NSA Überwachung

Vor und nach 9/11

Dr. Erwin Hoffmann

19.11.2013

NSA Überwachung – vor und nach 9/11

Bis vor einem halben Jahr hätten nur die wenigsten hier mit den drei Buchstaben

N - S - A

etwas angefangen können, wo hingegegen

C - I - A

und

N - A - S - A

sofort Assoziationen geweckt hätten.

Inhalt des Vortrages:

- Aktuelle NSA Überwachungsprogramme und deren Ziele.
- Änderungen in der NSA Strategie nach 9/11.
- Einfluss der NSA auf die Kryptographie und die standardisierten Verschlüsselungsalgorithmen.
- Funktioniert Kryptographie überhaupt noch und welche Alternativen gibt es ?

Hintergründe

Zu meiner Person:

- Von 2007 bis 2013 Professor für Informatik an der FH Frankfurt am Main: Netzwerke, Betriebssysteme, IT-Security.
- Implementierung von TLS in UCSPI-SSL und Qmail.
- Freiberuflicher IT-Berater.

Zum Vortrag:

- Der Vortrag stützt sich auf lediglich öffentlich bekannte Informationen.
- Speziell dem Wistleblower *Edward Snowden* und den Veröffentlichungen im *Guardian*.
- Ergänzende Kenntnisse kommen aus den langen Jahren der Begleitung von Prof. Daniel Bernstein (djb).

$\Longrightarrow$ Ich möchte keine 'politische' oder 'rechtliche' Bewertung der aktuellen Diskussion über die NSA vornehmen, sondern technische Fragen klären.

Der Beginn der Überwachung: ECHELON

ECHELON ist ein Kind des kalten Kriegs:

Abbildung : Echeleon Radiodome: Station 81 in Bad Aibling, Bayern

- ECHELON wurde geschaffen, die militärische und diplomatischen Kommunikation der *Sowjet Union* und der Staaten des Ostblocks abzufangen.
- Später wurde das System auch dazu genutzt, per ECHELON auch private und geschäftliche Kommunikation mitzuschneiden.

$\Longrightarrow$ ECHELON ist also ein klassisches, stationäres Spionage-System, das mit Wissen und Einwilligung der Verbündeten betrieben wird.

`http://en.wikipedia.org/wiki/ECHELON`

Wide Area Airborne Surveillance – WAAS

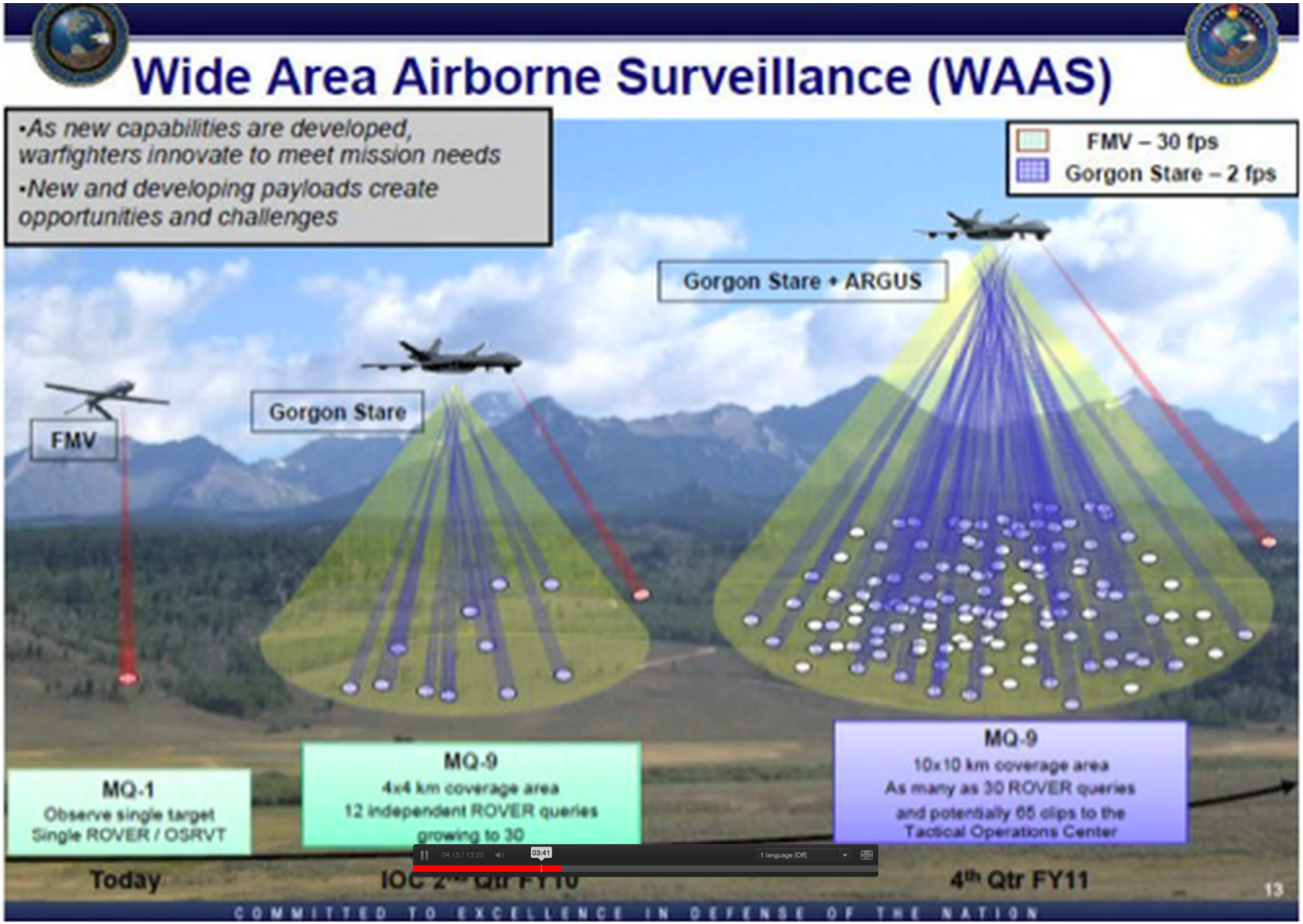


Abbildung : Abfangen der Drahtlos-Kommunikation mittels 'ECHELON mobile'

9/11: CIA's Peral Harbor

Bei der Schaffung des NSA 'CyberCommand' sind zwei zentrale Entwicklungen hervor zu heben:

1. Mit der Verbreitung des Internets Anfang der 90er Jahre und mit der 'Erfindung' der *Public Key* Kryptographie ist es nun nicht mehr nur dem 'Eingeweihten' möglich *starke Verschlüsselung* einzusetzen, sondern Kryptographie wird quasi 'public'.

   $\Longrightarrow$ Die Versuche der US-Regierung *starke Kryptographie* nicht ausserhalb der USA zu 'exportieren' müssen als gescheitert betrachtet werden.
2. Mit den Anschlägen von 11. September 2001 in den USA ('9/11') sahen sich diese der Tatsache gegenüber gestellt, dass zwar Informationen über die Attentäter gesammelt wurden, aber es keine Verknüpfungen gab:

   $\Longrightarrow$ 'Pearl Harbor' der CIA.

Im weiteren Verlauf wurde 2002 das 'Homeland Security Department' gegründet und die Mittel für die NSA drastisch aufgestockt, z.Z. wohl ca. 60 Mrd. $ pa.

$\Longrightarrow$ Die Programme der NSA und CIA wurden neu geordnet, sowie mit den engsten Verbündeten ('five eyes' `FVEY` *Tier 1*) gemeinsam betrieben.

NSA 'CyberCommand'

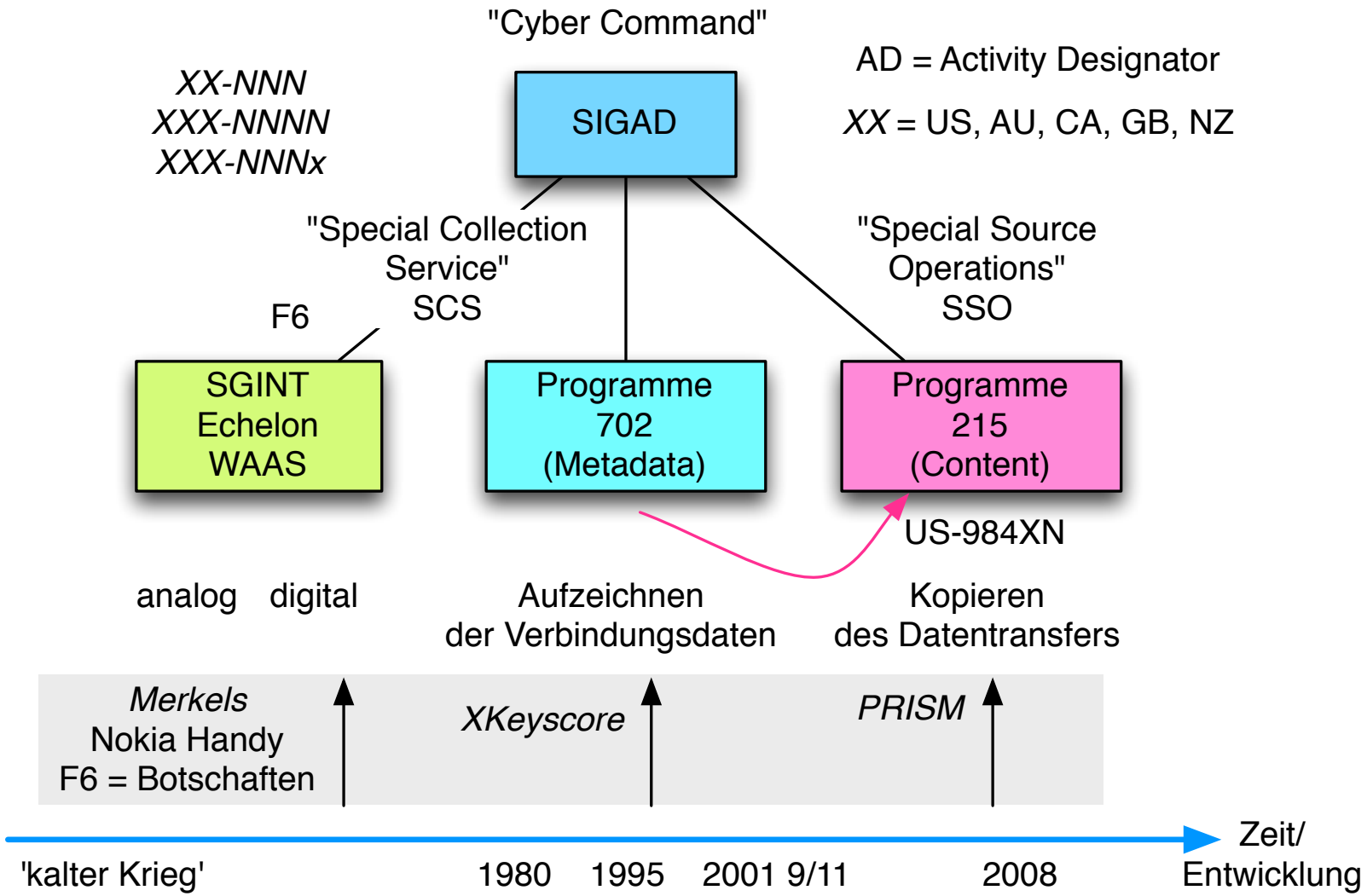


Abbildung : Überblick über die NSA-Überwachungsprogramme

SCS Lokationen

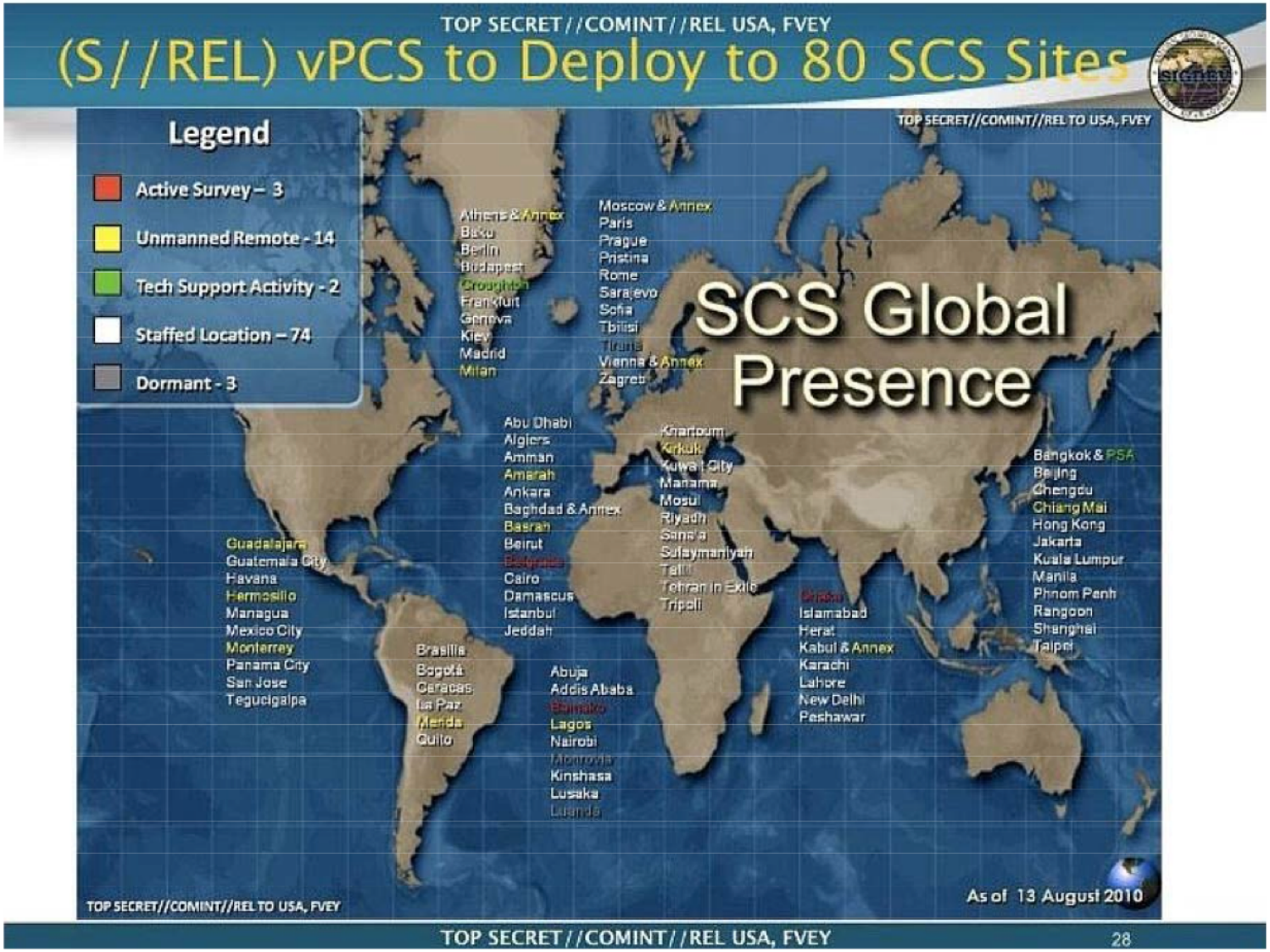


Abbildung : Weltweite Lokationen des NSA 'Special Collection Service'

Verbindungsdaten

Das Abgreifen von Verbindungsdaten (Telefon) ist seit Jahrzehnten gängige Praxis. In USA werden diese speziell für die Bekämpfung von Drogenkriminalität genutzt:

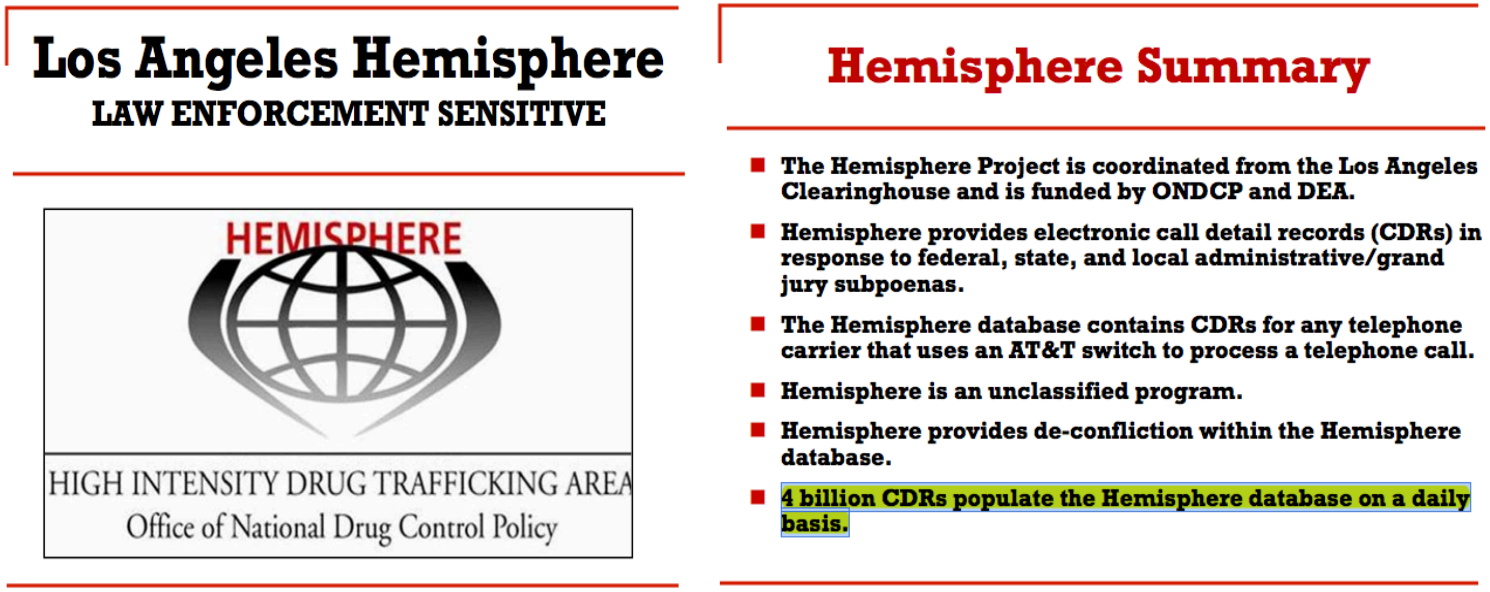


Abbildung : Abgreifen *Call Detail Records* in Los Angeles

Um diese Verbindungsdaten *Call Detail Records* **CDR** abzugreifen, sind in den TK-Standards, die von der ETSI definiert werden, wohldefinierte Schlüsselfelder vorgesehen, die insbesonderer von der Polizei bei Bedarf genutzt werden können: *Lawfully Authorized Electronic Surveillance*.

$\Longrightarrow$ Bei der Definition der ETSI-Tap-Schnittstellen ist die 'Surveillance group SA3 LI' mit dabei.

Capture des Internet-Datenverkehrs

Nach 9/11 war klar, dass nicht nur die Meta-Daten (Verbindungsdaten) aufgezeichnet werden müssen, sondern das Gesamtvolumen des Internet-Verkehrs. Offene Fragen:

- Wie und Wo können die IP-Pakete abgegriffen werden ?
- Wie werden diese aufgezeichnet und bevorratet (*Datenvolumen*) ?
- Wie kann das Datenvolumen sinnvoll ausgewertet werden (‘*BigData*’)?

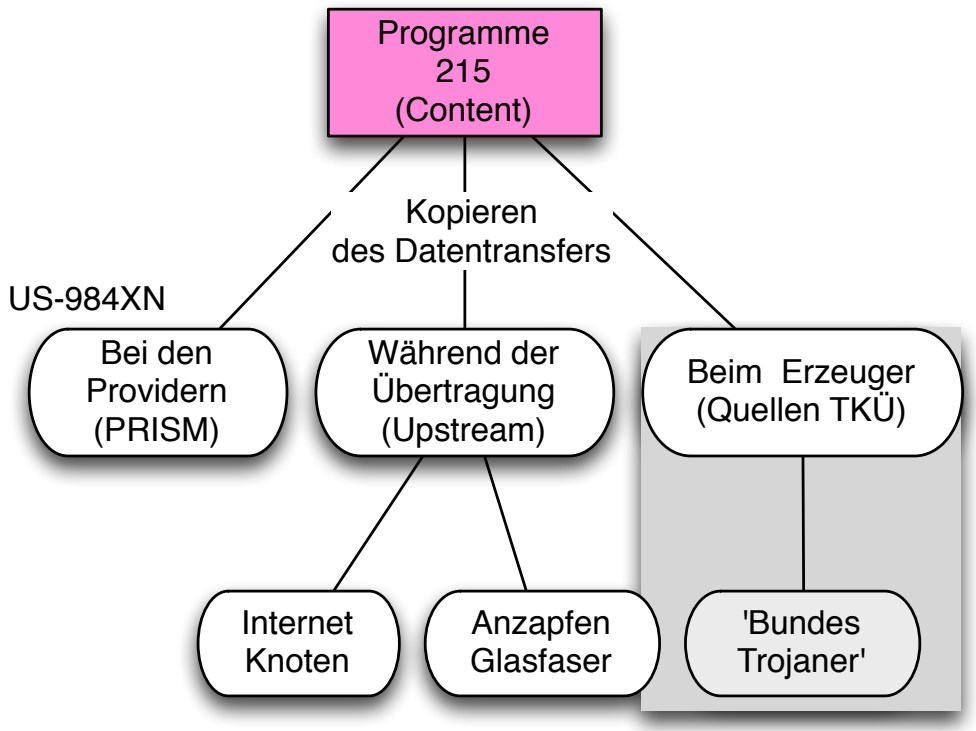


Abbildung : Mögliche Aufzeichnungspunkte für den Internet-Datenverkehr

$\Longrightarrow$ Hierfür wurde das *Special Source Operations* Team gegründet.

Das Programme US-984XN – PRISM

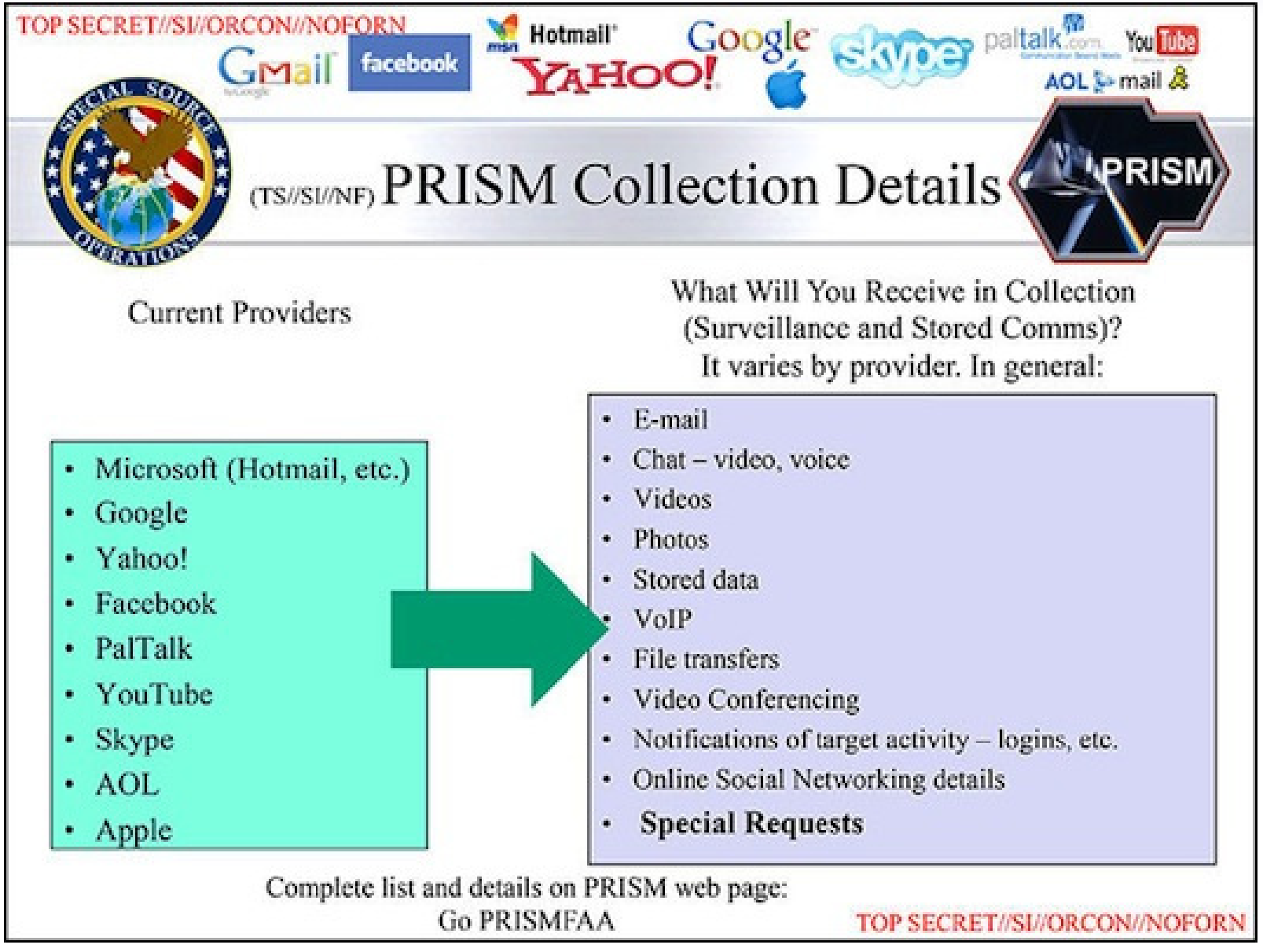


Abbildung : Ablauf der PRISM Datennahme

Die PRISM 'Programm-Partner'

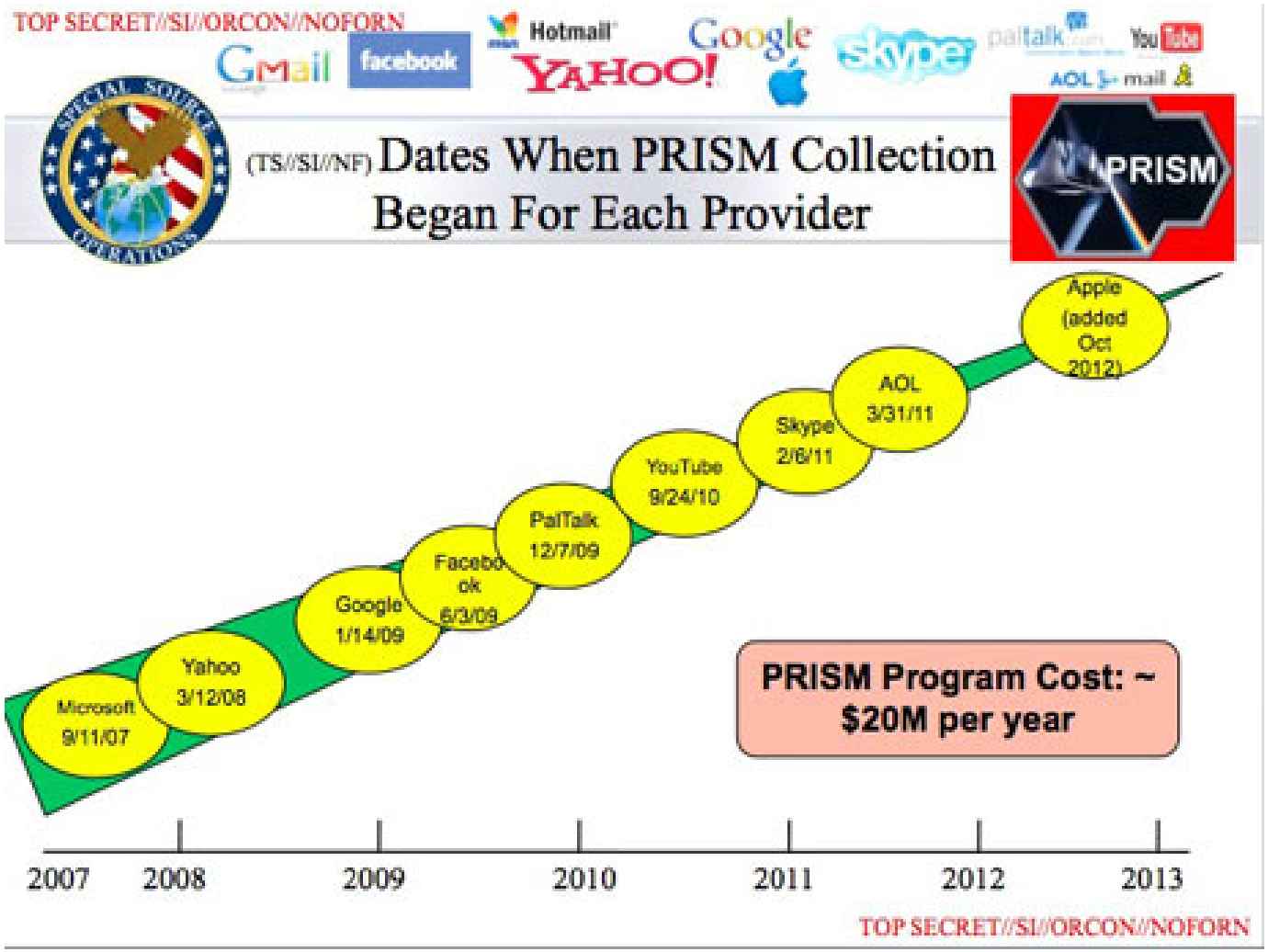


Abbildung : Firmen mit PRISM Schnittstelle

Statements zu PRISM-Zugriffen

Obwohl über *Edward Snowden* bekannt gemacht wurde, dass PRISM die Benutzerdaten von Apple, Google und anderen Firmen seit 2007 abgreift, leugnen die betroffenen Firmen Kenntnisse über den Einsatz von PRISM:

$\Longrightarrow$ Die US-Gerichtsbarkeit nutzt geheime sog. *National Security Letters* **NSL**, die es den Betroffenen bei Strafe verbietet, über das Programm zu sprechen.

Allgemein wurden folgende Zahlen bekannt:

- Yahoo: Zwischen Dezember 2012 und dem 31. Mai 2013 wurden zwischen 12.000 und 13.000 offizielle Datenanfragen gemacht.
- Apple: 4.000 sowie 5.000 Anfragen kamen von US-Offiziellen bzw. Bundesstaaten und lokalen Stellen.
- Facebook: 9.000 und 10.000 Daten-Anfragen für 18.000 bis 19.000 Benutzer-Accounts.

Das 'offizielle' PRISM Statement

James Clapper, *Office of the Director of National Intelligence* **ODNI**:

> *"The statement that a single analyst can eavesdrop on domestic communications without proper legal authorization is incorrect and was not briefed to Congress. Members have been briefed on the implementation of Section 702, that it targets foreigners located overseas for a valid foreign intelligence purpose, and that it cannot be used to target Americans anywhere in the world."*

Abbildung : 'Chef' der NSA: James R. Clapper

↪ Das PRISM Programm sieht vor, nur Daten bedarfsweise von *nicht US-Bürgern* zu erfassen.
Eine Datenerfassung mittels PRISM muss vom (*geheimen*) FISA-Court abgesegnet werden.

PRISM Datenquellen

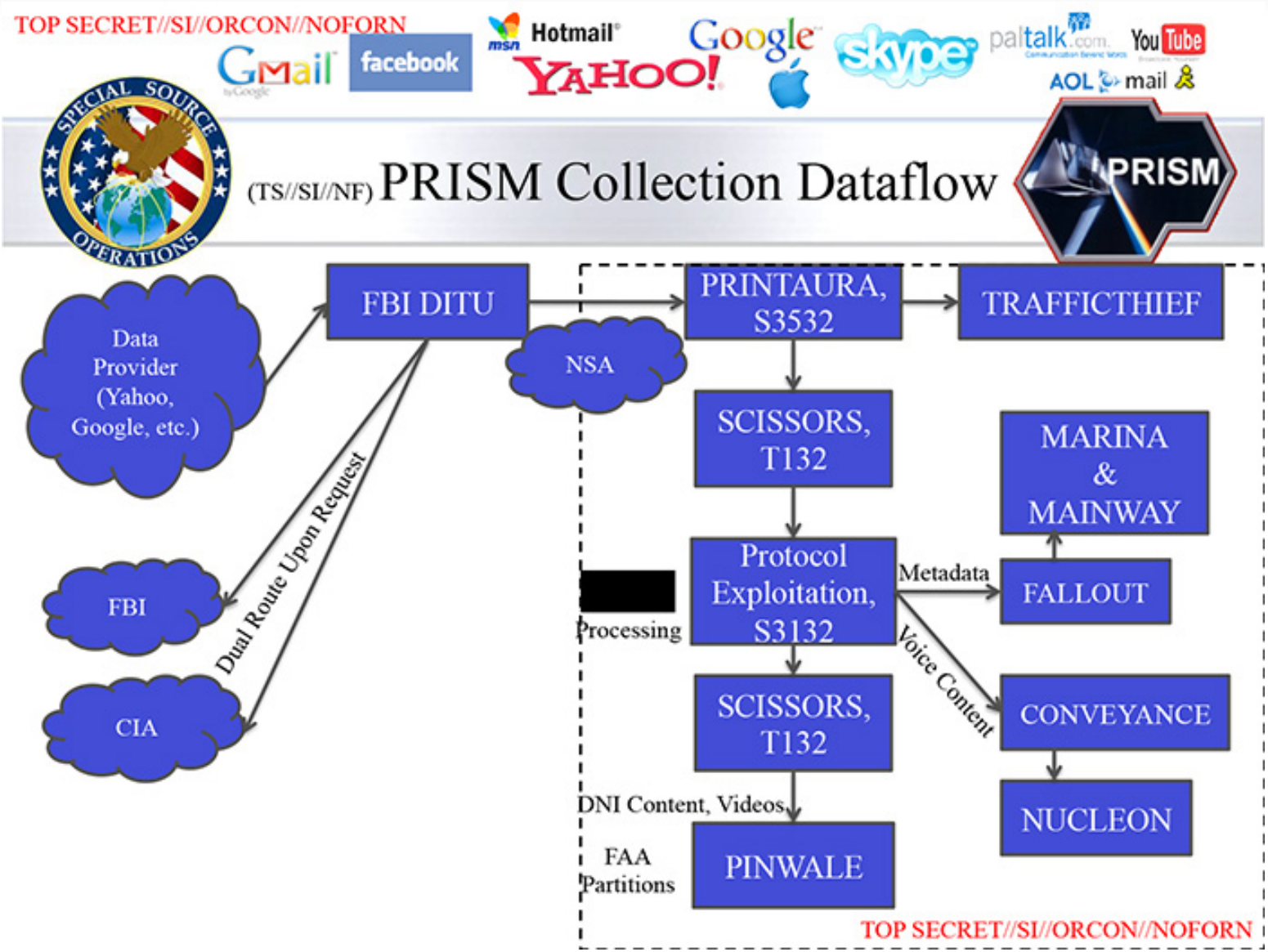


Abbildung : Verknüpfung der Datenquellen bei PRISM

Ein PRISM ist nicht genug !

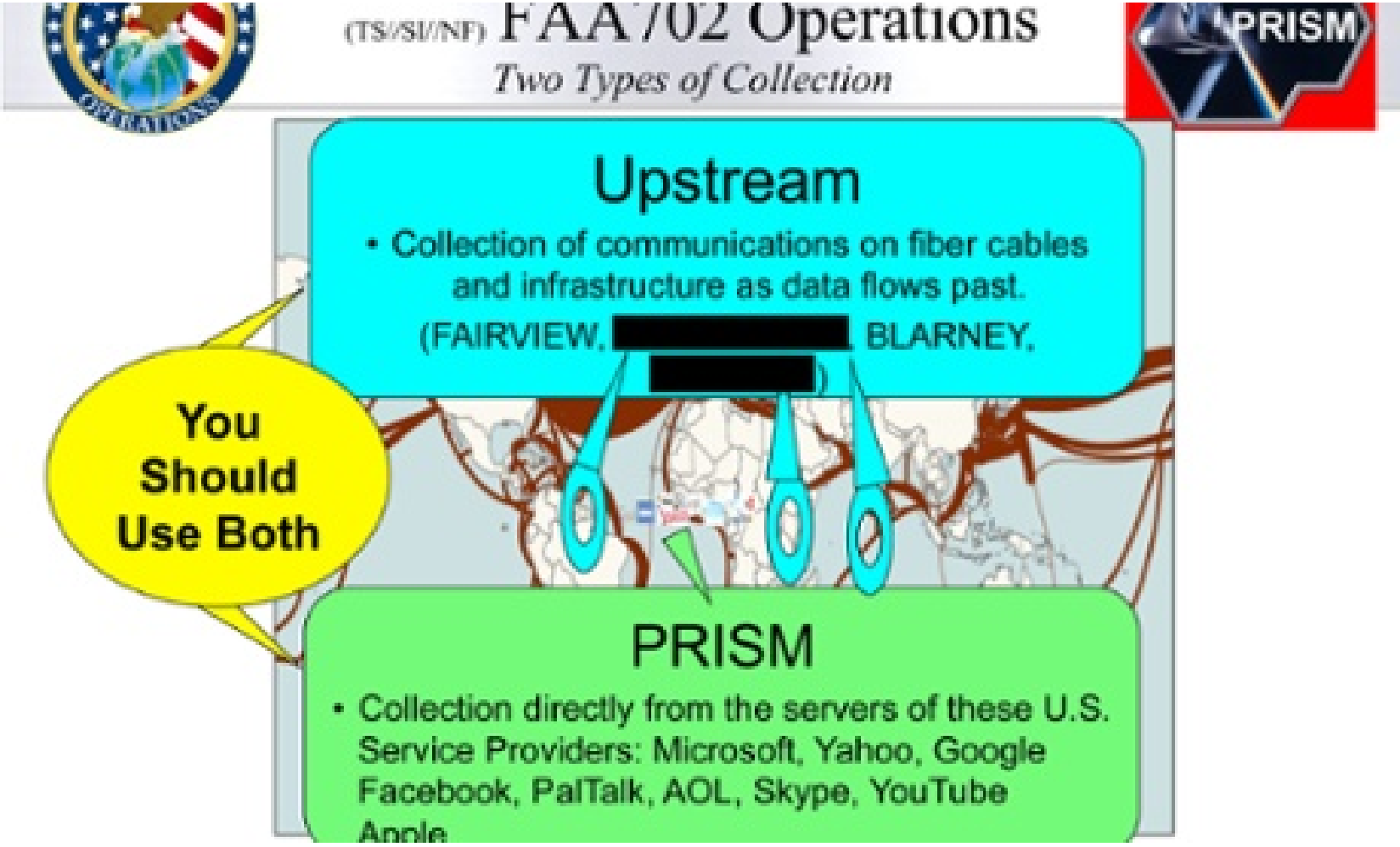


Abbildung : 'Offizielle' PRISM Aufgabenstellung

Der NSA Krake

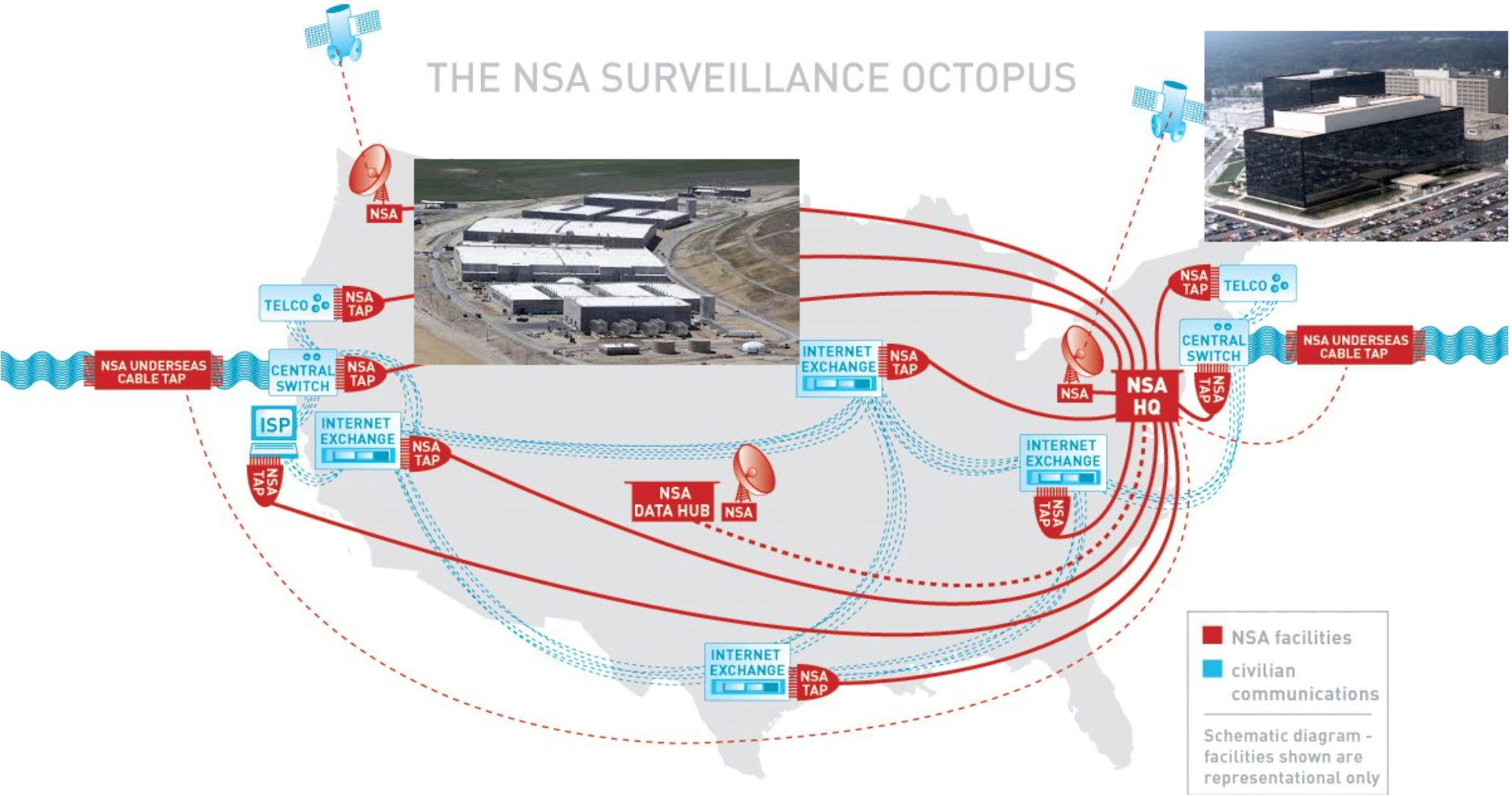


Abbildung : NSA Internet tapping `http://www.pacificviews.org/weblog/archives/017425.php`

NSA Kommandozentrale

Abbildung : NSA Command Office

Zugriff auf die Internet-Infrastruktur

- Die NSA hat Zugriff auf die IP-Exchange-Knoten in den USA.
- AT&T Techniker haben über verborgene 'Überwachungsräume' der NSA berichtet: 'Raum 641A' `http://en.wikipedia.org/wiki/Room_641A`.
- Der damit überwachbare *domestische* Datenverkehr reicht aber nicht aus, erweiterte 'Kenntnisse' zu sammeln.
- Zusammen mit den anderen 'Tier 1' Partnern (`EYFIV`) werden auch die Internet-Knoten – speziell in Gross Britannien – abgezapft. Hierfür werden gemeinsame Geheimdienst-Einheiten gebildet und eingesetzt.

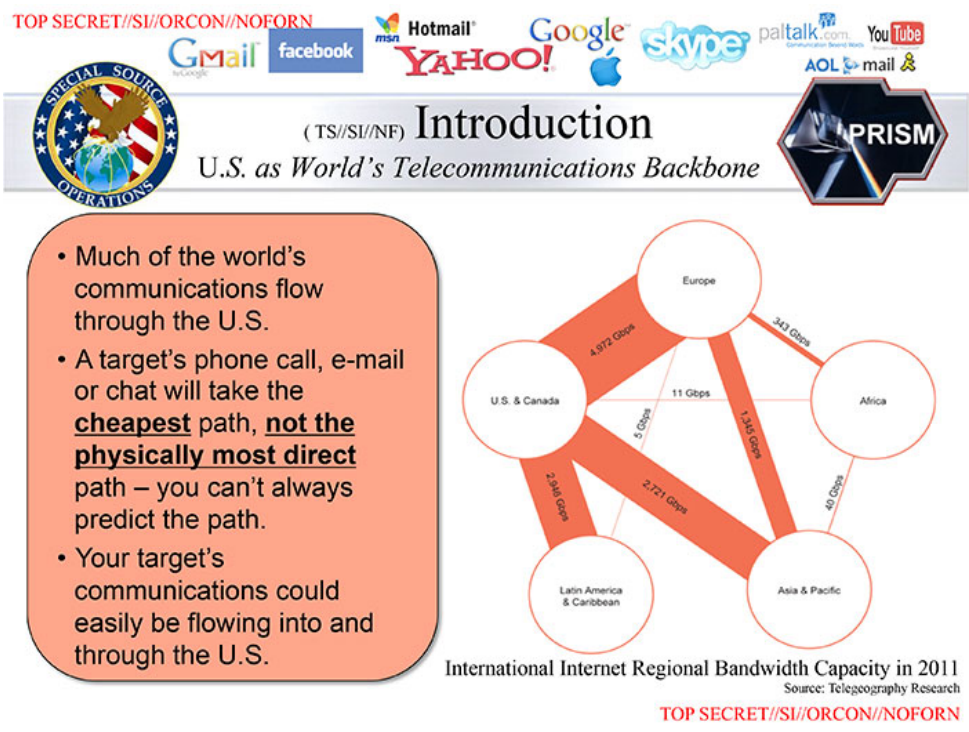


Abbildung : 'Upstream Collection' – Europa/US
Link-Kapazität: ca. 5 Tbit/s (2011); im Vergleich: DE-CIX Knoten für Deutschland: 2,5 Tbit/s *Durchsatz* (2013)

$\Longrightarrow$ Ein Grossteil des Internet-Datenverkehrs von Europa zu den USA läuft über den (Glasfaser) Internet-Exchange-Knoten in London.

Tap-Schnittstelle in CISCO-Router

Lawful Intercept Administration

Lawful intercept administration (LIA) provides the authentication interface for lawful intercept or wiretap requests and administration.
The SP and ISP use the LI administration function to provision intercepts by interface with the other components in the network.
The LI administration function is responsible for the following:

- *Provisioning components in the network*
- *Administering intercept orders*
- *Tracking and maintaining intercept information*

The LI administration function also supervises the security and integrity of the LI process. The function continuously audits activity logs to ensure that only authorized intercepts are provisioned and that authorized intercepts are not disrupted.

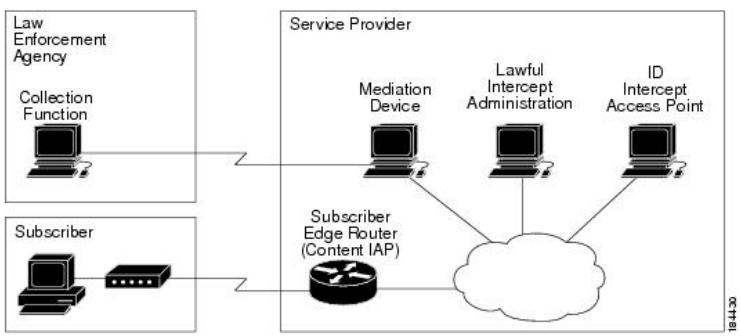
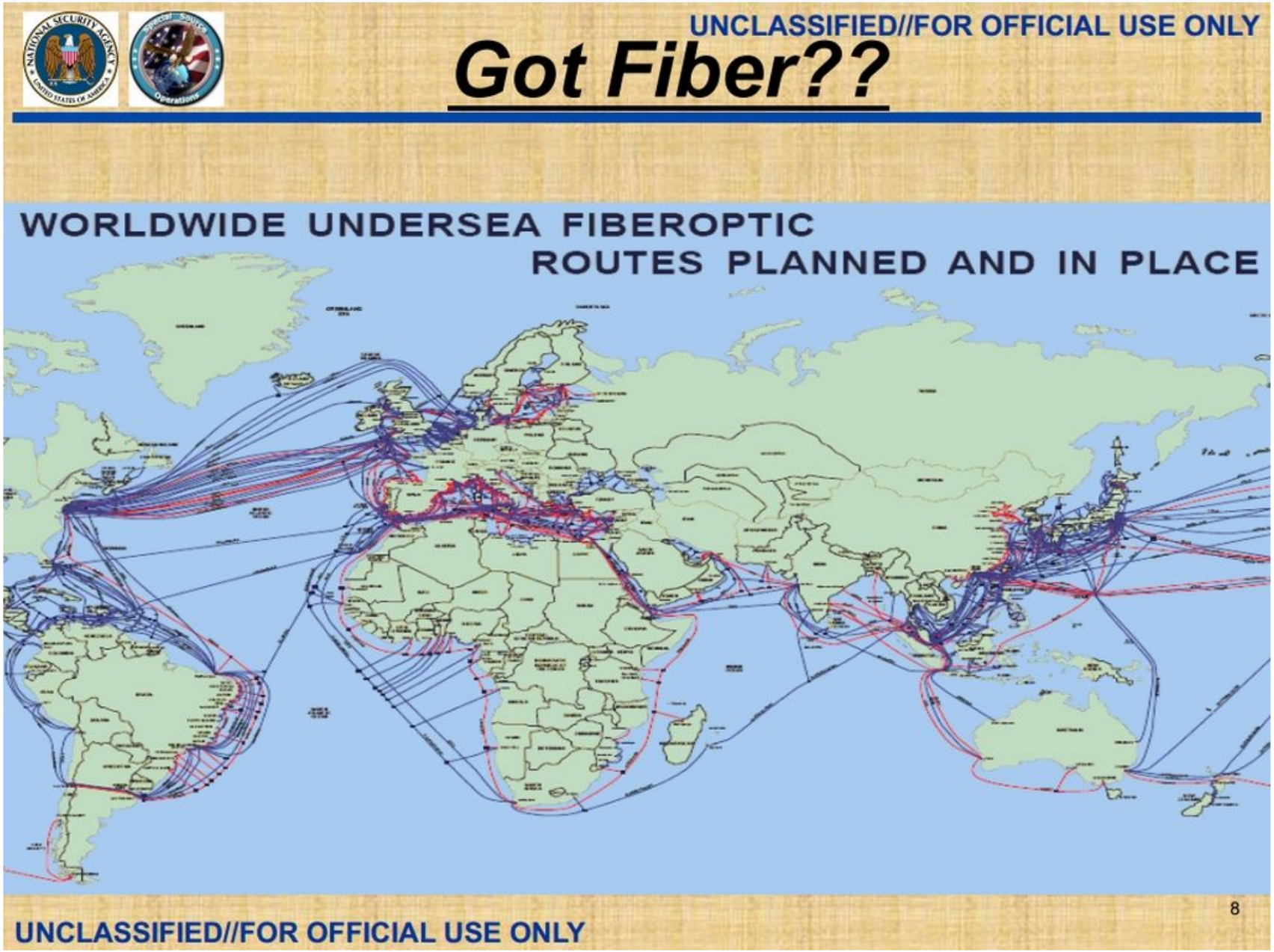


Abbildung : CISCO Router 'Lawful Interception' Schnitttstelle – `http://www.cisco.com/en/US/docs/routers/7600/ios/12.2SR/configuration/lawful_intercept/76LIch1.html`

Internet-Seekabel



Anzapfen der Glasfaser-Unterseekabel

Beim Anzapfen von (Tief-)See-Glasfaser-Kabel gibt es einige Besonderheiten zu beachten:

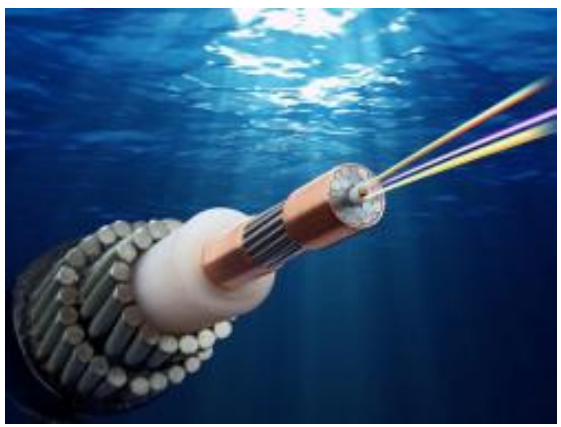


Abbildung :
Unterwasser-Glasfaser-Bündel

- Das Seekabel muss geortet werden und die Signal-Belegung der mehreren hundert Glasfasern bekannt sein (sind markiert).
- Die Ummantelung muss aufgebrochen und die spezifische Faser unterbrochen, das Lichtsignal ausgeleitet und die Faser anschliessend neu gespleisst werden.
- Die Ummantelung ist so herzustellen, dass sie das Kabel wieder schützt.
- Die Faser ist eine Mono-Mode-LWL mit 10 μm Durchmesser.
- Der Lichtverlust ist $>$ 3 dB, was einen hohen *Gain* beim Sender verlangt; kann also nicht 'irgendwo' vorgenommen werden.

$\Longrightarrow$ Dies kann eigentlich nur im 'Trockenen' vorgenommen werden!
Und: Wohin mit den ausgeleiteten Daten?

Anzapfen der Glasfaser-Internet-Verbindungen

Vorkommnisse:

1. Ende Januar 2008: '*Die beiden beschädigten Leitungen wurden rund acht Kilometer nördlich von der ägyptischen Stadt Alexandria unterbrochen.*'
   `http://www.heise.de/tr/artikel/Warum-das-Netz-zusammenbrach-274898.html`
2. Zeitgleich: '*Am vergangenen Freitag kam dann die nächste Hiobsbotschaft für die Region: Auch im persischen Golf, vor der Küste des Emirates Dubai, ging ein weiteres Kabel kaputt, die sogenannte Falcon-Verbindung. Und am gestrigen Sonntag gab eine vierte Netzverbindung ihren Geist auf - wieder im persischen Golf, diesmal aber zwischen Katar und den Vereinigten Arabischen Emiraten.*'
   `http://www.spiegel.de/netzwelt/tech/internet-seekabel-vierter-netzausfall-naehrt-verschwoerungs-theorien-a-533html`
3. 2013: USA fragen Japan, das Untersee-Kabel, das an ihrer Küsten entlang läuft anzapfen zu dürfen; Japan lehnt ab.
   `http://www.japantimes.co.jp/news/2013/10/27/world/nsa-asked-japan-to-tap-regionwide-fiber-optic-cables-in-2011/`

Die 'Jimmy Carter'

Mittels des Atom-Uboots 'Jimmy Carter' (SSN-23), das 2004 in Betrieb genommen wurde, besitzen die USA ein entsprechendes Gerät.
Über den den Zusatzbau

> *'This is due to the insertion of a plug (additional section) known as the Multi-Mission Platform (MMP), which allows launch and recovery of ROVs and Navy SEAL forces.'*

können Arbeiten in der Tiefsee quasi 'on-board' durchgeführt werden.

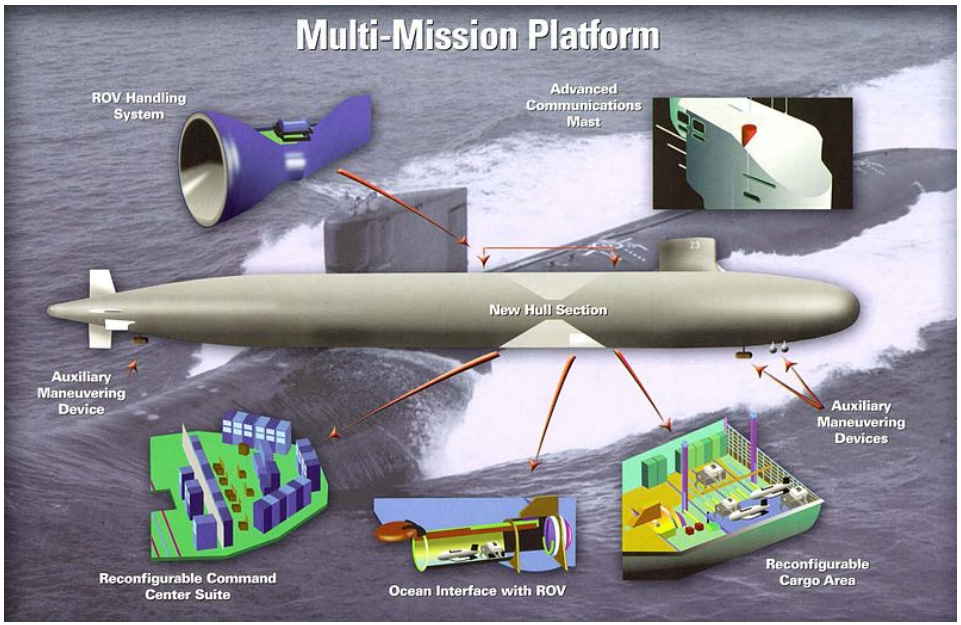


Abbildung : Die 'Jimmy Carter' auf dem Dock

`http://en.wikipedia.org/wiki/USS_Jimmy_Carter_(SSN-23)`

Arbeitsteilung NSA/GCHQ

Die NSA steht in regen Austausch mit dem britischen Geheimdienst GCHQ im Rahmen des FVEY Programms. Der GCHQ betreibt das Program 'Tempora'.

- Die NSA hat direkten Zugang auf die GCHQ Datenbestände und ungekehrt, was unter dem Programmnamen 'Muscular' läuft.
- Zwischen NSA und GCQH besteht eine direkte Datenverbindung mit 4*2,48 Gbit/s (STM-16) $\Longrightarrow$ *TURMOIL*.

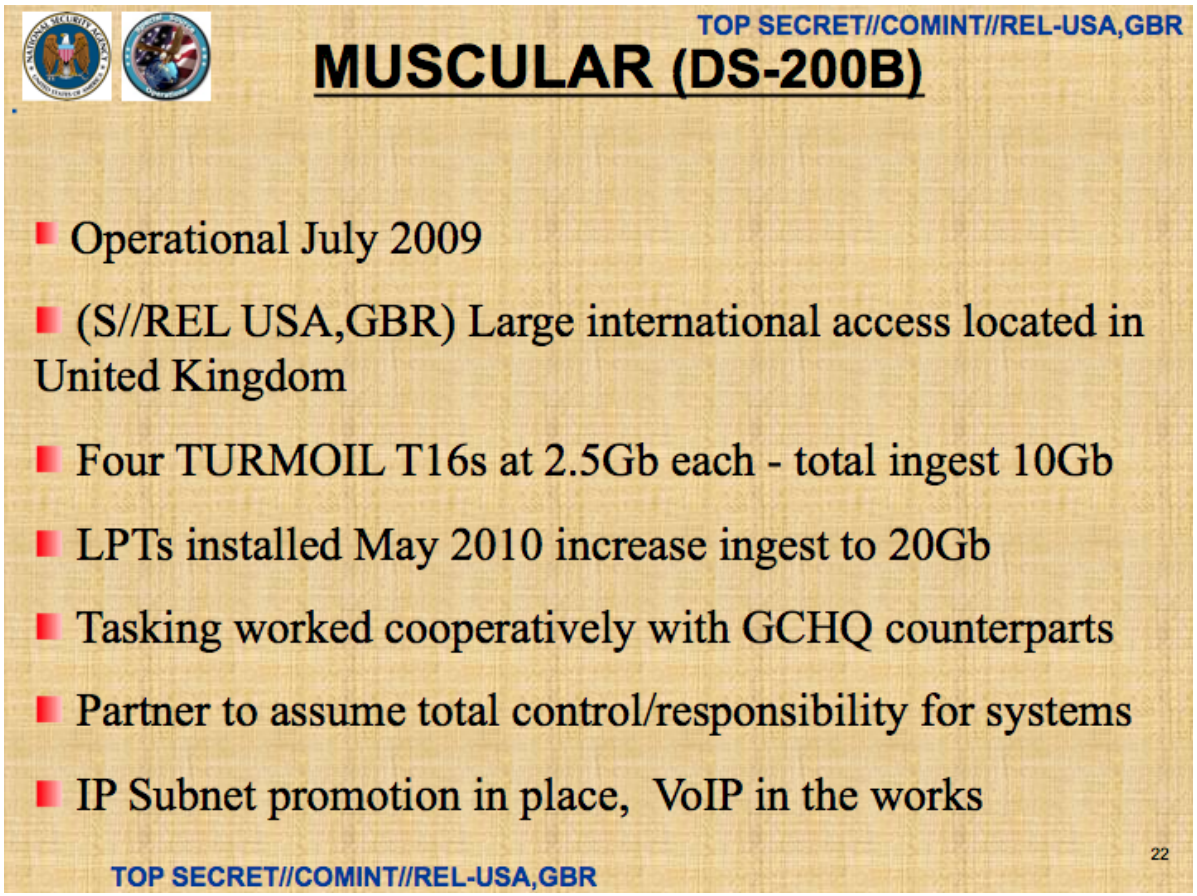


Abbildung : D-200 NSA Zugriff auf GCHQ Tempora Daten

Aufbereitung der Daten

- Die PRISM-Daten werden *fall-weise* (nach der Zustimmung des FISA-Gerichts) ermittelt und stellen somit spezifische Daten dar, die nur bei einem genügend grossen Anfangsverdacht genommen werden können.
  Als Fallbeispiel mag die *General Patraeus*-Affäre dienen.
- Damit überhaupt ein Anfangsverdacht 'gefunden' wird, muss ein konkretes Vorkommnis existieren, oder die vorliegenden Verbindungsdaten weisen darauf hin.
- Ein geeignetes Mittel ist die *Verschlagwortung* von möglichen Terror-Begriffen und deren *Entdeckung* im Internet-Datenverkehr:

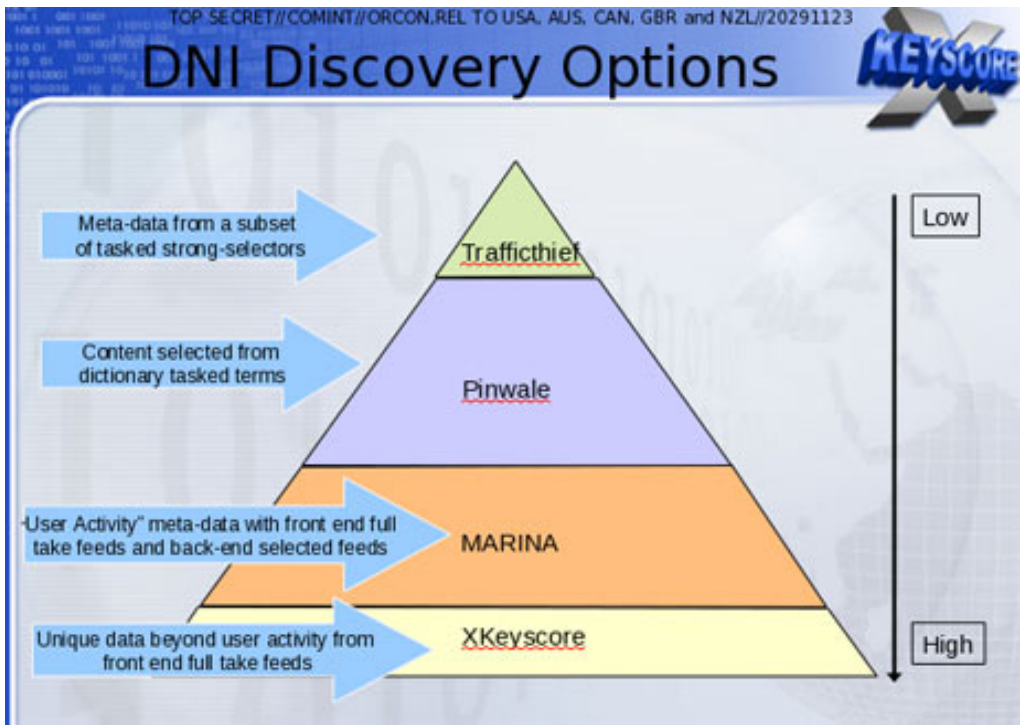


Abbildung : *Director of National Intelligence* DNI Auswertelogik

XKeyScore

XKeyscore ist ein Programm gemeinsam mit dem GCHQ. Grundsäulen:

- Aufbau einer Metadaten-Datenbank, die vom NSA und GCHQ zugänglich ist.
- Auswertung der *BigData* mittels fortgeschrittener *Graphen-Algorithmen*.
- Nutzung 'öffentlicher Dienste' wie Google-Maps zur Lokation von Subjekten.

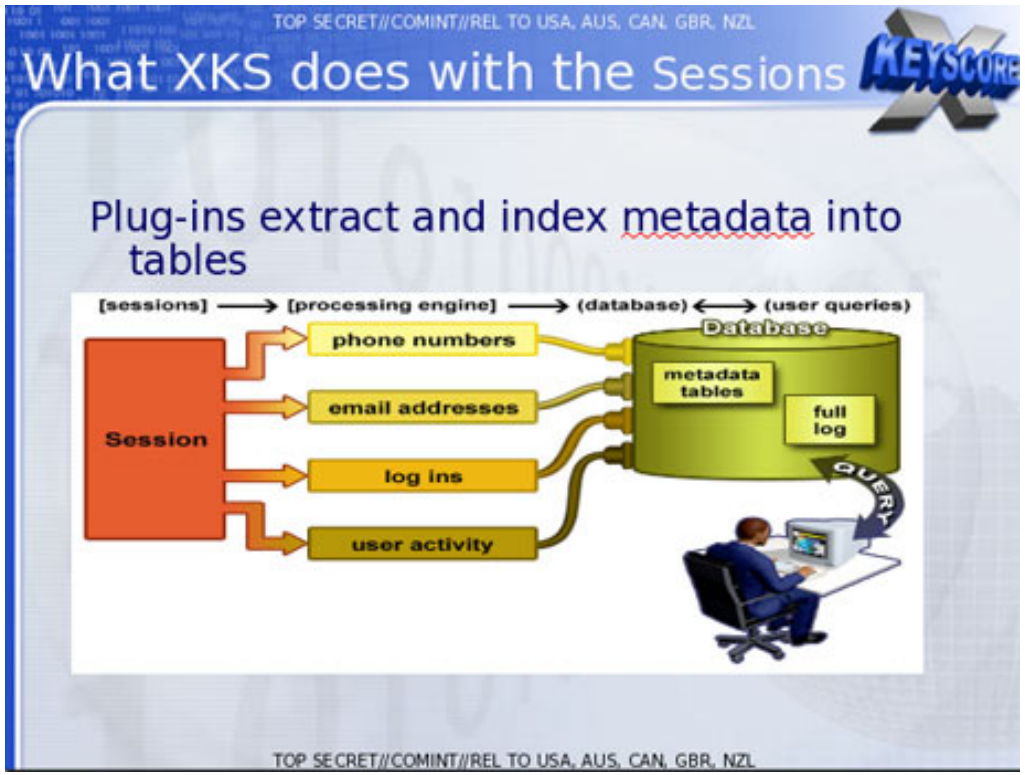


Abbildung : XKeyscore Metadaten-Verarbeitung

$\Longrightarrow$ Mittels eines *Selectors*, z.B. Email-Adressse, Telefon-Nummer können die Daten aufgerufen und die aufgezeichnete Internet-Konversation (Web-Zugriff, Voip, Skype) ausgewertet werden.

Brechen der Verschlüsslung

Grösstes Problem stellt das *entziffern* verschlüsselter Kommunikation (TLS, HTTPS, PGP) dar:

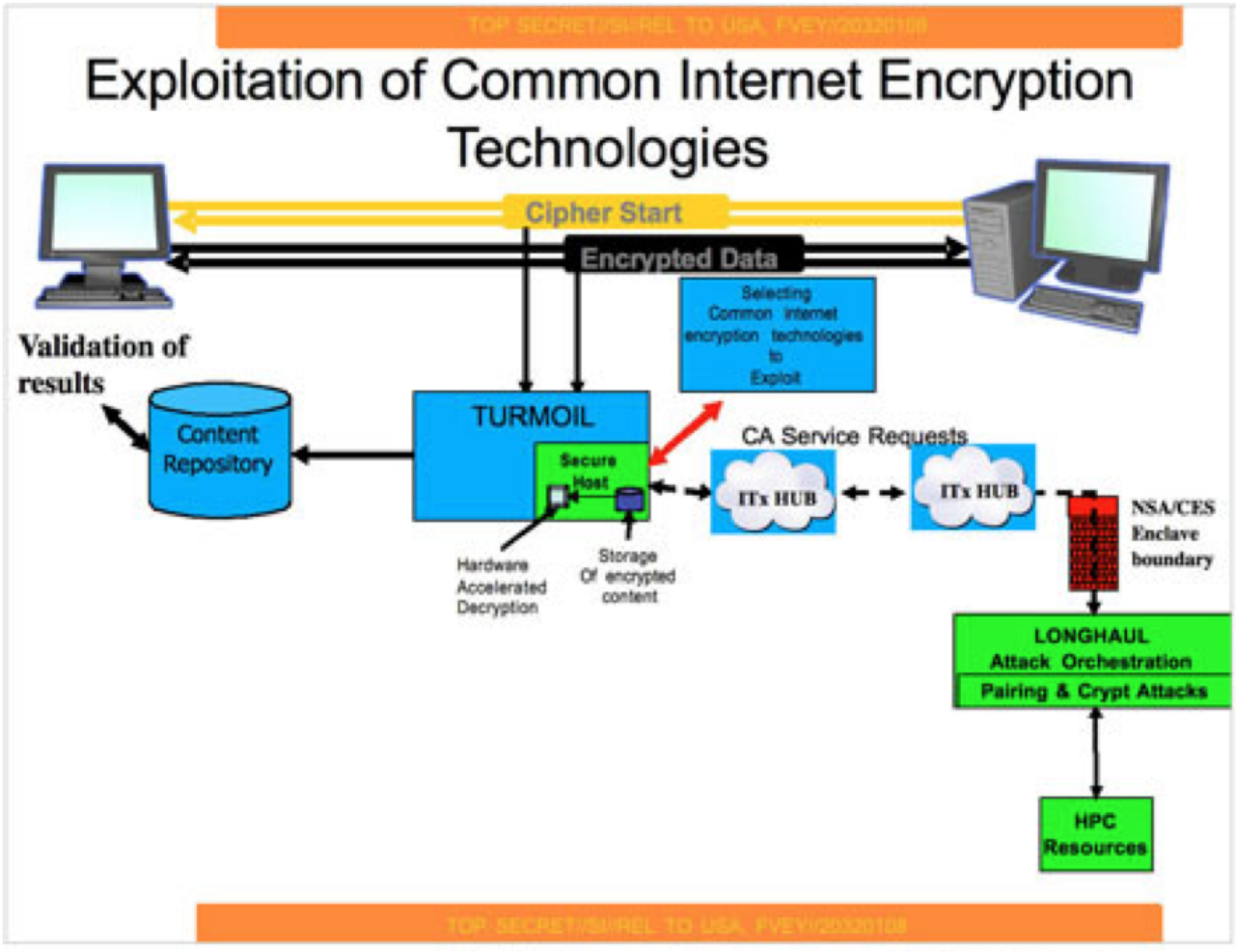


Abbildung : Brechen der TLS/HTTPS Verschlüsselung

Perfect Forward Secrecy – PFS

Bei der TLS-Verschlüsselung beginnt der Handshake

- entweder mit einem *fixen* RSA-Schlüssel, der von einer CA beglaubigt wurde,
- oder mit einem *ephemeralen* Schlüssel beim Diffie-Hellman Algorithmus.
  $\Longrightarrow$ Dies ist als *Perfect Forward Secrecy* bekannt geworden.

Ist speziell der RSA-Schlüssel einmal gebrochen, können alle nachfolgenden Sessions entschlüsselt werden, auch wenn der eigentliche *Session Key* ephermal gebildet wird: Die Schlüsselbildung geschieht mittels einer *Pseudo Random Function* deterministisch.

Zum Brechen *starker Verschlüsselung* wird das **BULLRUN** Programm eingesetzt:

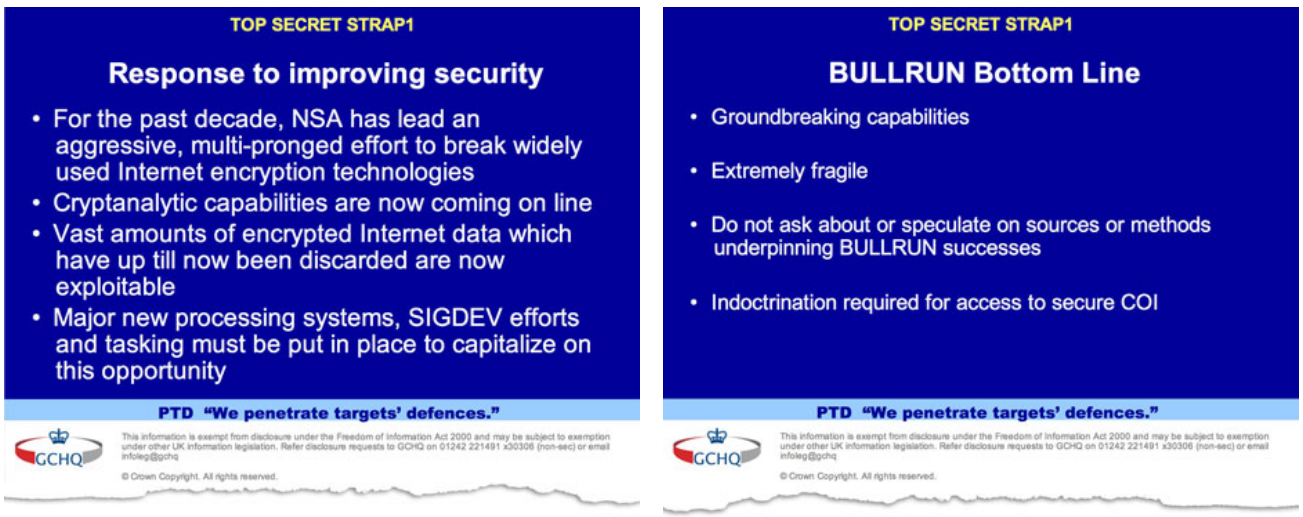


Abbildung : Aufgaben des BULLRUN Programms

BULLRUN: Cluster von Linux-Rechnern mit GPU-Acceleration zum 'Schlüsselknacken'.

Einbruch ins Google Netzwerk: Serendipity

Google nutzt zur Kommunikation seiner Rechenzentren untereinander sog. *Dark Fibers*. Das sind exklusiv angemietete LWL-Strecken bei den ISP. Der Datenaustausch hierüber wird nicht, z.B. per **IPsec** verschlüsselt, sondern es wird ein *Metadata*-Modell genutzt.

Das NSA-Programm *Serendipity* greift diese Daten (über die GCHQ) ab und ist in der Lage, diese zu entschlüsseln.

Google-Mitarbeiter Brandon Downey: *Fuck these guys.*

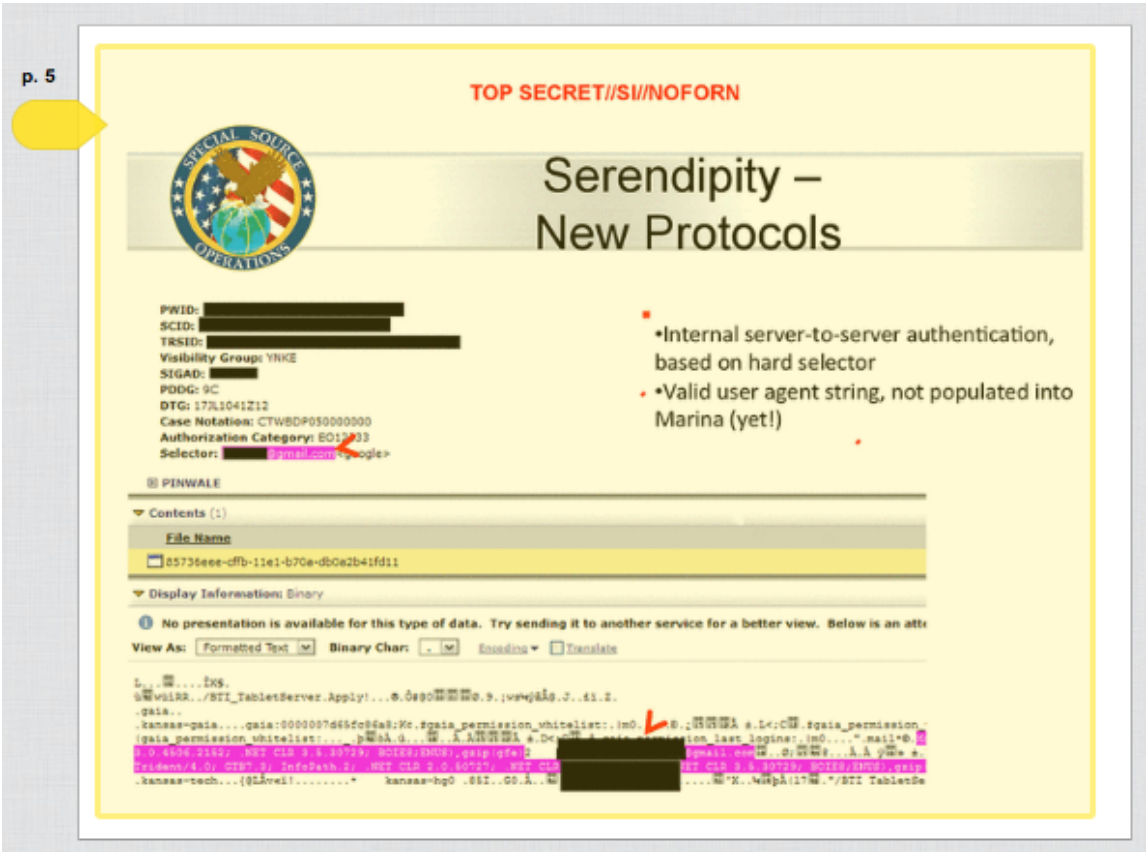


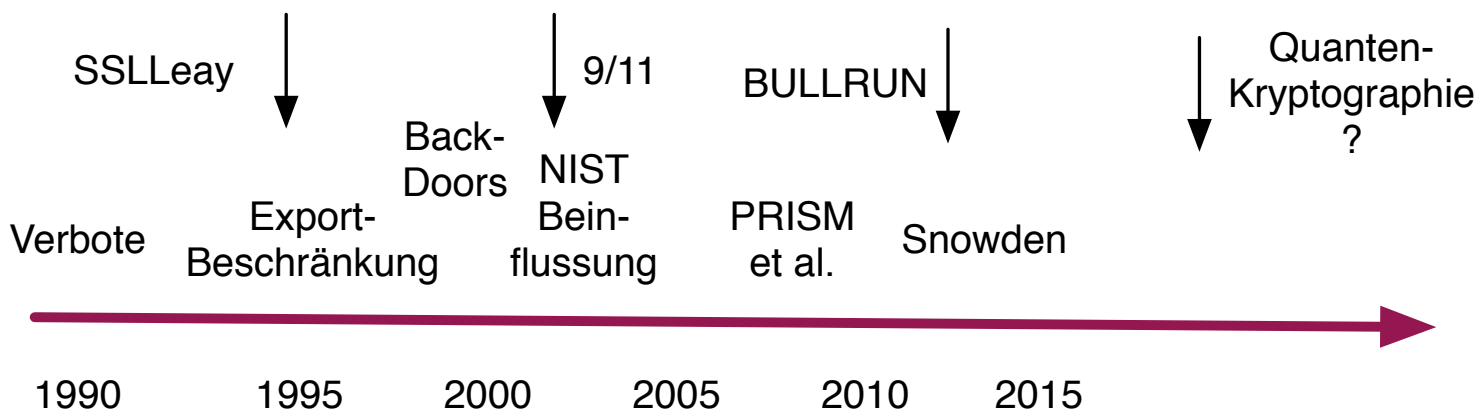
Abbildung : Zugriff auf die Google-Transferdaten

$\Longrightarrow$ Google hat mittlerweile seine Search-Request/Responses per HTTPS verschlüsselt und sucht derzeit nach Lösungen auch den Inter-RZ-Datenverkehr abzusichern.

Einfluss der NSA auf die Verschlüsselung

Der Einfluss der NSA auf die bestehende Verschlüsselungstechnik kann an mehreren Punkten festgemacht werden:

- Export-Verbot von starken Verschlüsselungs-Verfahren.
- Erzeugung von Hintertüren (Traps): Hinterlegung von 'geheimen' NSA-Schlüsseln in Produkten wie *Windows* und *Lotus Notes*.
- Manipulation zertifizierter Komponenten zur Schlüsselerzeugung, dass häufig die gleichen Zufalls- bzw. Primzahlen bei kryptographischen Operationen gewählt werden.
- Verbot von Kryptographie-Verfahren auf die die NSA keine Zugriffsmöglichkeit besitzt.
- Abschwächung von Kryptographie-Verfarhren, in dem die NIST-Standardisierung beeinflusst wird.



Verbot 'unabhängiger' Kryptographie-Methoden – Snuffle

Anfang der 90er Jahre erfand Dan Bernstein als Doktorand an der University of Berkeley '*Snuffel*':

- Eine Einweg-Hash-Funktion
- mit symmetrischer Verschlüsselung und 'Zero-Delay' ('The Snuffel Encryption System')

Sein Vorhaben war, diesen Algorithmus im Rahmen einer 'elektronischen Konferenz' in `sci.crypt` international bekannt zu machen. Nach einigen Konsultationen reichte er jedoch 1992 dieses Verfahren dem State Department zur Begutachtung ein. Die USA hatten zu dieser Zeit 'ihren Daumen' auf jeder Art von Verschlüsselungsverfahren, wie dies im 'International Traffic in Arms Regulations' (ITAR) formuliert ist.

$\Longrightarrow$ Der Export von Verschlüsselungsmethoden fällt daher unter die gleichen Regularien wie die Ausfuhr von Waffen selbst. Verstösse hiergegen werden mit $ 1 Million, 10 Jahren Haft und zivilrechtlicher Wiedergutmachung bestraft.

Dan Bernstein lehrt z.Z. an der TU Eindhoven und entwickelt neuerartige Verschlüsselungsverfarhren auf Grundlage der *Elliptic Curve Cryptography* ECC.

Export-Verbote für starke Verschlüsselungstechniken

Bis Anfang des ersten Jahrzehnts in diesem Millenium, versuchte der NSA 'starke' Kryptographie-Verfahren nur innerhalb der USA/Kanada zuzulassen.
Hierfür wurden speziell für die TLS-Verschlüsselung 'schwache' sog. *EXPORT* Schlüssel eingeführt. Der eigene fixe RSA-Key durfte z.B. nur einen geringe Länge von 512 bit besitzen.

$\Longrightarrow$ Bei TLS bzw. beim `mod_ssl` findet sich hierfür das Schlüsselwort: `AlgKey/UseKey`.

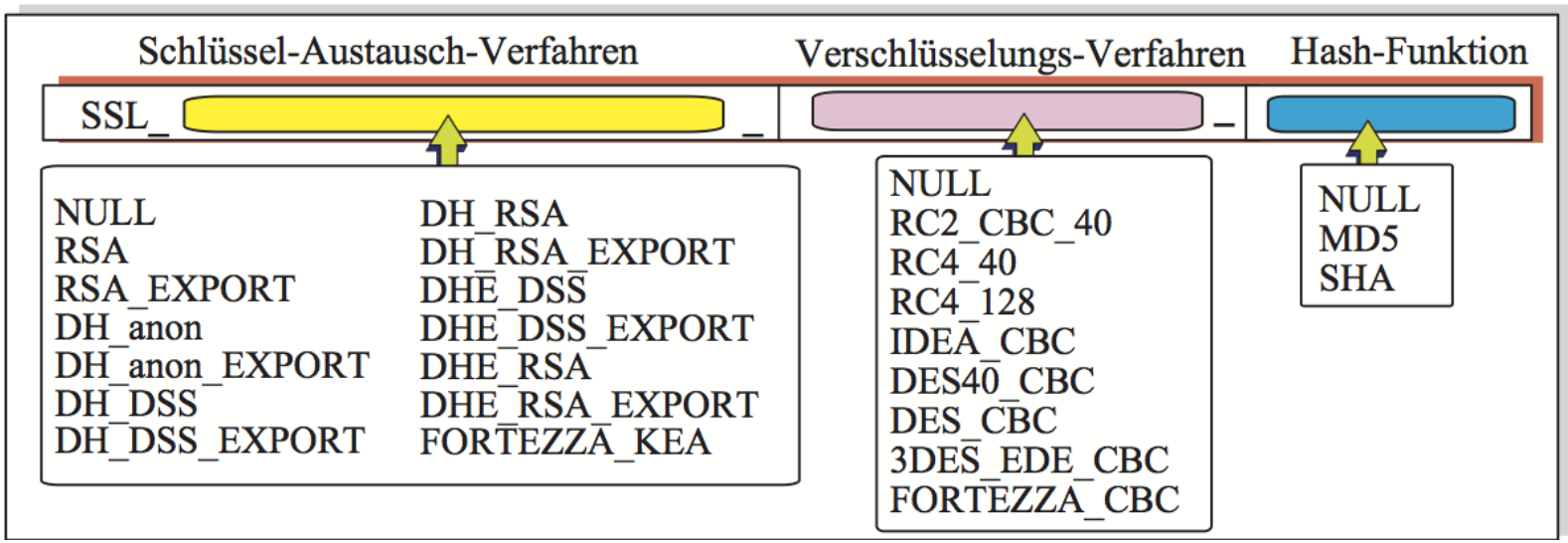


Abbildung : SSL mit Export-beschränkten Schlüsseln

Einbau NSA-genehmer Verfahren bei SSL: FORTEZZA

Eric Rescorla in seinem Buch über SSL und TLS (Seite 105):

> *"FORTEZZA was originally designed by the NSA to provide strong cryptography while allowing the NSA to intercept communications. The conflict between these goals was resolved by incorporating a key escrow feature into the device. Each card had its own key, which was escrowed with the NSA. Thus, when the NSA wished to decrypt a communication, it could recover the key for the card used to encrypt it, but the encryption would be secure against all other attacks."*

$\Longrightarrow$ FROTEZZA war für SSLv3 spezfiziert, aber später aus TLS entfernt.

Backdoors in Betriebssystemen

Telepolis 9.9.1999:

Ein unbedachter Fehler von Microsoft-Programmierern hat offengelegt, dass spezielle Zugriffscodes, die von der US-amerikanischen National Security Agency präpariert worden waren.

- *Sicherheitsspezialisten wissen seit zwei Jahren, dass im Standard-Treiber für Sicherheits- und Verschlüsselungsfunktionen von Windows unübliche Features enthalten sind. Der Treiber mit der Bezeichnung `ADVAPI.DLL` ermöglicht und kontrolliert eine ganze Reihe von Sicherheitsfunktionen. Windows-Nutzer können ihn im `C:\Windows\system` Verzeichnis finden.*
- *`ADVAPI.DLL` arbeitet eng mit dem Microsoft Internet Explorer zusammen, benutzt aber nur kryptographische Funktionen, die die amerikanische Regierung für den Export freigegeben hat. Diese Information enthält von Europa aus betrachtet eigentlich schon ausreichend schlechte Nachrichten.*
- *Inzwischen ist aber klar, dass `ADVAPI` spezielle Programme beinhaltet, die von der NSA dort installiert wurden und von ihr auch kontrolliert werden. Bis dato weiss niemand, welche Programme das sind, und was sie tun.*

'Aufweichungen' von Standards – Backdoors

NIST PRNG:

> *SP 800-90 specifies four different algorithms for securely generating pseudorandom numbers. Each of the four algorithms is based on a different cryptographic technique, on the basis that if the underlying technique is secure, then it makes sense to use that same technique in other applications where security is useful.*

`http://arstechnica.com/security/2013/09/the-nsas-work-to-make-crypto-worse-and-better/`

SHA-3 statt *Keccak*:

1. *The security level is "reduced": instead of offering 224-bit, 256-bit, 384-bit, and 512-bit versions of the hash (as found in the Keccak submission), the SHA-3 standard will only offer 128-bit and 256-bit versions.*
2. *Some of the internals of the algorithm have been tweaked by NIST.*

`https://docs.google.com/file/d/0BzRYQSHuuMYOQXdHWkRiZXlURVE/edit?pli=1`

Manipulation von Crypto-Hardware

RSA-Schlüssel zertifizierter Smartcards geknackt

- *Einem internationales Forscher-Team rund um Daniel J. Bernstein ist es gelungen, 184 RSA-Schlüssel mit 1024 Bit zu knacken.*
- *Diese wurden von Chip-Karten erstellt, die die taiwanische Regierung als digitale Bürger-Zertifikate ausgibt (Citizen Digital Certificate).*
- *Der Clou dabei: Die eingesetzten Smartcards waren offiziell zertifiziert – unter anderem gemäß Common Criteria durch das BSI und nach FIPS des amerikanischen NIST.*

Die Sicherheit von RSA beruht darauf, dass kein effizientes Verfahren bekannt ist, große Zahlen mit mehreren hundert Stellen effizient in ihre Primzahl-Faktoren zu zerlegen. Diese Komplexität reduziert sich dramatisch, wenn Schlüssel die gleichen Primzahl-Faktoren verwenden.

`http://www.heise.de/security/meldung/RSA-Schluessel-zertifizierter-Smartcards-geknackt-1959704.html`

NIST ECC-Kurven ?

- 'ECC Brainpool Standard Curves and Curve Generation version 1.0', 2005.10.19:

  'The choice of the seeds from which the curve parameters have been derived is not motivated leaving an essential part of the security analysis open.'

- Bruce Schneier, 'NSA surveillance: A guide to staying secure', The Guardian, 2013.09.06:

  'Prefer conventional discrete-log-based systems over elliptic-curve systems; the latter have constants that the NSA influences when they can.'

Kryptographische Verfahren bei Internet-Anwendungen

Im wesentlichen sind drei kryptographische Methoden bei den Internet-Anwendungen im Einsatz:

1. TLS für HTTPS, SMPTS, POP3S und IMAP4S sowie LDAPS. Hier finden immer die gleichen Algorithmen Anwendung; in der Regel auf Grundlage der OpenSSL oder GnuTLS Bibliotheken bzw. der Implementierung von Microsoft. Üblicherweise wird hier ein *Public Key Infrastruktur* PKI genutzt; was aber nicht zwingend ist.
2. SSH (Secure Shell), genutzt zum interaktiven Arbeiten, aber auch Dateien kopieren (scp, rsync) und als SSH-Proxy. Dies ist im wesentliche eine Peer-2-Peer Anwendung.
3. PGP (von Phil Zimmerman) für die Verschlüsselung von Email-Inhalten.

Applikationen wie OpenVPN und TOR nutzten die von diesen Implementierungen bereit gestellten SW-Bibliotheken.
$\Longrightarrow$ Es erscheint (mir) unwahrscheinlich, dass die starken kryptographischen Verfahren von SSH und PGP selbst von 'BULLRUN' gebrochen werden können.

- IPsec ist ein weiterer Vertreter, der im wesentlichen die gleichen Bibliotheken wie TLS einsetzt, aber das *Internet Key Exchange* Protokoll benötigt. IPsec kann für eine Verschlüsselung zwischen zwei IP-(End-)Knoten genutzt werden, z.B. als verschlüsselter VPN.

Sicherheit beim TLS-Verfahren

Beim TLS-Protokoll kann ein geneigter Mitleser die eingesetzten kryptographischen Verfahren aus der Verbindung entnehmen: Die TLS Cipher-Suite.

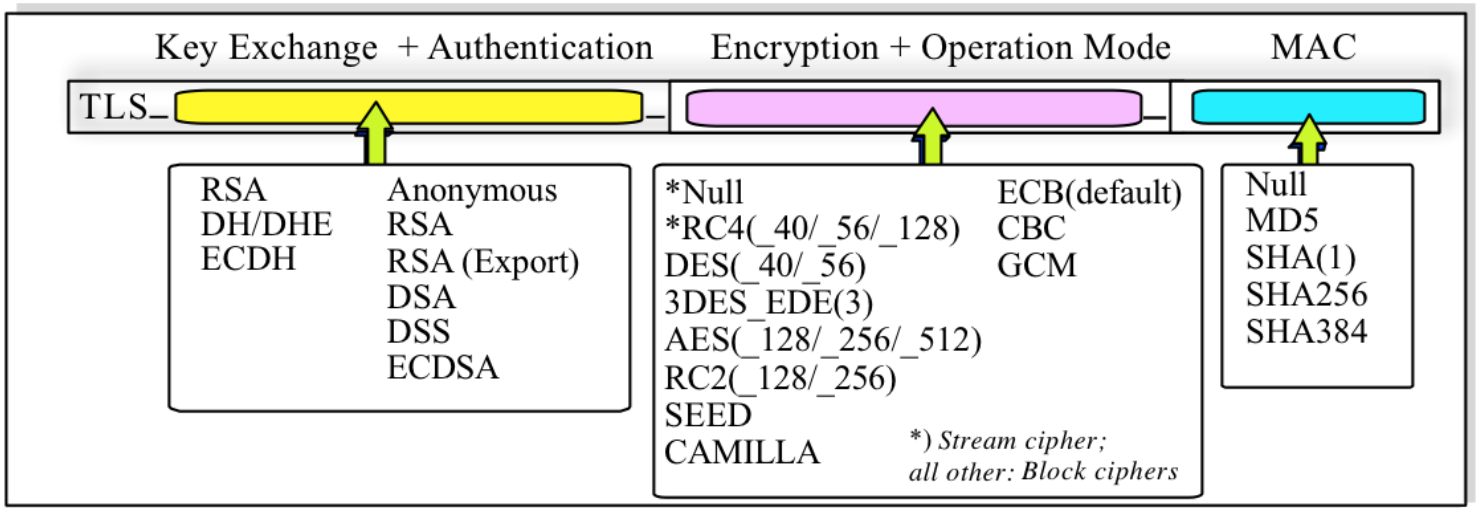
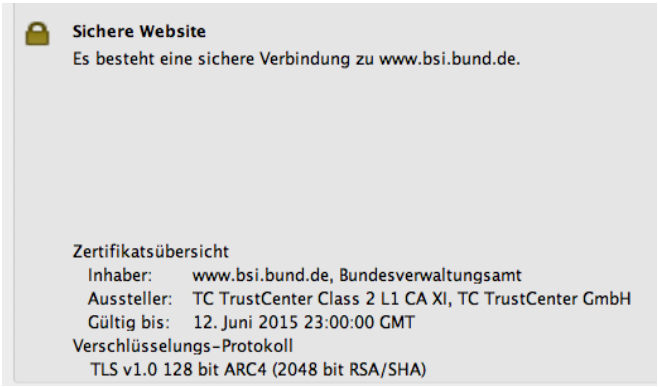


Abbildung : Aktuelle TLS Cipher-Suites

Aus den Verbindungsdaten kann folgendes ermittelt werden:

- Aus der Cipher-Suite: Die eingesetzten Verfahren.
- Die Version der genutzten SW (OpenSSL 0.9.8 beispielsweise).
- Den Beglaubiger (*Certificate Authority*) CA des Server-Zertifikates und dessen öffentlicher Schlüssel samt Verfahren.
- Aus dem Timing der TLS-Frames die 'Qualität' der ephemeralen Schlüssel bzw. des *Premaster-Secrets*.

Knacken der TLS-Verschlüsselung – Am Beispiel der BSI-Webseite



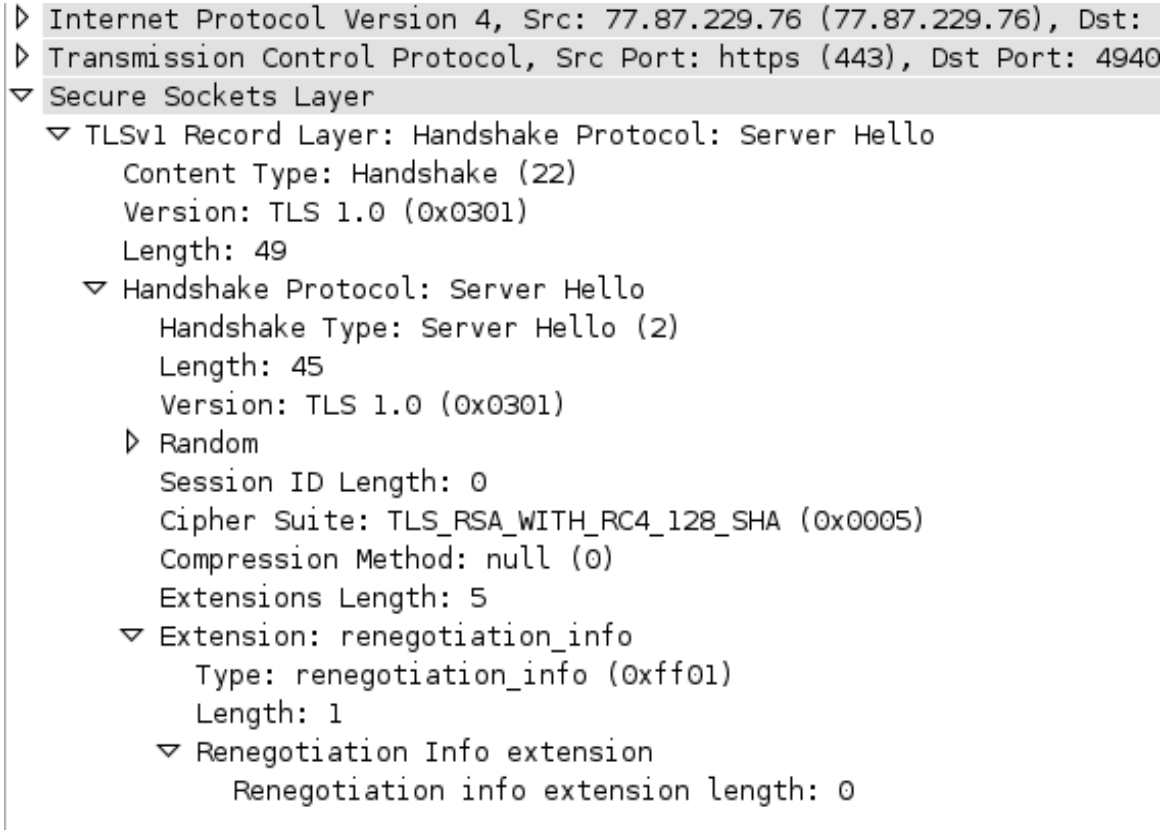


Abbildung : Die 'sichere' BSI-Webseite: `https://www.bsi.bund.de`

Meine Verbindungsdaten und mein Surfverhalten

Durch die HTTPS Verschlüsselung macht Google nun die Entschlüsselung der Anfrage und die Antwort für die NSA schwieriger.
Die Antwort gibt aber in der Regel eine URL mit der Quelle zurück:

- Liegt die URL auf einem Standard HTTP-Server, kann aus der übertragenen URL mittelbar auf die Frage geschlossen werden.
- Liegt die URL auf einem HTTPS-Server, ist zumindest das Zielsystem bekannt.

$\Longrightarrow$ Zudem verraten die DNS Query/Responses unseren Verbindungswunsch.
DNSSEC verschlüssselt – entgegen seinem Namen – die DNS Anfragen/Antworten nicht, sondern 'macht sie nur authentisch'.

Alternativen: Bernstein's CurveDNS und CurveCP

Die (mir bekannte) einzig gangbare Alternative einer offenen, aber vertraulichen Internet-Nutzen liegt mittels

- CurveDNS (verschlüsselte DNS-Kommunikation) und
- CurveCP (verschlüsselte Ende-zu-Ende IP-Kommunikation)

vor. Diese Protokolle bieten auf Grundlage von Elliptischen Kurven (die speziell ausgwählt und stärker als die des NIST sind) eine *Transportverschlüsselung* der IP-Pakete, ohne komplexe Protokolle wie IPsec zu bemühen.

$\Longrightarrow$ Bernstein liefert eine schnelle und kryptographisch starke SW-Bibliothek in Form des NaCl mit.

- `http://dnscurve.org/`
- `http://curvedns.on2it.net/`
- `http://curvecp.org/`
- `http://nacl.cr.yp.to/`

Fragen ?? Anwerkungen ?? Widerspruch ??

Vielen Dank für Ihre Aufmerksamkeit !

Fragen ?
Anmerkungen ?
Widerspruch ?

Weiterführende Links – 1

Glasfaser-Tapping:

- http://www.heise.de/tr/artikel/Warum-das-Netz-zusammenbrach-274898.html
- http://www.spiegel.de/netzwelt/tech/internet-seekabel-vierter-netzausfall-naehrt-verschwoerungs-theorien-a-533html
- http://www.japantimes.co.jp/news/2013/10/27/world/nsa-asked-japan-to-tap-regionwide-fiber-optic-cables-in-2011/
- http://www.spiegel.de/netzwelt/web/aegypten-taucher-wollten-offenbar-internetkabel-kappen-a-891386.html

Wikipedia:

- http://en.wikipedia.org/wiki/USS_Jimmy_Carter_(SSN-23)
- http://en.wikipedia.org/wiki/XKeyscore
- http://en.wikipedia.org/wiki/SIGINT_Activity_Designator#Joint_Base_SIGADs
- http://en.wikipedia.org/wiki/UKUSA_Agreement
- http://en.wikipedia.org/wiki/Tempora
- http://en.wikipedia.org/wiki/2013_global_surveillance_disclosures
- http://de.wikipedia.org/wiki/Ueberwachungs-_und_Spionageaffaere_2013

Weiterführende Links – 2

Rechtliche Grundlagen des 'Anzapfens':

- https://ssd.eff.org/foreign/fisa
- https://www.fas.org/irp/agency/doj/fisa/
- http://en.wikipedia.org/wiki/John_Michael_McConnell
- http://en.wikipedia.org/wiki/FISA
- http://en.wikipedia.org/wiki/National_Security_Letter
- http://www.cisco.com/en/US/docs/routers/7600/ios/12.2SR/configuration/lawful_intercept/76LIch1.html
- http://cryptome.org/spook-wishlist.htm

PRISM, NSA+GCHQ:

- https://netzpolitik.org/2013/wer-kooperiert-mit-der-nsa-neue-dokumente-lassen-umfassende-zusammenarbeit
- http://www.linkedin.com/pub/michael-foster/62/812/864
- http://www.guardian.co.uk/commentisfree/2013/jun/14/nsa-partisanship-propaganda-prism
- http://www.cbsnews.com/8301-205_162-57589797/yahoo-says-it-received-up-to-13000-data-requests/
- http://www.businessinsider.com/cnet-story-wiretapping-shot-dni-statement-james-clapper-2013-6
- http://www.dni.gov/index.php