ammen	TCC	Copenhagen	Tele Danmark
750	Amsterdam	KPN Netherlands	Salzburg	Telekom Austria
750	Amsterdam	KPN Netherlands	Bratislava	Slovak Telecom
750	Amsterdam	KPN Netherlands	Stockholm/Kista	Tele2Sweden
750	Amsterdam	KPN Netherlands	Kyiv	Utel
712	Amsterdam	KPN Netherlands	Dubai	Etisalat
750	Amsterdam	KPN Netherlands	Dubai	Etisalat
750	Amsterdam	KPN Netherlands	Jeddah	Saudi Telecom Co.
750	Amsterdam	KPN Netherlands	Banska Bystrica	Slovak Telecom
750	Amsterdam	KPN Netherlands	Yokohama/IDC	C&W IDC Tokyo
712	Rotterdam	KPN Netherlands	Singapore	SINGTEL
712	Rotterdam	KPN Netherlands	Taipei	Chunghwa Tele
750	Rotterdam	KPN Netherlands	Sydney	Reach GNL
750	Hong Kong	Reach Networks	Rotterdam	KPN Netherlands

750	Amsterdam	KPN Netherlands	Budapest	Matav
750	Amsterdam	KPN Netherlands	Brno	Czech Telecom
750	Amsterdam	KPN Netherlands	Ljubljana	Telecom Slovenje
750	Amsterdam	KPN Netherlands	Moscow	Rostelekom
750	Amsterdam	KPN Netherlands	Bucuresti	SNTc Romtelecom
750	Amsterdam	KPN Netherlands	Prague	Czech Telecom
750	Amsterdam	KPN Netherlands	Katowice	Telekom Polska
750	Bahrein	Batelco	Rotterdam	KPN Netherlands
750	Budapest	Matav	Rotterdam	KPN Netherlands
712	Amsterdam	KPN Netherlands	Istanbul	Turk Telekom
750	Amsterdam	KPN Netherlands	Istanbul	Turk Telekom
703	Rotterdam	KPN Netherlands	Siv	Bezeq
750	Bahrein	Batelco	Rotterdam	KPN Netherlands
703	Rotterdam	KPN Netherlands	Shanghai	China Telekom
750	Amsterdam	KPN Netherlands	Brasov	SNTc Romtelecom
750	Brasov	SNTc Romtelecom	Rotterdam	KPN Netherlands
750	Dubai	Etisalat	Rotterdam	KPN Netherlands
750	Bangkok	CAT	Rotterdam	KPN Netherlands
712	Limassol	CYTA	Rotterdam	KPN Netherlands
750	Amsterdam	KPN Netherlands	Kelana Jaya	Telecom Malaysia
712	Amsterdam	KPN Netherlands	Jeddah	Saudi Telecom Co.
750	Amsterdam	KPN Netherlands	Jeddah	Saudi Telecom Co.
750	Amsterdam	KPN Netherlands	Riyadh	Saudi Telecom Co.
712	Amsterdam	KPN Netherlands	Riyadh	Saudi Telecom Co.
712 2x	Amsterdam	KPN Netherlands	Jeddah	Saudi Telecom Co.
750	Amsterdam	KPN Netherlands	Siv	Barak Israel
712	Amsterdam	KPN Netherlands	Siv	Barak Israel
712	Amsterdam	KPN Netherlands	Cairo	Telecom Egypt
750	Istanbul	Turk Telekom	Rotterdam	KPN Netherlands
712	Istanbul	Turk Telekom	Rotterdam	KPN Netherlands
750 2x	Budapest	Matav	Rotterdam	KPN Netherlands
750	Ljubljana	Telecom Slovenje	Rotterdam	KPN Netherlands
750	Minsk	BELTELCOM	Rotterdam	KPN Netherlands
750	Prag	Czech Telecom	Rotterdam	KPN Netherlands
750	Bratislava	Slovak Telecom	Rotterdam	KPN Netherlands
750	Brno	Czech Telecom	Rotterdam	KPN Netherlands
750	Poznan	Telekom Polska	Rotterdam	KPN Netherlands
750 2x	Katowice	Telekom Polska	Rotterdam	KPN Netherlands

TATORT FRANKFURT

Im NSA-Untersuchungsausschuss des deutschen Bundestages sagte am 15.1.2015 Harald HELFRICH aus. Er arbeitet für die Deutsche Telekom AG am Knoten Frankfurt in der RESA, der „Regionalstelle für staatliche Sonderauflagen“.

Helfrich: *Transit ist Verkehr, der aus Ausland kommt, durch Deutschland geht und ins Ausland weitergeleitet wird. Übertragungsweg.*

Sensburg: *Transit-Verkehr. Aber kennen sie die Operation Transit?*

Helfrich: *Sagt mir gar nichts.*

Sensburg: Sind kein Jurist. [§ 27 Abs. 2 TKÜV](#): „Der Verpflichtete hat dem Bundesnachrichtendienst an einem Übergabepunkt im Inland eine vollständige Kopie der Telekommunikation bereitzustellen, die über die in der Anordnung bezeichneten Übertragungswege übertragen wird.“ Wie gestaltet sich die Datenherausgabe an eine Stelle wie den BND? Dopplung des Datenstroms, wie funktioniert das technisch?

[Greeve guckt zur Bundesregierung.]

Helfrich: Genau eine Leitung identifizieren, Verkehr mit technischer Einrichtung „T-Glied“ abzweigt und darauf Zugriff gegeben

Genau das geschah jahrelang mit den Leitungen von Belgacom und KPN Netherlands. Im Februar 2005 lief die Operation „Eikonal“ auf vollen Touren. Die Transitleitungen von Belgacom und KPN Netherlands standen auf der Prioritätenliste der NSA, die vom BND in Frankfurt abgearbeitet wurde. Der Verdacht ist ausreichend begründet, dass die Daten von Belgacom und KPN Netherlands am Knoten Frankfurt über das BND-Büro in der Deutschen Telekom AG ausgeleitet, dupliziert, nach Pullach in die BND-Zentrale weitergeleitet und von der Technischen Aufklärung (TA) des BND in Bad Aibling der NSA für den automatisierten Zugriff mittels Selektoren (Namen von Personen oder Unternehmen, Handy-Nummern, Kreditkartennummern etc.) online zugänglich gemacht wurden.

Der BND-Leiter der Aktion „Eikonal“ S.L. beschreibt am 4.12.2014 in der 26. Sitzung des NSA-UA des Bundestags:

„Das war der Beginn der Operation „Eikonal“. Dort haben wir Ausland-Ausland-Kommunikationsstrecken erfasst und diese nach unserem Auftragsprofil durchsucht. Das funktioniert so, dass Sie vom Betreiber eine vollständige Kopie der Strecke bekommen. Vollständige Kopie: Da schwirrt in den Köpfen vielleicht rum, da werden irgendwelche Datenträger ausgetauscht oder so was in der Art. Das ist es nicht. Die Strecken sind elektrisch oder Lichtwellenleiter. Das heißt, an dem elektrischen Leiter - das ist ein Koaxialkabel - wird ein Splitter eingebaut. Das können Sie sich eigentlich so vorstellen, wie wenn Sie daheim an die Fernsehantenne oder an den Kabelanschluss einen zweiten Fernseher anschließen. Der Splitter, das ist ein Prisma. Da geht ein Teil weiter an den Betreiber, da, wo es aus seinen betrieblichen Gründen hinsoll, und ein Teil des Lichtes geht dann zum BND.“

„Das Kabel - ob das Lichtwellenleiter oder Koaxialkabel ist, ist eigentlich unerheblich - geht in einen Betriebsraum, den wir normalerweise vom Betreiber anmieten.“

„Aus Pullach wurde das Ganze zu JSA nach Bad Aibling weitergeleitet.“

Vorsitzender Dr. Patrick Sensburg: Mit welchem Grund?

Zeuge S. L.: Ich verstehe Ihre Frage nicht.

Vorsitzender Dr. Patrick Sensburg: Warum hat man das von Pullach nach Bad Aibling weitergeleitet? Dafür muss es ja einen Grund gegeben haben.

Zeuge S. L.: Weil dort das Sachgebiet JSA war, wo die bearbeitet wurden.

Vorsitzender Dr. Patrick Sensburg: Bearbeitet oder mit der Intention in Pullach schon, das weiterzuleiten an die NSA?

Zeuge S. L.: Mit der Intention, das Ganze nach Bad Aibling weiterzuleiten, damit dort die Mitarbeiter von JSA, also die deutschen und US-Mitarbeiter, das bearbeiten konnten.“

Später gibt S.L. an:

„In diesem Fall für die Operation „Eikonol“ wurden Selektoren eingestellt durch den BND nach dem Auftragsprofil des BND und Selektoren von US-Seite.“

So wurden im Rahmen der JSA (Joint Signal Activity) zahlreiche Transit-Leitungen der Telekom Austria, der Belgacom, der KPN Netherlands und anderer Telekom-Provider für die NSA abgeleitet.

Die Zeugenaussagen vor dem Untersuchungsausschuss des Deutschen Bundestags er Belegen, dass nicht in Einzelfällen, sondern großflächig abgeleitet und abgesaugt wurde.

DIE SELEKTOREN

Die NSA wertet die abgesaugten Telekom-Daten mittels Selektoren – Suchbegriffen wie Namen, Handy-Nummern, Kreditkartennummern - aus.

In Wien, Genf und Brüssel wurden die Selektoren des UN-Personals auf Basis eines HUMINT-Befehls des Sate Departments der USA beschafft.

Der Spionagebefehl vom 31. Juli 2009 mit der Kopfzeile CLASSIFICATION SECRET//NOFORN - S E C R E T SECTION 01 OF 24 STATE 080163 ging an vier Adressen in Österreich, in der Schweiz und in Belgien: RUEHVI/AMEMBASSY VIENNA 8905, RUEHUNV/USMISSION UNVIE VIENNA 5248, RUEHGV/USMISSION GENEVA 8154 und RUEHBS/AMEMBASSY BRUSSELS 4458.

NOFORN heißt „No Foreigners“. Damit soll sichergestellt werden, dass keine ausländischen Freunde von diesem Befehl erfahren. Die USMISSION UNVIE ist die US-Mission bei der UNO in Wien, die USMISSION GENEVA ihr Pendant in Genf. Auf den Dächern dieser Missionen sitzt auch der Special Collection Service von NSA und CIA mit seinen Hochleistungsantennen.

Ziel der HUMINT-Aktionen sind Namen, Telefonnummern, Kreditkartennummern, Kontonummern, e-mail-accounts, IP-Adressen u.a. In Deutschland sollen bei den Aktionen der NSA 8,7 Millionen Selektoren eingesetzt worden sein. Bei ein Schnitt von fünf Selektoren pro Zielperson kommt man auf rund 1,7 Millionen ausgespähte Personen.

Die SIGINT-Daten werden über das Abschöpfen von Telekom-Leitungen, Satelliten-Überwachung, direkte Angriffe auf Rechner und das Special Collection Service SCS von NSA und CIA beschafft. In Wien sind zwei und in Genf ist eine SCS-Anlage in Betrieb.

Die ausspionierten HUMINT-Daten sind dann die Selektoren, mit denen die NSA ihre in Frankfurt abgeschöpften Massendaten durchsucht.

DER VERDACHT

Mit den Unterlagen zur Aktion „Transit“ gegen Österreich, Belgien, die Niederlande und 21 weitere Mitgliedsstaaten der EU wird der Verdacht illegaler Handlungen durch BND und NSA mit Hilfe der Deutschen Telekom AG erstmals mit Beweisen begründet.

FRAGEN AN DIE DEUTSCHE BUNDESREGIERUNG

Eikonal, Joint Signal Activity, Frankfurt – Pullach – Bad Aibling - es ist bekannt, wozu vor rund zehn Jahren die Prioritätenlisten der NSA gebraucht wurden.

Dazu sind nach wie vor einige der wichtigsten Fragen offen:

1. Wurden alle in den Prioritätenlisten aufgeführten Leitungen dem BND „zugeschaltet“?
2. Welche Daten von Personen aus Österreich, Belgien und den Niederlanden befanden sich in den abgeleiteten Datensätzen?
3. Welche NSA-Selektoren wurden zur Auswertung dieser Daten verwendet?
4. Welche Verträge mit welchen Kunden gab es zu diesen Leitungen zwischen 2004 und 2008 und was wussten NSA und BND über diese Kunden?
5. Sind dabei auch Regierungen, internationale Organisationen und Unternehmen abgeschöpft worden?
6. Wie lange unterstützte der BND die NSA beim Zugriff auf die internationale Telekommunikation von europäischen Staaten?
7. Ist es heute noch möglich, dass der BND die NSA bei derartigen gegen EU-Mitgliedsstaaten gerichteten Tätigkeiten unterstützt?
8. Von wem und mit welchem Ergebnis wurde geprüft, ob der Geschäftsbesorgungsvertrag „Transit“ zwischen der Deutschen Telekom AG und dem BND vom 1.3.2004, mit dem das Fernmeldegeheimnis flächendeckend außer Kraft gesetzt wurde, gesetzwidrig ist?
9. War das deutsche Bundeskanzleramt über die Aktion „Transit“ gegen befreundete Staaten aus der EU informiert?
10. Sind Unternehmen oder staatliche Stellen in den betroffenen Ländern über die Aktion informiert worden?

Eine elfte Frage dient nicht der Aufklärung, sondern der Wiederherstellung des beschädigten Vertrauens:

Wird die deutsche Bundeskanzlerin ihr Bedauern über das Ausspähen ihrer Freunde zum Ausdruck bringen?