# Inside NSA

## NSA Surveillance aus Prozesssicht

Erwin Hoffmann

FEHCom

**CHAOS COLOGNE**
*Edge of Control*

Köln 17. Mai 2015 (public)

# About Me:

- **Name**: Erwin Hoffmann
- **Beruf**: Diplom-Physiker
- **Tätigkeit**: Professor für Informatik an der Provadis Hochschule Frankfurt/Main
- **Internet**: Von den ersten Stunden an; Autor verschiedener Bücher ('Technik der IP-Netze')
- **CCC**: ?? Unix-affin, D.J. Bernstein-Weiterentwickler (public domain)
- **Web**: `http://www.fehcom.de`
- **Blog**: `https://www.fehcom.net/diary`
- **Mail**: `mailto:feh@fehcom.de` PGP Key-Id: 7E4034BE

# Inside NSA


- Was sind die *Aufgaben* der NSA und wie ist deren *Organisationsstruktur*?
- Welche rechtlichen Grundlagen (*Compliance*) liegen der NSA Überwachung zugrunde?
- Worin besteht das NSA *Portfolio* und wie kann es genutzt werden?
- Was versteht die NSA unter 'Selectors', 'Tasking' und 'Enabling' innerhalb von *Operationen*?
- Welche *Prozess-Kennzahlen* sind für die NSA bekannt?

# Aufgaben der NSA

# Aufgaben der NSA

Laut Wikipedia[1], besitzt die National Security Agency folgende Aufgaben:

> *The National Security Agency (NSA) is a U.S. intelligence agency responsible for global monitoring, collection, decoding, translation and analysis of information and data for foreign intelligence and counterintelligence purposes – a discipline known as* **Signals intelligence** *(SIGINT). The agency is authorized to accomplish its mission through clandestine means, among which are* **bugging electronic systems** *and allegedly engaging in* **sabotage through subversive software**.

Neben der NSA verfügen die USA über die Aufklärungsdienste (*National Intelligence*):

- *Defense Intelligence Agency* (**DIA**[2]) – Militärische Aufklärung.
- *Central Intelligence Agency* (**CIA**[3]) – Auslandsspionage.

Koordiniert werden diese Dienste durch das *Office of the Director of National Intelligence* (**ODNI**), dem z.Z. *James Clapper* vorsteht.

↪ Die NSA betreibt ihre Aufklärung nicht durch *Spione* (wie der CIA), sondern durch *technische Aufklärung* (*Intelligence* = Nachrichtendienst).

Gemeinsames Budget dieser Dienste (2013) beträgt ≈ 52,6 ... 80 Mrd. US $ pa.

[1] http://en.wikipedia.org/wiki/National_Security_Agency
[2] http://en.wikipedia.org/wiki/Defense_Intelligence_Agency
[3] http://en.wikipedia.org/wiki/Central_Intelligence_Agency

# 9/11: CIA's Peral Harbor

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 Anschluss hieran,

- wurden die Programme der NSA und CIA wurden neu geordnet,
- ein NSA 'CyberCommand' eingerichtet und dies
- mit den engsten Verbündeten ('five eyes' `FVEY` *Tier 1*) gemeinsam betrieben.

$\Longrightarrow$ Die FVEY[4] umfassen die Nachrichtendienste von Kanada, Australien, Neu Seeland und Groß-Britannien.

[4] `http://en.wikipedia.org/wiki/Five_Eyes`

# Aufbau-Organisation der NSA

# Führungsstruktur der NSA

Federführend bei der NSA ist der *Director of the National Security Agency* (DIRNSA) mit den (militärischen) Verantwortlichkeiten:

- *Chief of the Central Security Service* (CHCSS)
- *Commander of the United States Cyber Command* (USCYBERCOM)


The Central Security Service (CSS) provides timely and accurate cryptologic support, knowledge, and assistance to the military cryptologic community[5].

[5] https://www.nsa.gov/about/central_security_service/

# Organisationsstruktur der NSA

Die NSA verfügt über mehrere, mit Buchstaben bezeichnete Hauptabteilungen. Fachabteilungen werden in der Regel mit Nummern geführt. Die für den Aufklärungsdienst wichtigsten sind:

- `F(6)`: *Special Collection Service* (SCS) gemeinsam mit der CIA.
- `J(2)` *Cryptologic Intelligence Unit*
- `S`: *Signals Intelligence Directorate* (SID) mit folgenden Fachabteilungen:
  - `SA`: *Legal Interception*
  - `S1`: *Customer Relations*
  - `S2`: *Analysis and Production Centers* für spezielle Länder und Aufgaben:
    - `S2F/ICN`: S2 *Foreign/Intelligence Community Network*
  - `S3`: *Data Acquisition* mit den Unterabteilungen:
    - `S31`: *Cryptanalysis and Exploitation Services* (CES)
    - `S32`: *Tailored Access Operations* (TAO) – Hackertruppe.
    - `S33`: *Global Access Operations* (GAO)
    - `S34`: *Collections Strategies and Requirements Center*
    - `S35`: *Special Source Operations* (SSO)

$\hookrightarrow$ Innerhalb dieser Fachabteilungen werden spezielle NSA Programme (mit Kunstnamen wie PRISM) entwickelt, die zielgerichtete Aufgabenstellungen realisieren.

# Cyber Command

Nach dem 11. September 2001 (9/11) wurden die Dienste neu aufgestellt und

- Das Ministerium *Department of Homeland Security* (DHS) [6] wurde gegründet, sowie
- ein Dienste-übergreifendes *Cyber Command* [7] eingerichtet, und
- die Befugnisse der FISA für 'Anlass-lose Überwachung' ausgedehnt.

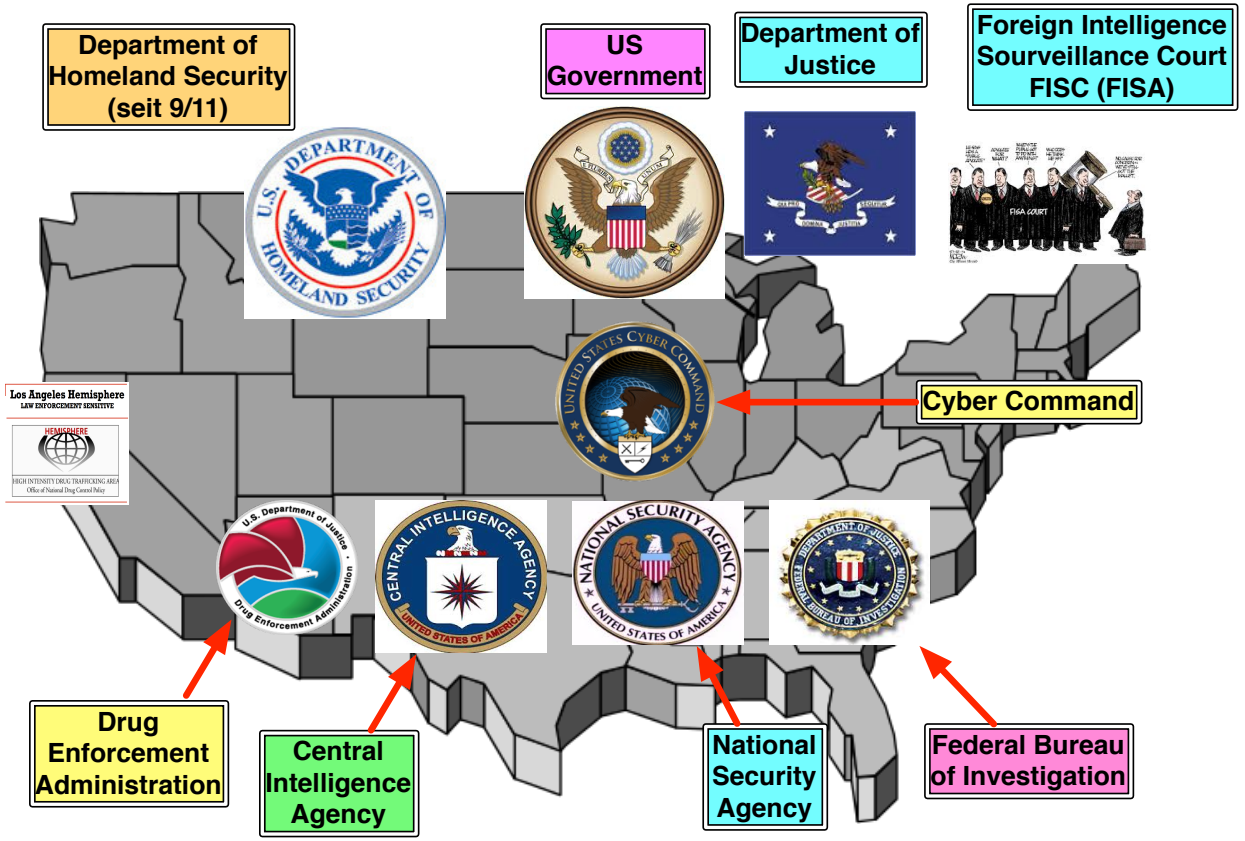


**Abbildung :** High-Level Organisationsstrukturen für das US Cyber Command

[6] http://en.wikipedia.org/wiki/Homeland_security

[7] http://en.wikipedia.org/wiki/United_States_Cyber_Command

# Der NSA Krake

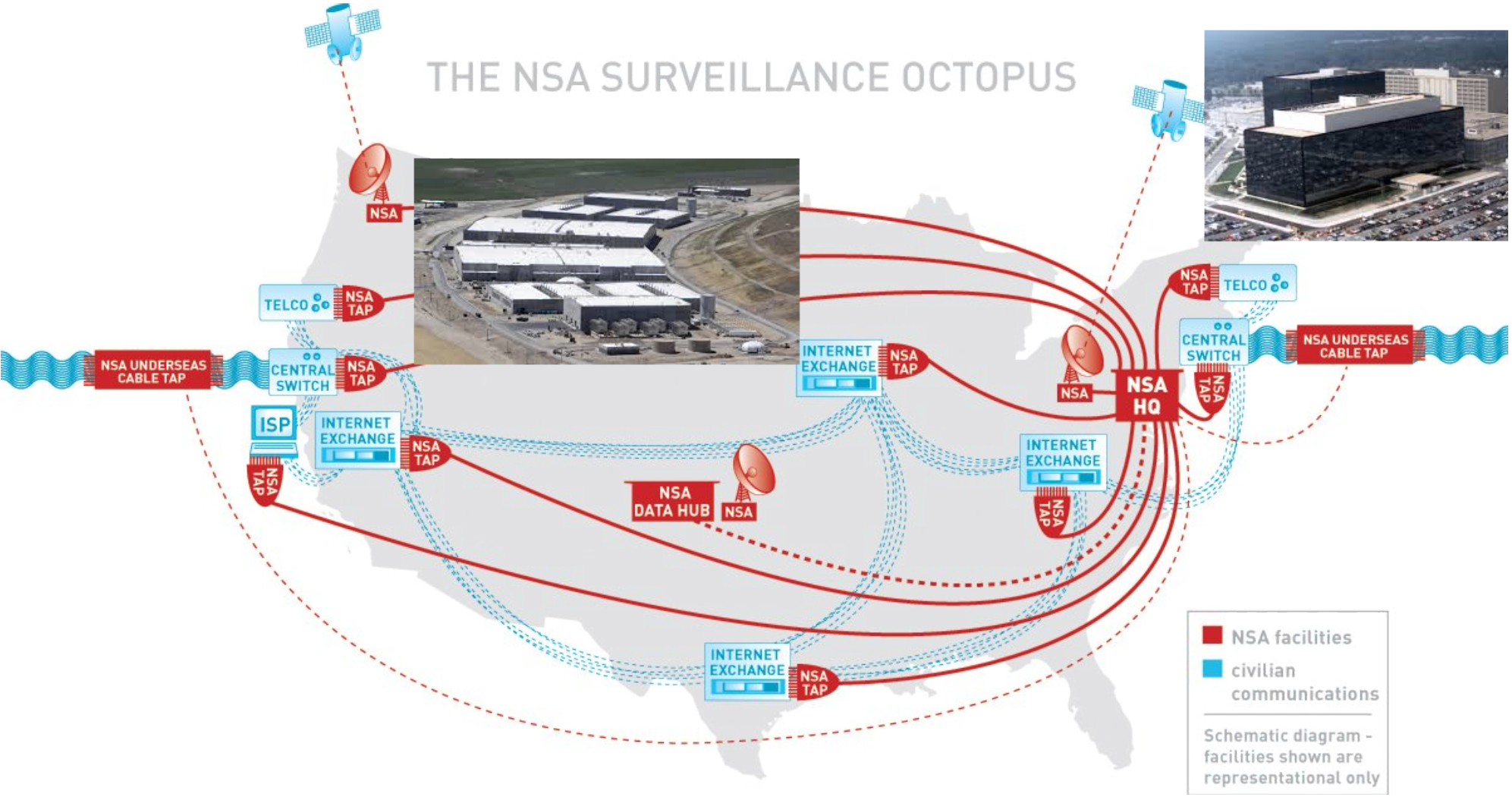


**Abbildung :** NSA Internet tapping `http://www.pacificviews.org/weblog/archives/017425.php`

# NSA Kommandozentrale

**Abbildung :** NSA Command Office (Maryland)

# Rechtsgrundlagen der NSA-Aktivitäten

# Rechtsgrundlagen der USA für die Überwachung

- *First Amendment* der US-Verfassung,
  das die freie Sprache in der Öffentlichkeit gewährleistet[8]. Dies gilt nur für US-Bürger.
- *Foreign Intelligence Surveillance Act* von 1978 (FISA) (Jimmy Carter) und ergänzt um die 'verdachtslose Überwachung' von George W. Bush in 2001[9].
- Patriot Act (George W. Bush):
  *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act* von 2001[10].

↪ Im Rahmen der FISA Gesetzgebung wurde ein geheim tagender FISA Gerichtshof (FISC) mit 11 Richtern eingerichtet, dessen Rechtssprüche ebenfalls geheim sind[11].

Für US-Bürger kann der FBI sog. *National Security Letter* (**NSL**) aussprechen, die sowohl zur Herausgabe der Daten zwingen und zudem, dass hierüber öffentlich nicht verlautbart werden darf. Ein Einspruch gegen die NSL ist nicht möglich[12].

[8] https://www.aclu.org/free-speech

[9] http://en.wikipedia.org/wiki/NSA_warrantless_surveillance_(2001\OT1\textendash07), http://en.wikipedia.org/wiki/Foreign_Intelligence_Surveillance_Act_of_1978_Amendments_Act_of_2008

[10] http://en.wikipedia.org/wiki/Patriot_Act

[11] http://en.wikipedia.org/wiki/United_States_Foreign_Intelligence_Surveillance_Court

[12] https://www.eff.org/issues/national-security-letters/faq/, http://lavabit.com/

# Patriot Act - Section 215

Mit dem Ergänzung 'Section 215' des Patriot Act wurde kurz nach 9/11 durch den *FISA Amendment Act* (FAA) folgendes ermöglicht[13]:

- FISA Anfragen an den FISA Court können nun gemacht werden, als Abwehrmassnahmen gegen den *Internationalen Terrorismus* oder falls *geheime nachrichtendienstliche Tätigkeiten* geschützt werden müssen.
- Diese Massnahmen können sich nicht nur gegen Personen richten, sondern gestatten auch eine *allgemeine Überwachung*.

[13] http://en.wikipedia.org/wiki/Foreign_Intelligence_Surveillance_Act_of_1978_Amendments_Act_of_2008

# Patriot Act - Section 702

Ein interessante Ergänzung ist die 'Section 702'[14] des Patriot Acts. Dies erlaubt es zunächst Personen aufgrund der Metadaten (Verbindungsdaten) ausfindig zu machen ('*targeting*'), sofern sie sich ausserhalb der US befinden:

> *Procedures for Targeting Certain Persons Outside the United States Other Than United States Persons:*
>
> - *This authority allows only the targeting, for foreign intelligence purposes, of communications of foreign persons who are located abroad.*
> - *The government may not target any U.S. person anywhere in the world under this authority, nor may it target a person outside of the U.S. if the purpose is to acquire information from a particular, known person inside the U.S.*
> - *There must be a valid, documented foreign intelligence purpose, such as counterterrorism, for each use of this authority. All targeting decisions must be documented in advance.*

[14] `http://fas.org/irp/news/2013/06/nsa-sect702.pdf`

# FISA Gerichtsbarkeit

## Aufgaben der FISA Gerichtsbarkeit

*FISA requires the government to get search warrants and wiretap orders from a court even when it is investigating foreign threats to national security. However, the FISA process is different from the law enforcement processes described in earlier sections.*

## Der FISA Secret Court[15]

*First, all government requests for foreign intelligence surveillance authorization are made to a secret court: the FISA court. In order to get authorization, a significant purpose of the surveillance must be to gather foreign intelligence information — information about foreign spies, foreign terrorists, and other foreign threats — instead of evidence of a crime.*

[15] https://www.fas.org/irp/agency/doj/fisa/

# National Security Letters

Die *National Security Letters* (NSL) stellen eine Zwangsvorladung (*subpoena*) das ursprünglich 1978 im Zuge illegaler Finanztransaktionen einführt wurde, aber im Zuge des Patriot Act in 2001 erweitert wurde, "*to protect against international terrorism or clandestine intelligence activities*".

Das FBI kann einen NSL gegen eine Person oder eine Firma aussprechen, ohne eine richterliche Erlaubnis im Vorfeld einholen zu müssen. Im Zuge eines NSL brauchen nur Meta-Daten herausgerückt werden (z.B. E-Mail-Adresse). Andererseits kann mittels eines NSL verlangt werden, dass der Betroffene die Zustellung und die Auflagen des NSL nicht Dritten bekannt gemacht werden kann.

Quelle: `http://en.wikipedia.org/wiki/National_security_letter`

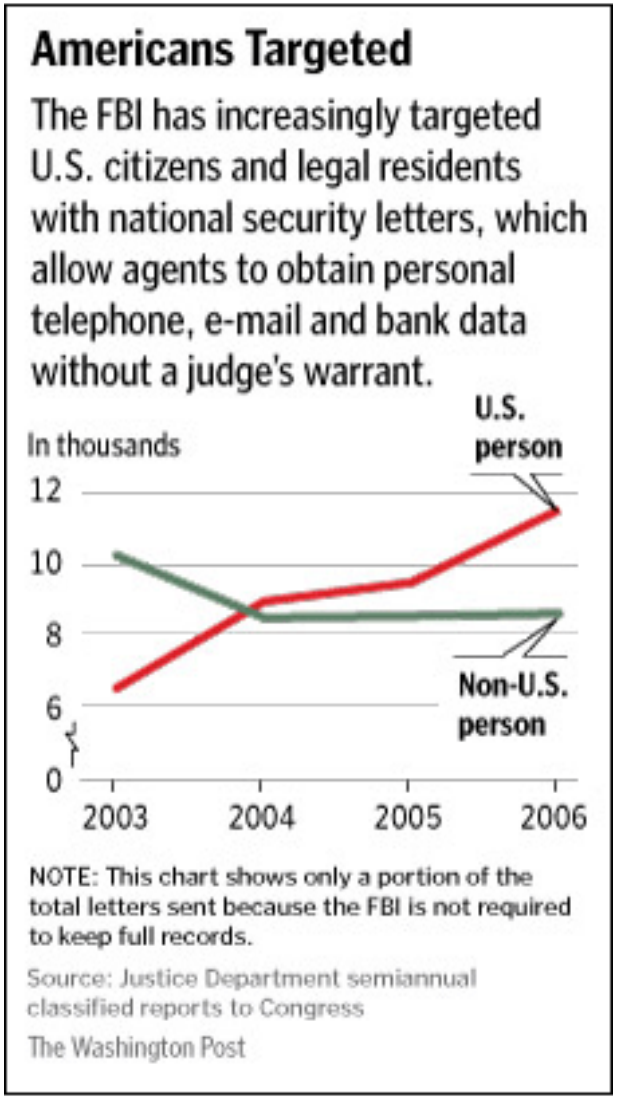


**Abbildung :** Anzahl der vom FBI ausgestellten NSL

# Ronald Reagan: Executive Order 12333

Ergänzt wird die FISA Gesetzgebung durch die von Ronald Reagan bereits am 4. Dezember 1981 in Kraft gesetzte

- 'Executive Order 12333'[16],
- die für die NSA quasi die Ausführungsbestimmungen ihrer Tätigkeit – also das mögliche Portfolio – beschreibt.

(U//~~FOUO~~) Executive Order 12333 was issued by the President of the United States to provide for the effective conduct of US intelligence activities and the protection of the rights of US persons. It is the primary source of NSA's foreign intelligence-gathering authority.

(U) NSA conducts the majority of its SIGINT activities solely pursuant to the authority provided by Executive Order (EO) 12333.

**Abbildung :** Interpretation der 'Executive Order 12333'

[16] https://www.aclu.org/files/assets/eo12333/NSA/Legal%20Fact%20Sheet%20Executive%20Order%2012333.pdf#page=1

# IT- und Datenschutz: Das Verständnis der USA

Das US-amerikanische Verständnis über Datenschutz und IT-Sicherheit unterscheidet sich grundlegend gegenüber Deutschem Recht[17]:

- **IT-Sicherheit**:
  IT-Sicherheit ist dann vorhanden, wenn sich die Daten bzw. IT-Systeme unter ausschliesslichem Zugriff der USA/NSA befinden.

- **Daten-Sicherheit**:
  Daten-Sicherheit liegt dann vor, wenn sich die Daten nicht nur im Zugriff, sondern auch unter Kontrolle der USA/NSA befinden.

> Generell gelten die Grundrechte der *US Constitution*
> im Kern immer nur für *US Citizens*.

↪ NSA Slogan: NOBUS – No one, but Us!

[17] http://media.ccc.de/browse/conferences/fiffkon/2014/fiffkon14_-_6526_-_de_-_saal_-_201411072015_-_nachrichtendienstliche_zugriffe_auf_telekommunikation_und_ikt-strukuren_und_ihre_implikationen_fur_individuelle_und_staatliche_souveranitat_-_andy_muller-maguhn.html#video

# Europäische 'Safe Harbor' Vorschriften

Innerhalb Europas gilt die 'Safe Harbor' Richtlinie: Persönliche Daten (Stammdaten) dürfen nicht an Länder ausserhalb der EU weitergegeben werden, die nicht die selben Sicherheits-Standards wie innerhalb der EU aufweisen[18].

↪ Für Firmen, wie *Google* und *Facebook* bedeutet das, dass die Account-Daten von Kunden, die Bürger der EU sind, unter anderen (schärferen) technischen Zugriffseinschränkungen zu halten sind, wie für Nicht-EU-Bürger, bzw. Bürger der USA.

Innerhalb der *Free-Trade* Verhandlungen zwischen den US und der US wird aber versucht, diese Einschränkungen zu verhindern[19].

[18] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:DE:NOT

[19] http://www.heise.de/newsticker/meldung/EU-Datenschutzreform-Klausel-gegen-NSA-Spionage-gestrichen-1887741.html

# NSA-Programme

# NSA Aufgabenbestimmung ... für Deutschland

Die NSA ist Bestandteil der Cyber Commands. Dessen Aufgaben reichen weit über die Spionage hinaus. Die Ziele für Deutschland lauten:


**Abbildung :** National Intelligence Priority Framework für Deutschland [Quelle: Constanze Kurz / CCC]

# NSA Programme

Ausgehend vom Anforderungsprofil der NSA entwickelt sich (natürlich nur auf gesetzlicher Grundlage)

- das NSA *Portfolio* – also die Menge an technischen Spionage, Sabotage und Überwachungsmöglichkeiten,
- die in *Programmen* organisiert sind. Die Programme sind nach den Spezifika der zu ermittelnden Informationen organisiert (Telefon-Mitschnitte, Internet-Daten, Meta-/Bewegungsdaten, ...),
- die in Form eines *Activity Designators* 'gezogen' werden können und für eine einzelne Person bzw. Institution (oder anderer Kriterien)
- mittels *Selectors* = **Fingerprints** (Telefon-Nummer, Email-Adresse ...) erfasst werden können und anschliessend
- in konkreten *Operationen* umgesetzt werden, wobei der Selector '*getaskt*' wird.

# NSA Cyber Command Programme

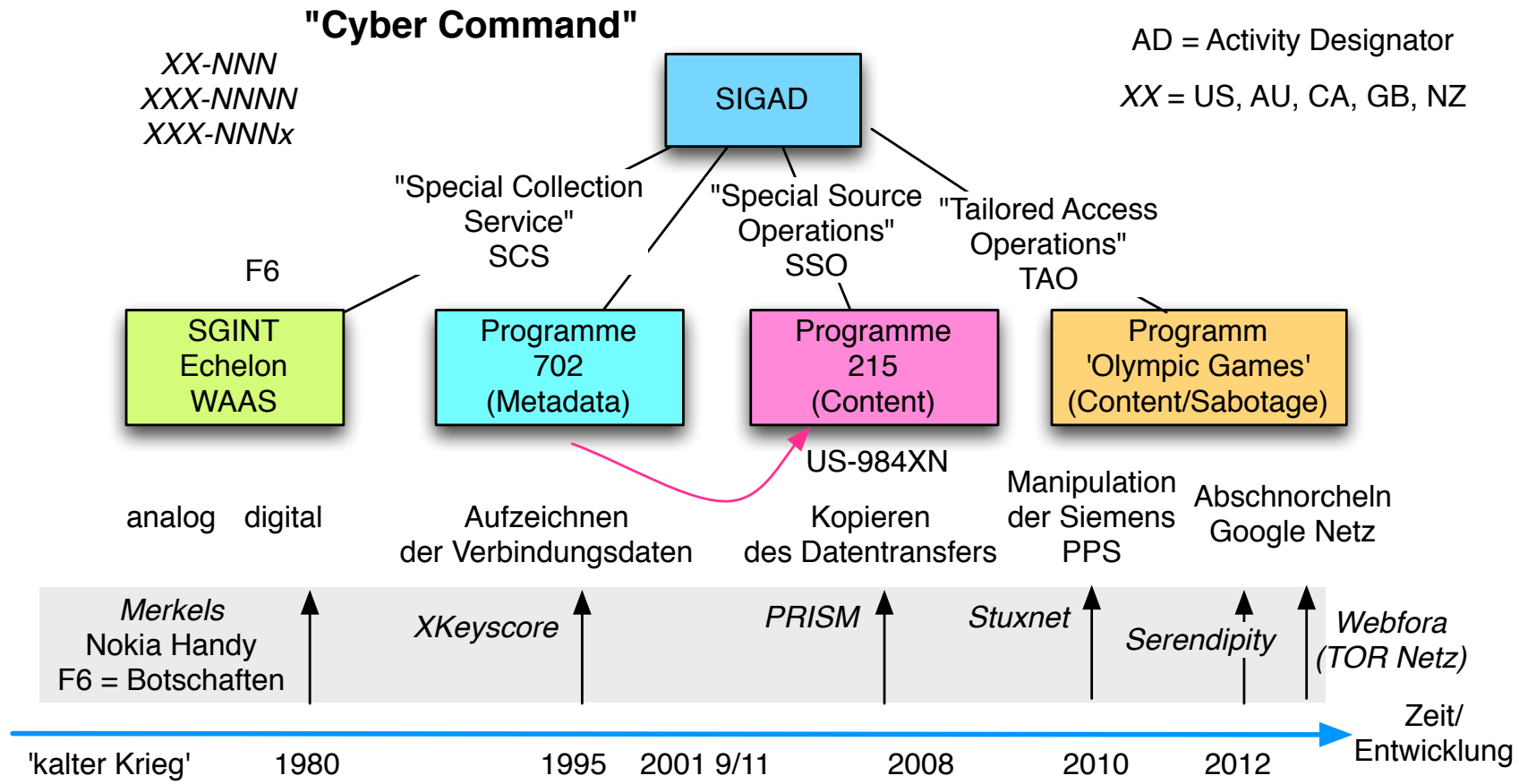


**Abbildung :** NSA Programme und ihre Entwicklung; WAAS: Wide Area Airborne Surveillance[20]

[20] http://www.academia.edu/9011629/Rise_of_Air_Force_Unmanned_Aircraft_Systems_UAS_

# NSA Programme zur Entnahme des Daten-Contents

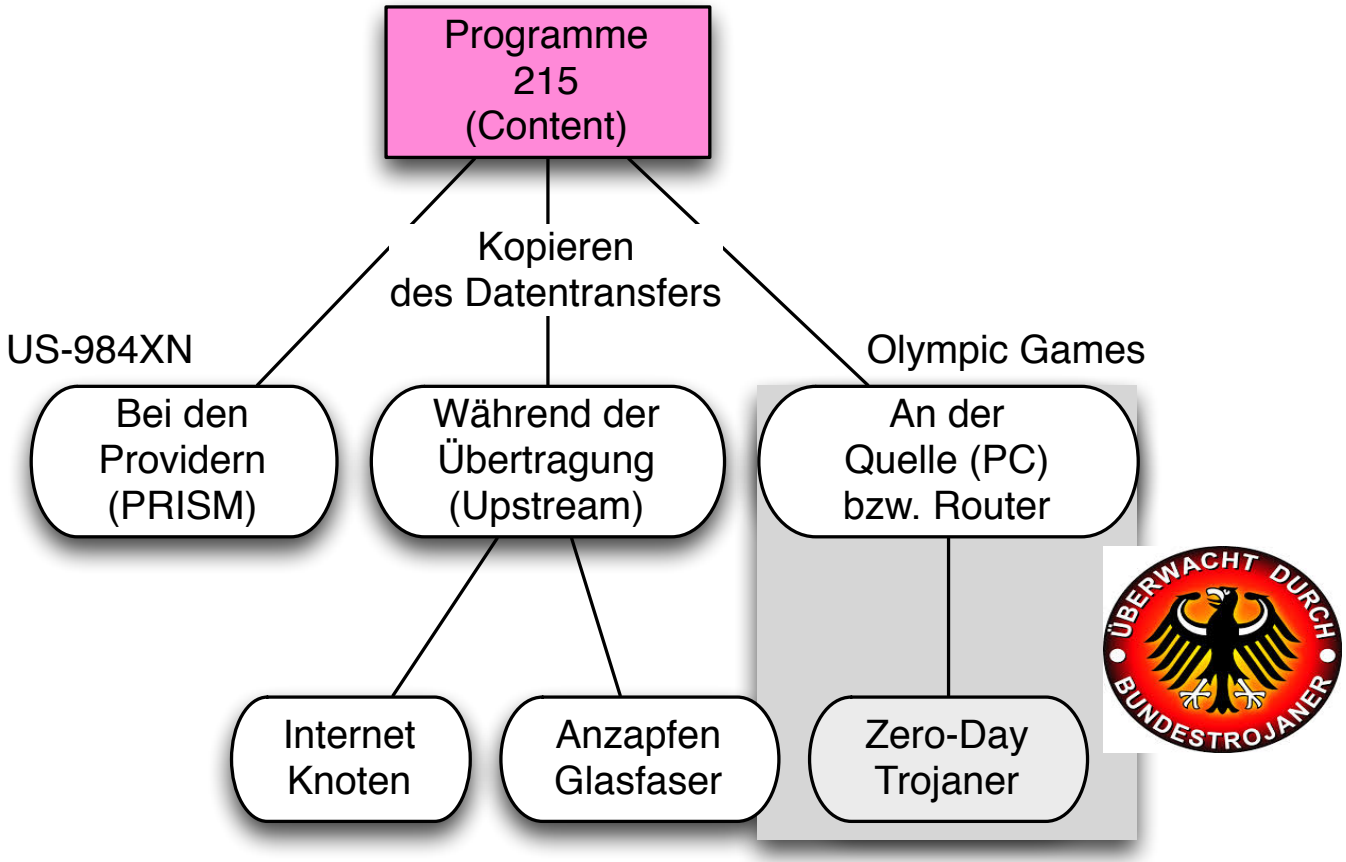


**Abbildung :** NSA Programme zur Absaugen von Daten-Verbindungen

# Special Source Operations – SSO

Unter die *Special Source Operations* (SSO) fallen alle die Aktivitäten, die Daten von Providern ausleiten, die unter US-Jurisdiktion fallen:

- Microsoft,
- Apple,
- Yahoo,
- Google,
- Facebook

↪ Diese Firmen können per NSL gezwungen werden, ihren Datenbestand zu öffnen und der NSA zur Verfügung zu stellen. Ferner sind die Unternehmen verpflichtet, ggf. *Private Keys* zum Entschlüsseln der Daten der NSA zu übergeben.

Ergänzende Unterprogramme:

- PRISM
- MARINA
- MAINWAY
- PINWALE
- NUCLEON

# Special Source Operations – Das PRISM Programm

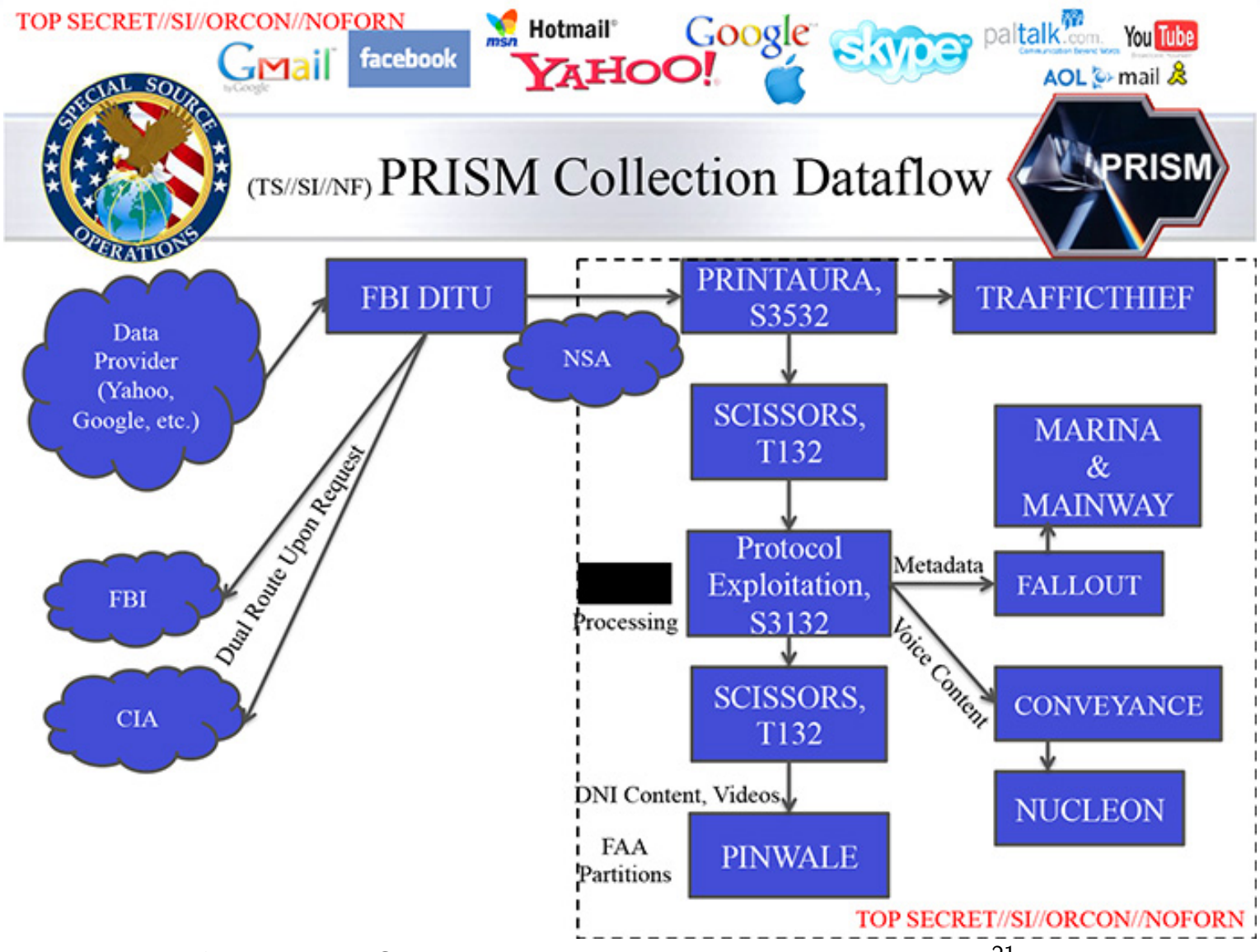


**Abbildung :** Datenfluss bei PRISM; DITU: Data Intercept Technology Unit[21]

[21] http://en.wikipedia.org/wiki/Data_Intercept_Technology_Unit

# Global Access Operations – GAO

Hierbei geht es um

- das weltweite Abgreifen (*Interception*) des Internet-Datenverkehrs und
- das Speichern der gesamten Daten bei der NSA.


**Abbildung :** Interception der Internet-Infrastruktur (gemeinsam mit GCHQ)

# SCS Lokationen

Der NSA *Special Collection Service* (SCS) arbeitet weltweit und im Verbund mit den FYES.

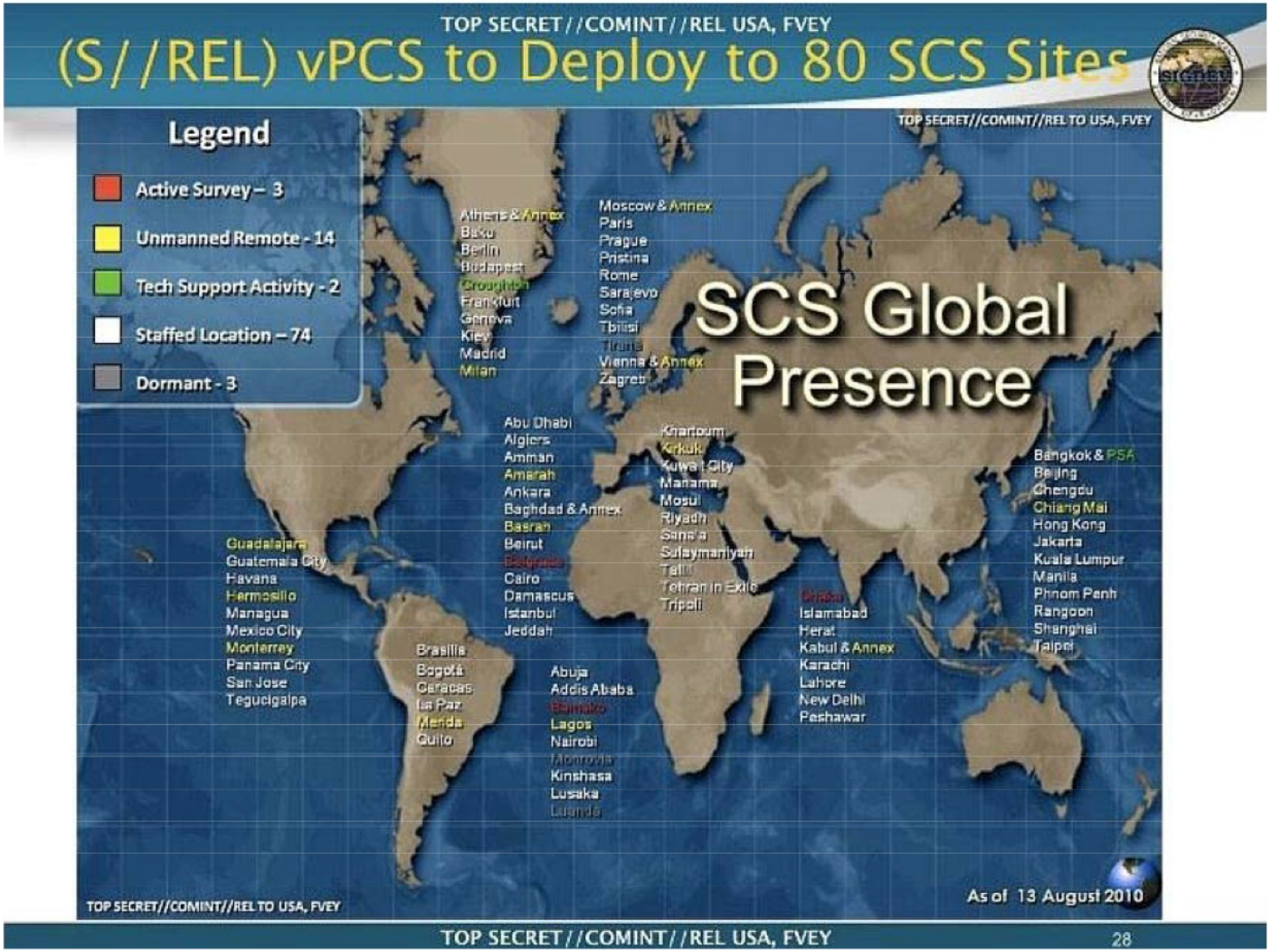


**Abbildung :** Weltweite Lokationen des NSA 'Special Collection Service'

# Tailored Access Operations – TAO

Die *Aufgaben*, die von der NSA realisiert werden ergeben sich aus ihrem *Auftrag* und den aktuellen weltpolitischen *Anforderungen*. Die TAO-Operationen umfassen

- Spionage und Überwachung sowie
- Sabotage.


**Abbildung :** Bericht des NSA TAO Teams in Texas

# NSA Prozesse

# NSA als Dienstleister

Die NSA ist Dienstleister für andere (US) Behörden:

- Weisse Haus
- US State Department
- US Office of Commerce
- US Department of Defence (DoD)
- Bundesnachrichtendienst (BND)

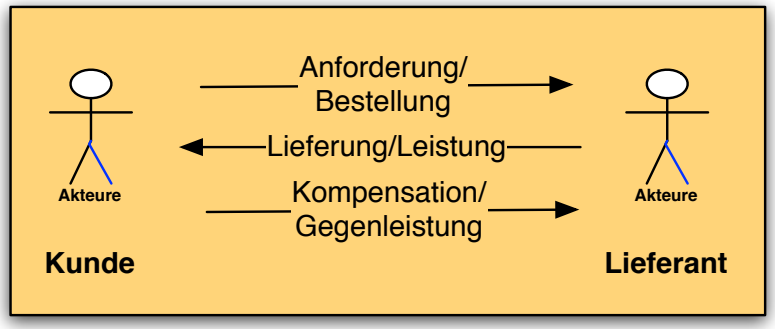


**Abbildung :** Der 'Geschäftsprozess' bei der NSA

↪ Ziel ist die Überwachung, Spionage aber auch Sabotage von IT-Systemen.

- Wirtschafts- und Industriespionage bei ausländischen Firmen.
- 'Strategische Aufklärung'.
- Bereitstellung von *Kompromant*[22] für unliebsame Personen und *Greymailing*.
- Sabotage und Manipulation von IT-Anlagen.

[22] http://de.wikipedia.org/wiki/Edathy-Affaere

# NSA Prozessstruktur

Die Prozessstruktur der NSA sieht im Grunde folgendermassen aus:

- Der Kunde bestellt eine Information (oder ggf. Aktion) für ein *Target*.
- Die NSA schaut nach, ob über Target hinreichende Informationen vorliegen bzw. gespeichert sein.
- Falls dies nicht der Fall ist, müssen neue 'Beschaffungsmodule' implementiert oder generiert werden.
- Die Informationen werden abgegriffen, bereinigt, verdichtet und dem Kunden geliefert.

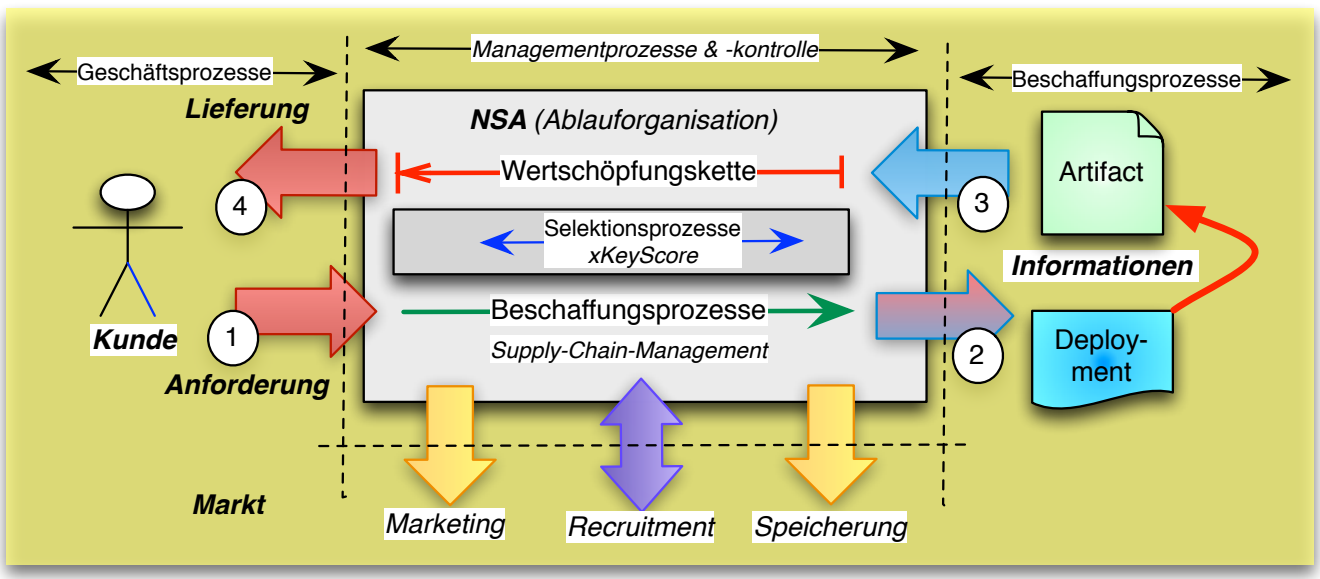


**Abbildung :** Grundlegende NSA-Prozesse

↪ Der Kompensationsprozess ist unklar.

# NSA Angebots- und 'Wertschöpfungsprozesse'

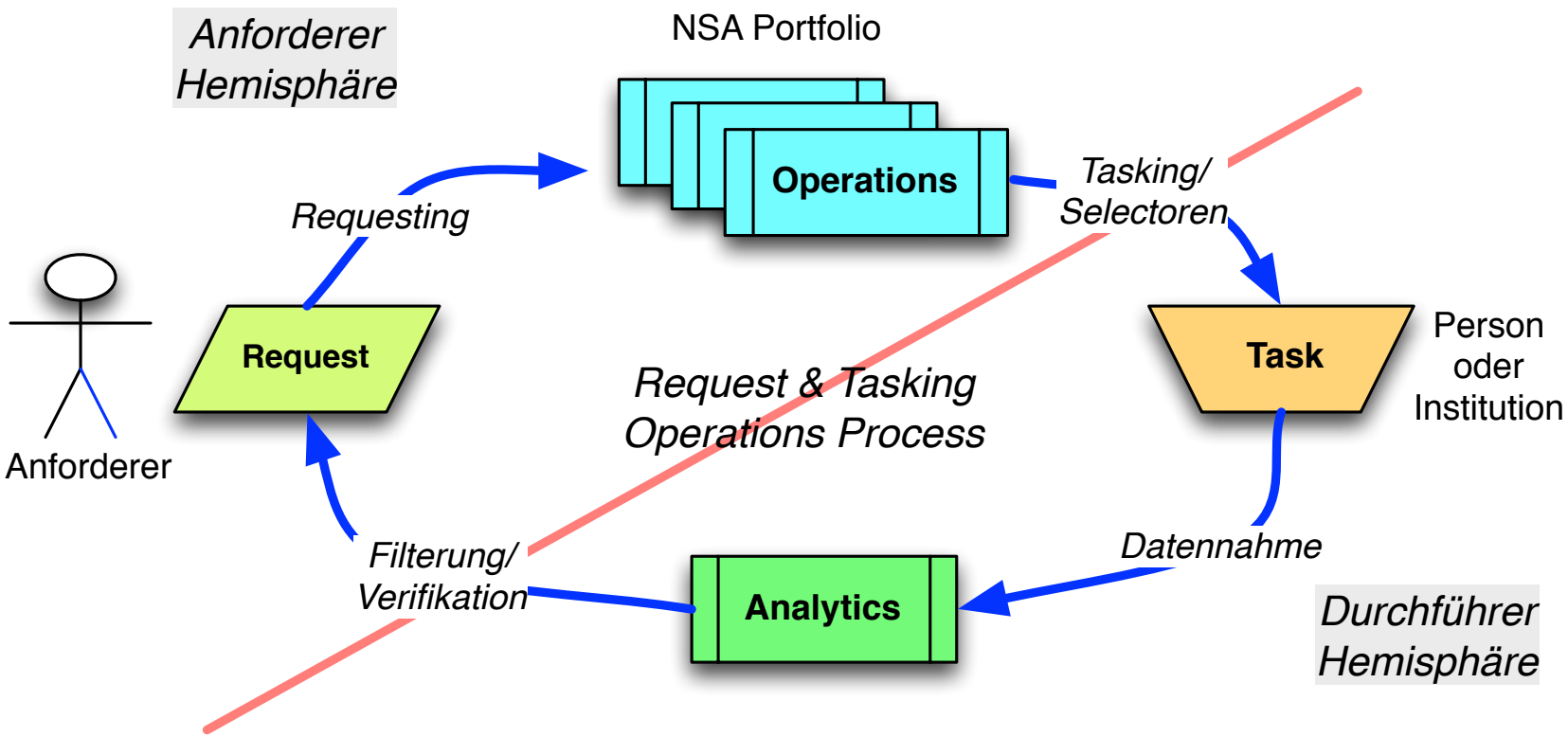


**Abbildung :** Kunde/Angebots-Hemisphären bei der NSA

# Die NSA Ablauforganisation

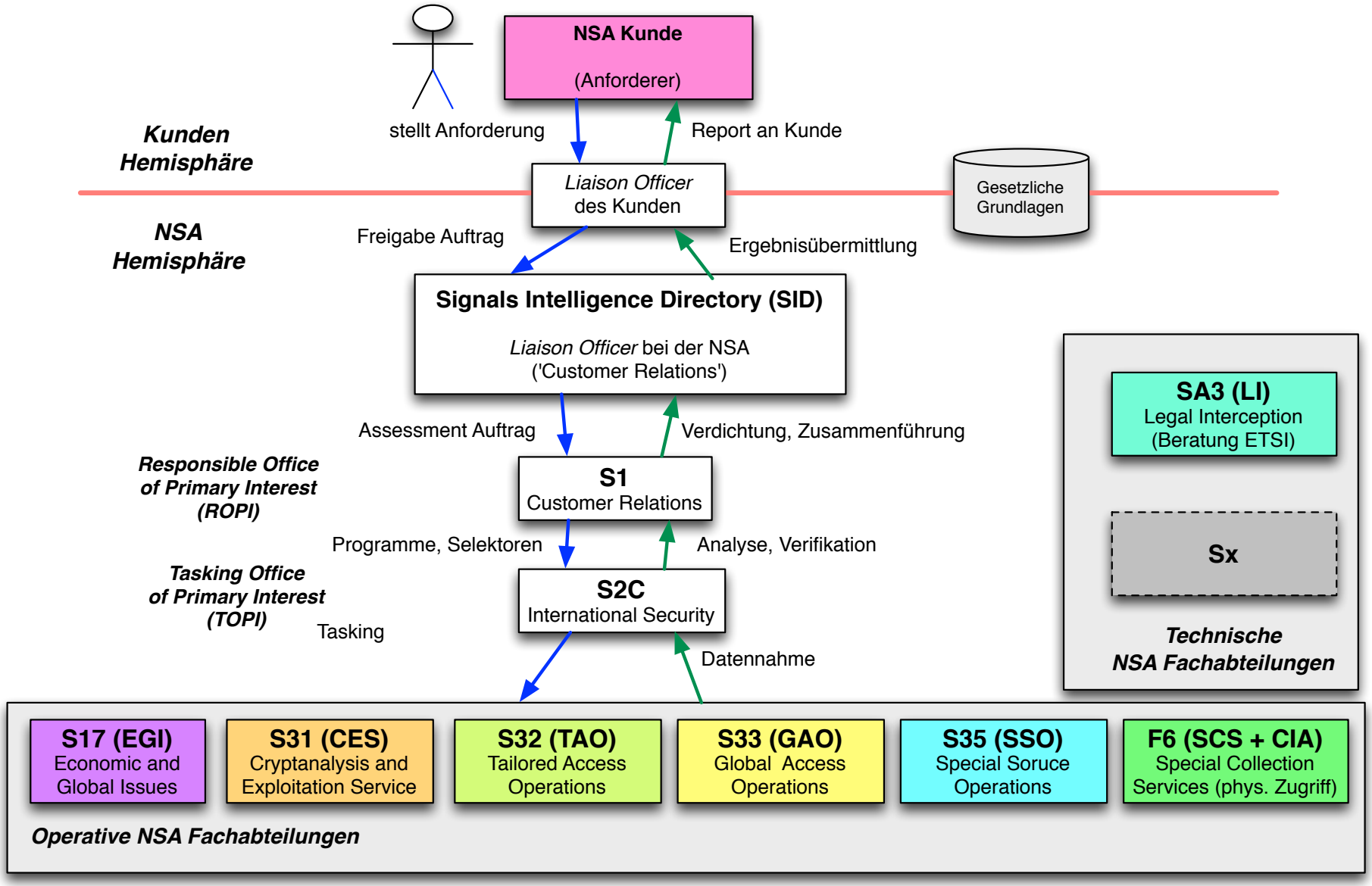


**Abbildung :** Fachabteilungen zur Bedienung der Kundenwünsche und der Informationsbeschaffung

# 'Verdachtslose' Datennahme nach 9/11

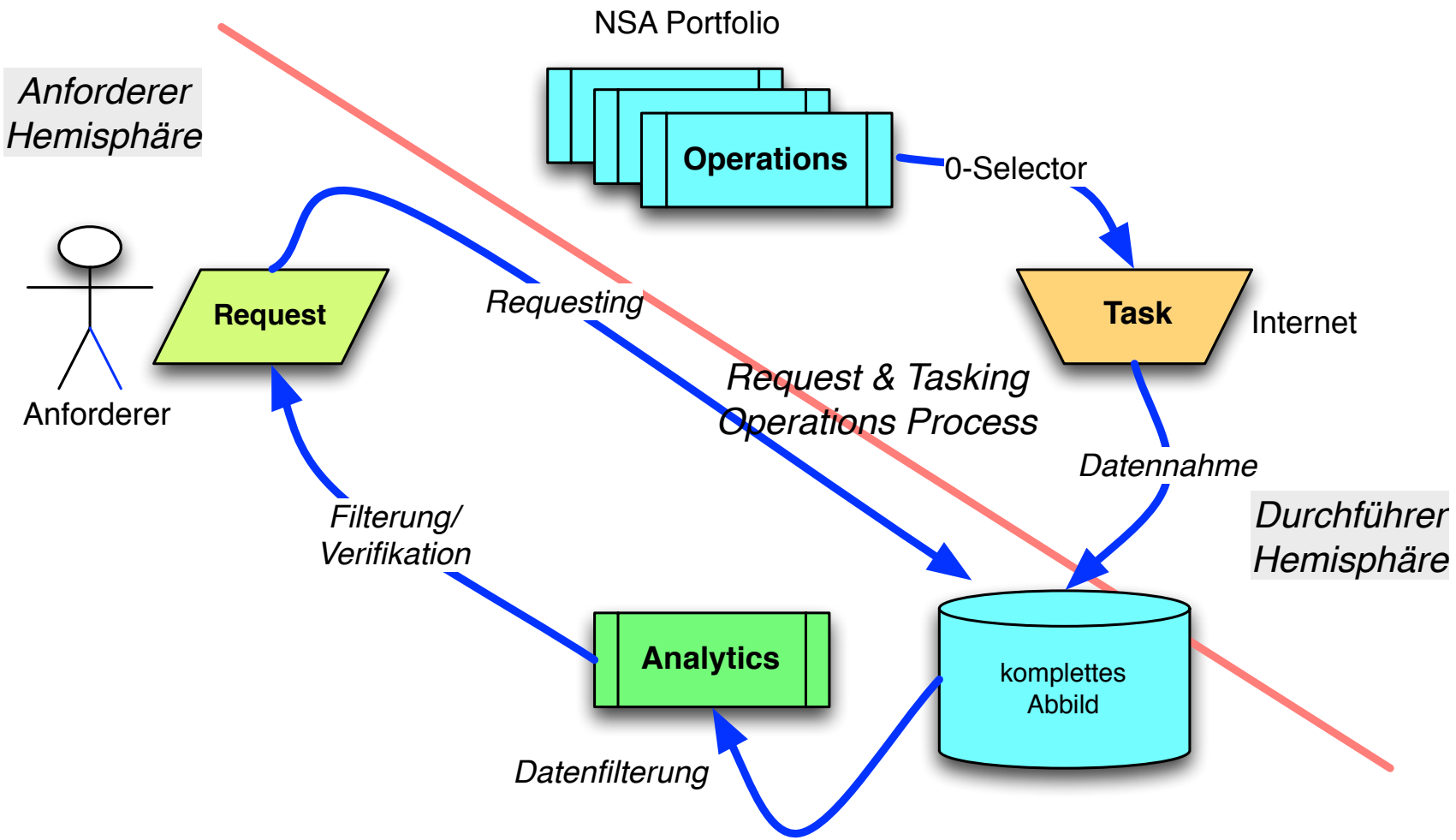


**Abbildung :** Datenbeschaffungsprozess läuft automatisch; unabhängig vom Anforderer

# Datenkorrelation mit XKeyscore

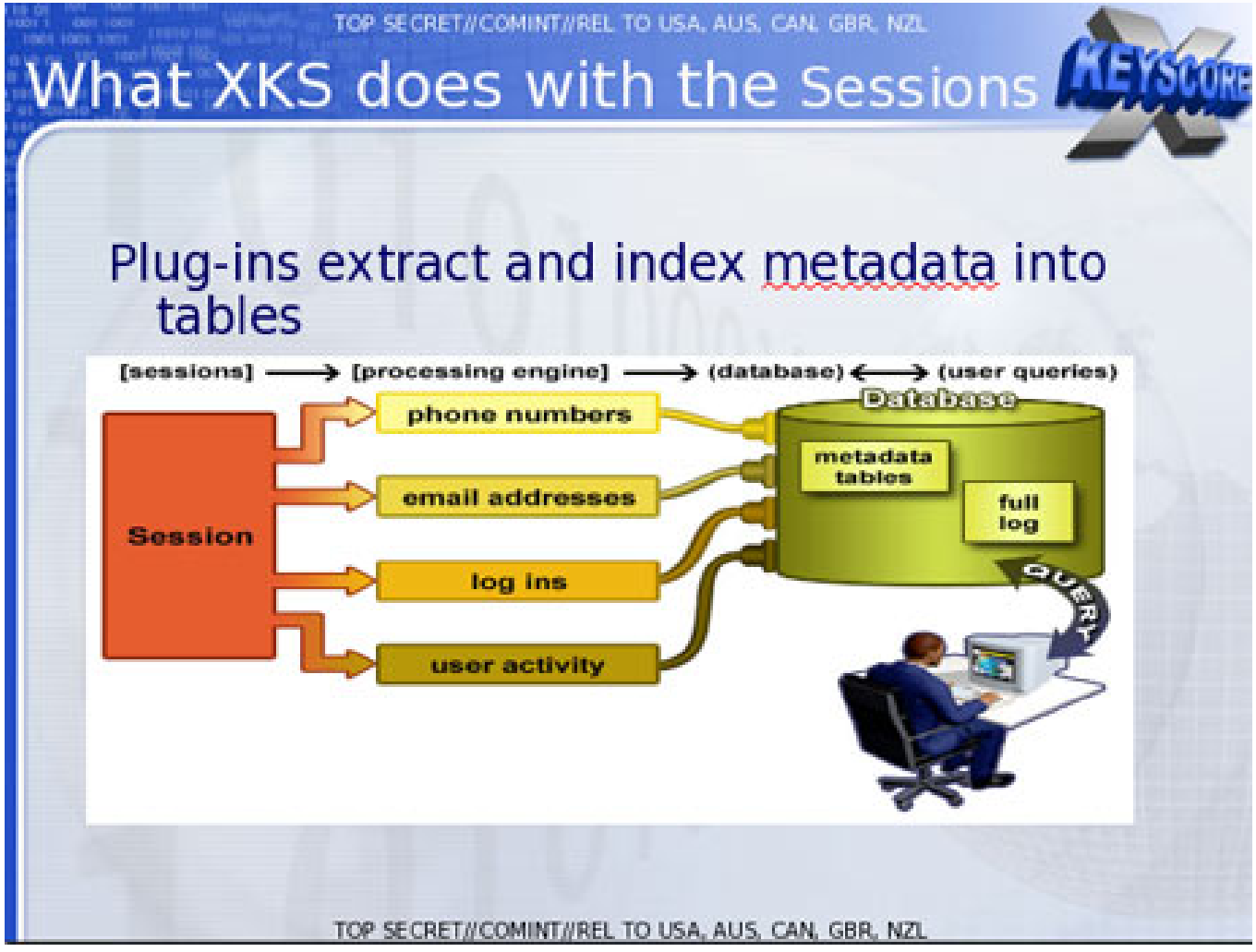


**Abbildung :** Einfacher Zugriff auf die gespeicherten Internet-Daten mittels XKeyscore

↪ Neue NSA Zentrale in Utah besitzt Kapazität den gesamten (zukünftigen!) Datenbestand der im Internet kursierenden Datenpakete für mehrere Jahre zu speichern.

# Business-Information Werkzeug 'XKeyscore'

In dieser Datennahme ist nicht nur die NSA sondern alle FVYE Staaten involviert (beim BND wurde das auch beim DE-CIX probiert).

↪ Auswerte-Werkzeug ist *XKeyscore*:

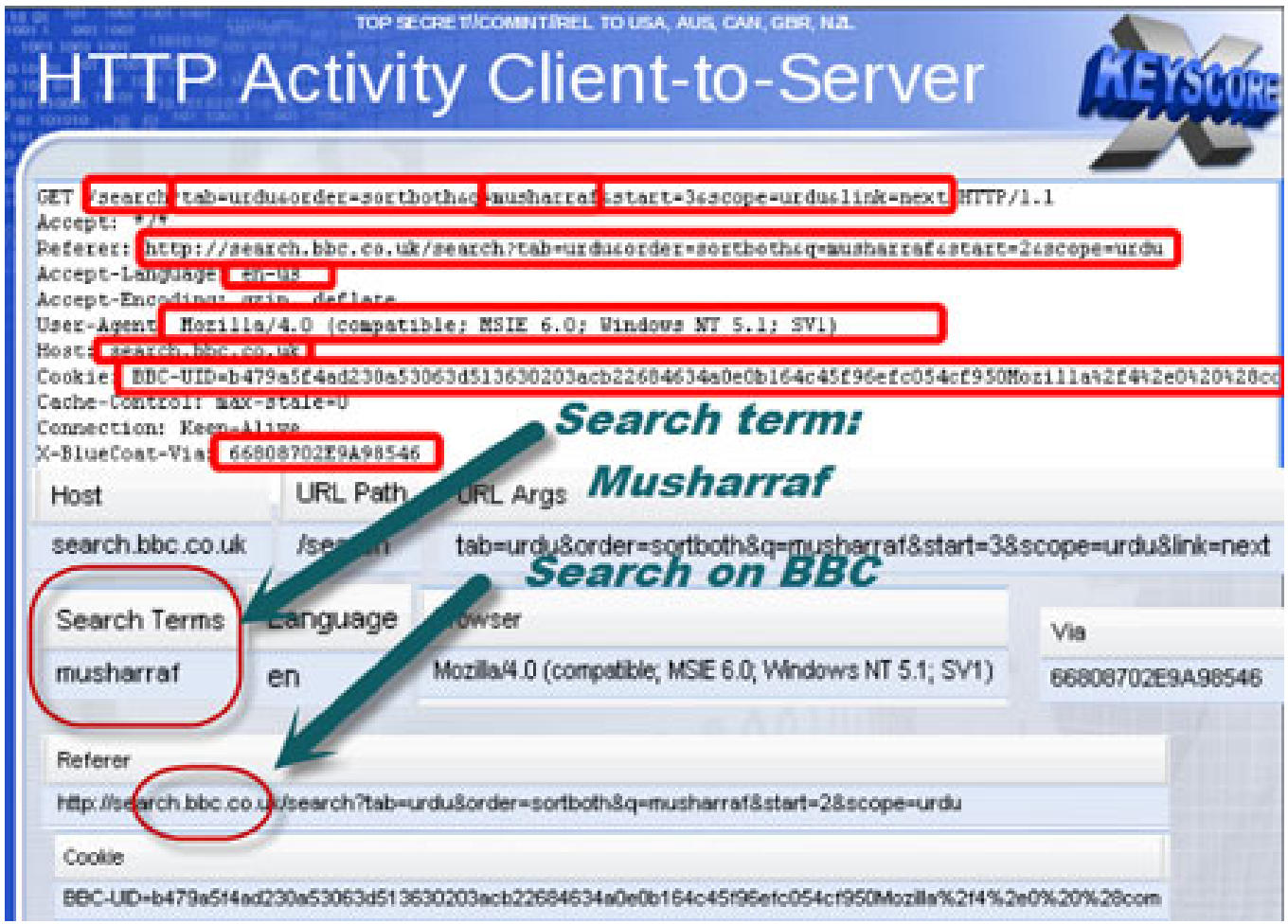


**Abbildung :** Einfacher Zugriff auf die gespeicherten Internet-Daten mittels XKeyscore

# Nachverfolgung von Emails mittels 'XKeyscore'

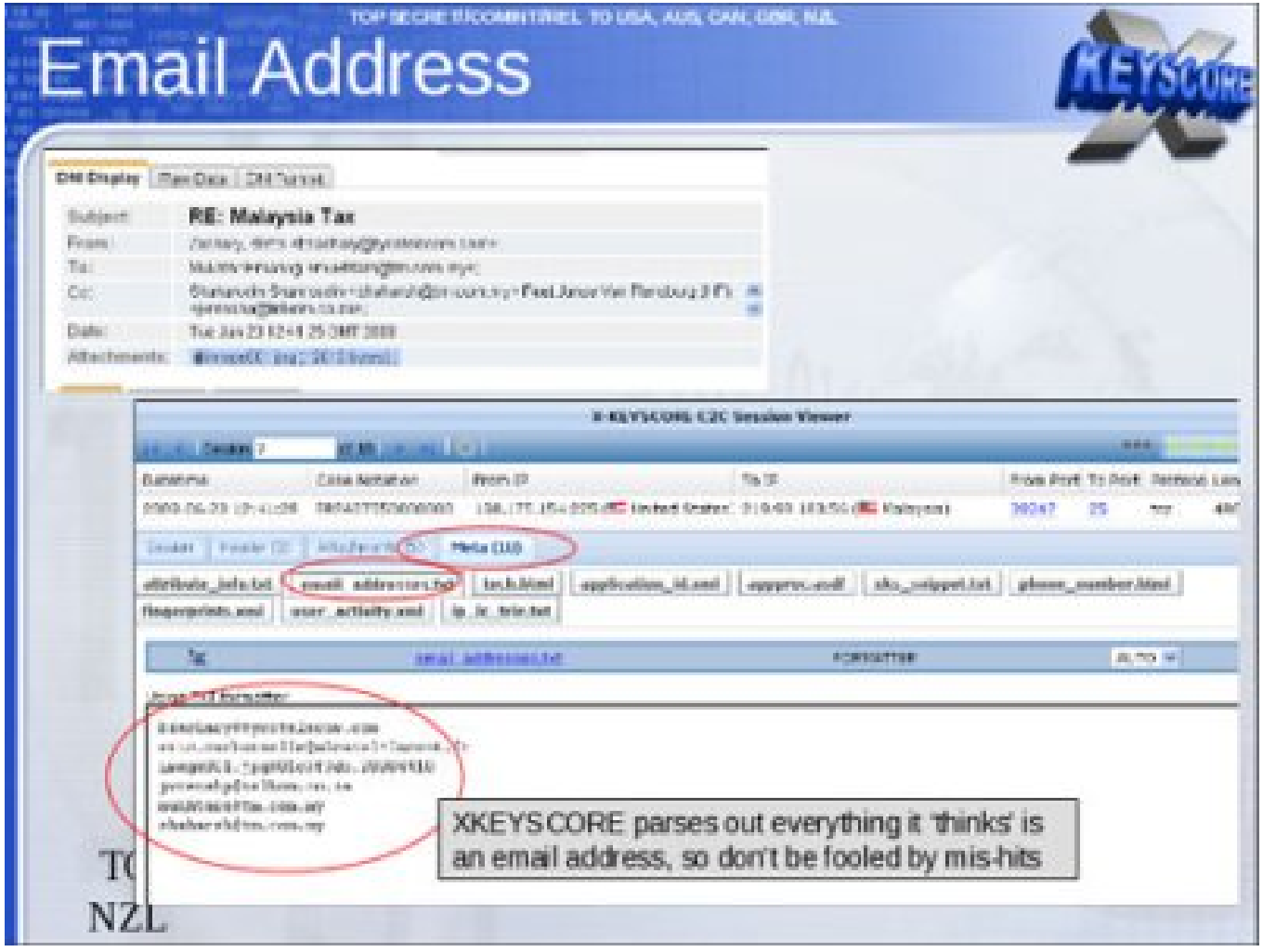


**Abbildung :** Email-Kommunikation transparent gemacht mittels XKeyscore

# NSA Angebotsportfolio

# Angebotsportfolio der NSA Operationen

Die NSA sieht sich als *omnipotenten* Informationsbeschaffer (weltweit!).

Zur Beschaffung der Informationen müssen zunächst die Grundlagen gelegt werden:

- (Klandistin) Abhören nationaler unter internationaler Internet-Verbindungen (Glasfaserkabel).
- (Klandistin) Verwanzung und Implantierung von Trojanern in Netzwerkwerk- und TK-Komponenten sowie Servern.
- (Klandistin) Verwanzung von Endgeräten, mit z.B. Keyloggern; Ausnützen von 0-Day Exploits.
- Einbeziehung von US-Firmen (Google, Apple, Microsoft, Yahoo, Facebook) per NSL (PRISM-Programm).
- Absprachen mit Sicherheitsfirmen (bzw. Kauf) zur Implantierung von Sicherheitsschwachstellen (z.B. RSA).
- Manipulation von Internet- und Security-Standards zum Einbau von Schwachstellen (**NIST**).
- Kauf von 0-Day Lücken auf dem 'grauen Markt' (ebenso wie Bundestrojaner).
- Kompromittierung von Firmen wie Apple oder Microsoft, bekannte Sicherheitslücken nicht zeitig zu schliessen.

$\hookrightarrow$ Aus diesem Vorgehen ergibt sich das Angebotsportfolio der NSA (gegenüber Kunden).

Kryptographie und speziell kryptographische Algorithmen/Implementierungen fallen in den USA unter das Kriegswaffen-Exportverbot.

# NSA als omnipotenter Datenlieferant

Ziel der Wertschöpfungskette bei der NSA: Die *Treasure Map* – NSA als *Enabler*.

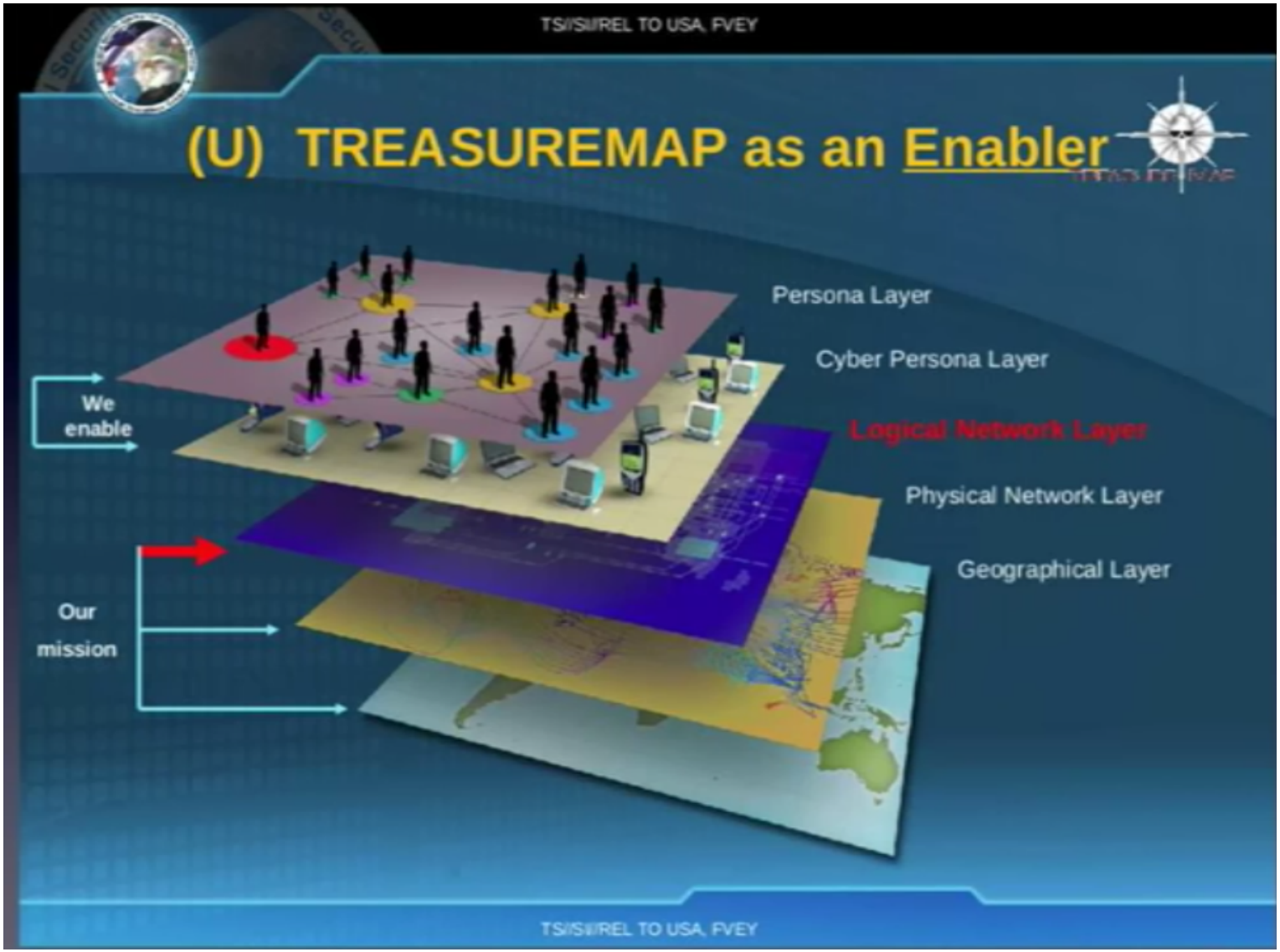


**Abbildung :** Die Welt, das Internet, die Server als zentrale Datenlieferanten

# NSA-Operationen

# Operationen

- Wirtschafts-Spionage 1998: Abzapfen der Telekommunikation der deutschen Firma *Enercon* zur Verhinderung eines Geschäfts mit Windenergieanlagen in den USA[23].
- Spionage 2009: Klima Gipfel in Toronto/Kanada[24]
- Sabotage 2010: Entwicklung des Stuxnet-Virus zur Sabotage iranischer Uran-Aufbereitungsanlagen[25] zusammen mit dem Mossad.
- Wirtschafts-Spionage 2012: Überwachung der Telekommunikation der brasilianischen Ölfirma *Petrobras* mit dem Programm FAIRVIEW (und den Bestandteilen BLARNEY, OAKSTAR und STORMBREW)[26].
- CIA Spionage 2014: Ausspionierung des US Senat Ausschusses zur Guantanamo-Folter[27]

---

[23] http://www.zeit.de/1998/39/199839.c_krypto_.xml

[24] http://www.information.dk/486360

[25] http://en.wikipedia.org/wiki/Stuxnet

[26] http://www.theguardian.com/world/2013/sep/09/nsa-spying-brazil-oil-petrobras

[27] http://www.nytimes.com/2014/03/05/us/new-inquiry-into-cia-employees-amid-clashes-over-interrogation-program.html?hp&_r=1

# Programm 'PRISM'

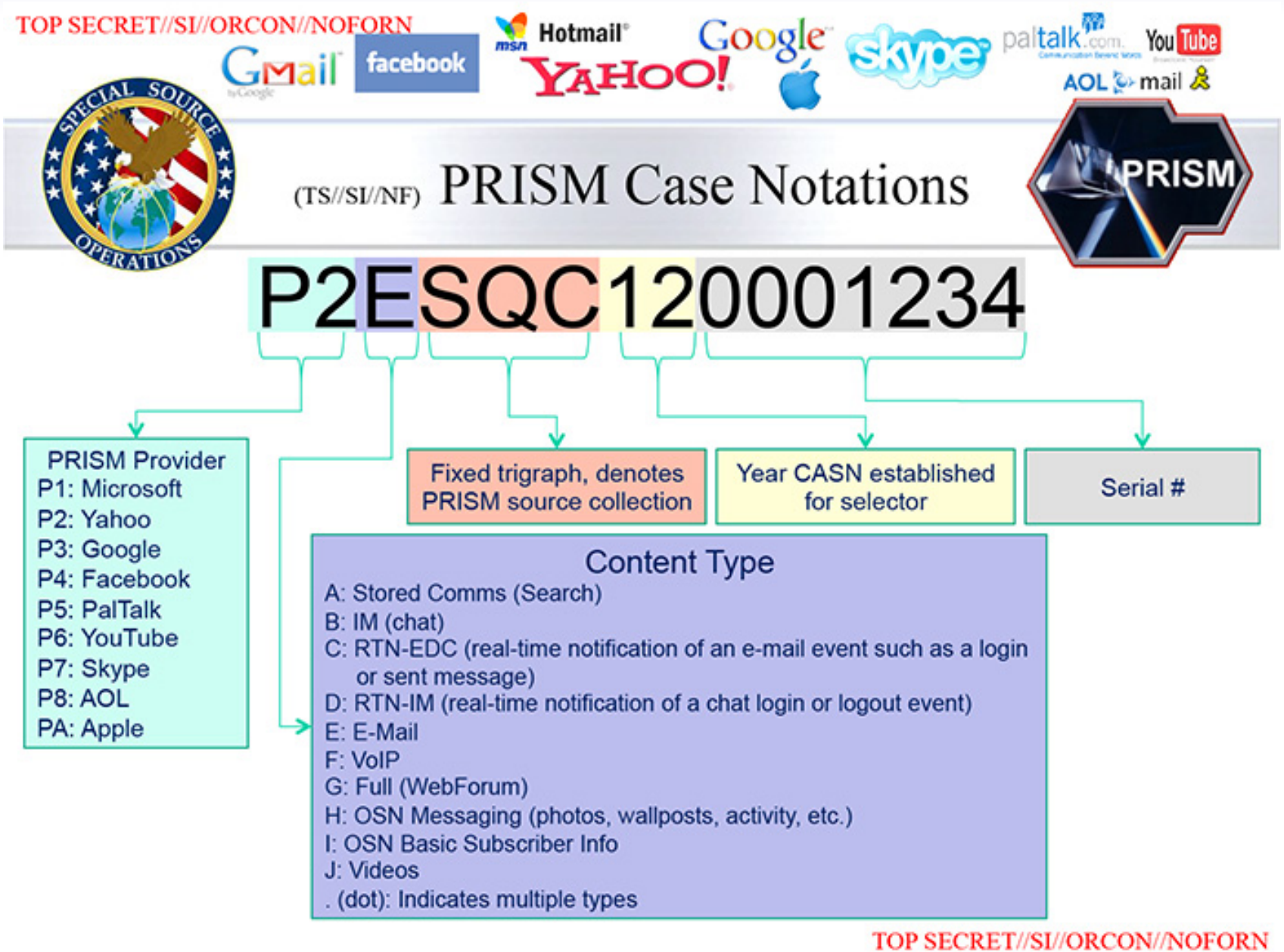


**Abbildung :** NSA sitzt bei den Providern in den Servern (per NSL)

# Programm 'Serendipity'

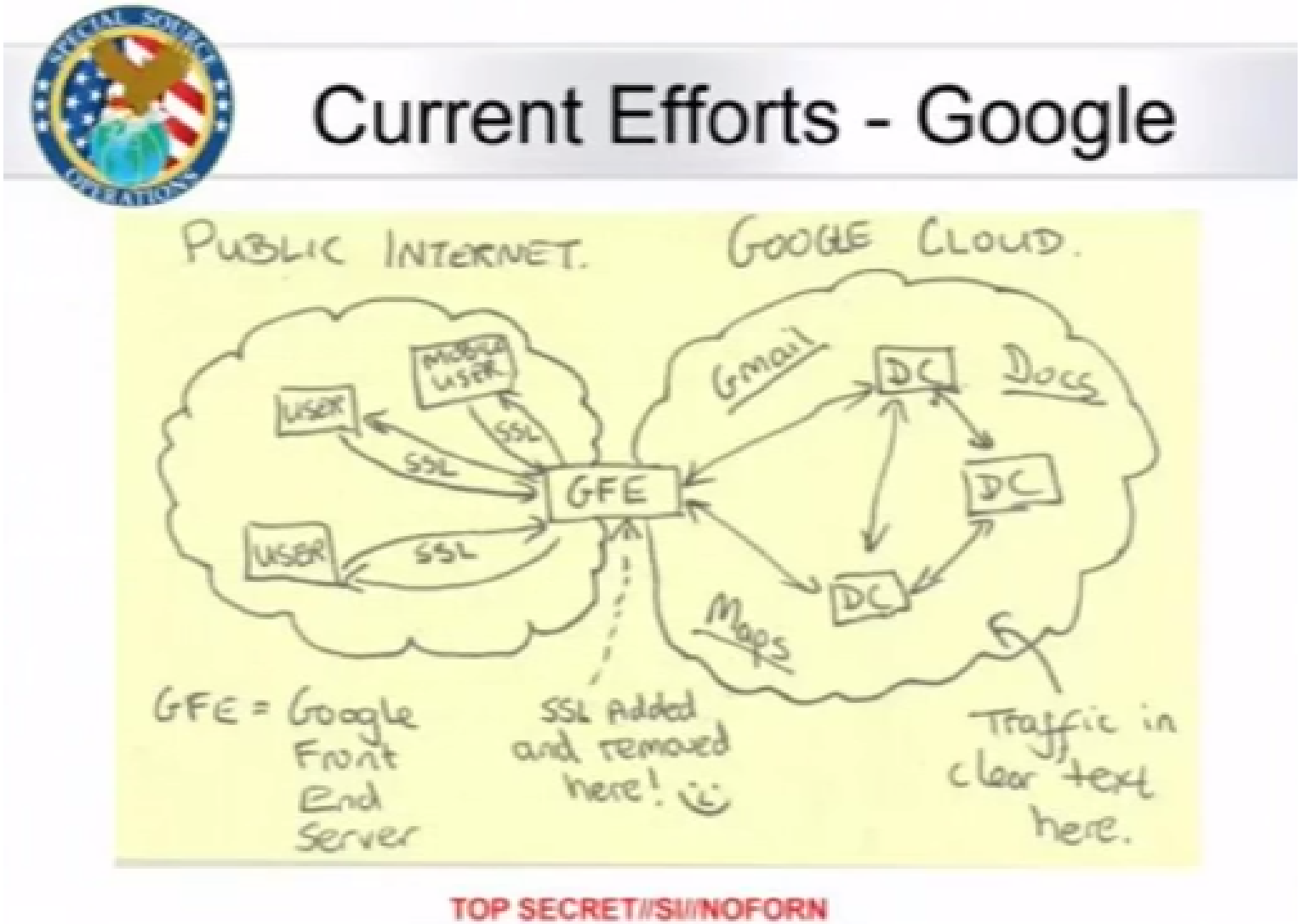


**Abbildung :** Abzapfen der 'Dark Fibre' zum Datenaustausch zwischen den Google-Rechenzentren

# NSA Kennzahlen

# Kennzahlen der NSA

Die NSA ist verpflichtet, ihren Auftraggebern (dem State Department) Kennzahlen für ihren Erfolg zu liefern und zugleich ihre Budget-Aufwendungen zu rechtfertigen.

High-Level Aktivitätenreport an den Präsidenten der Vereinigten Staaten:

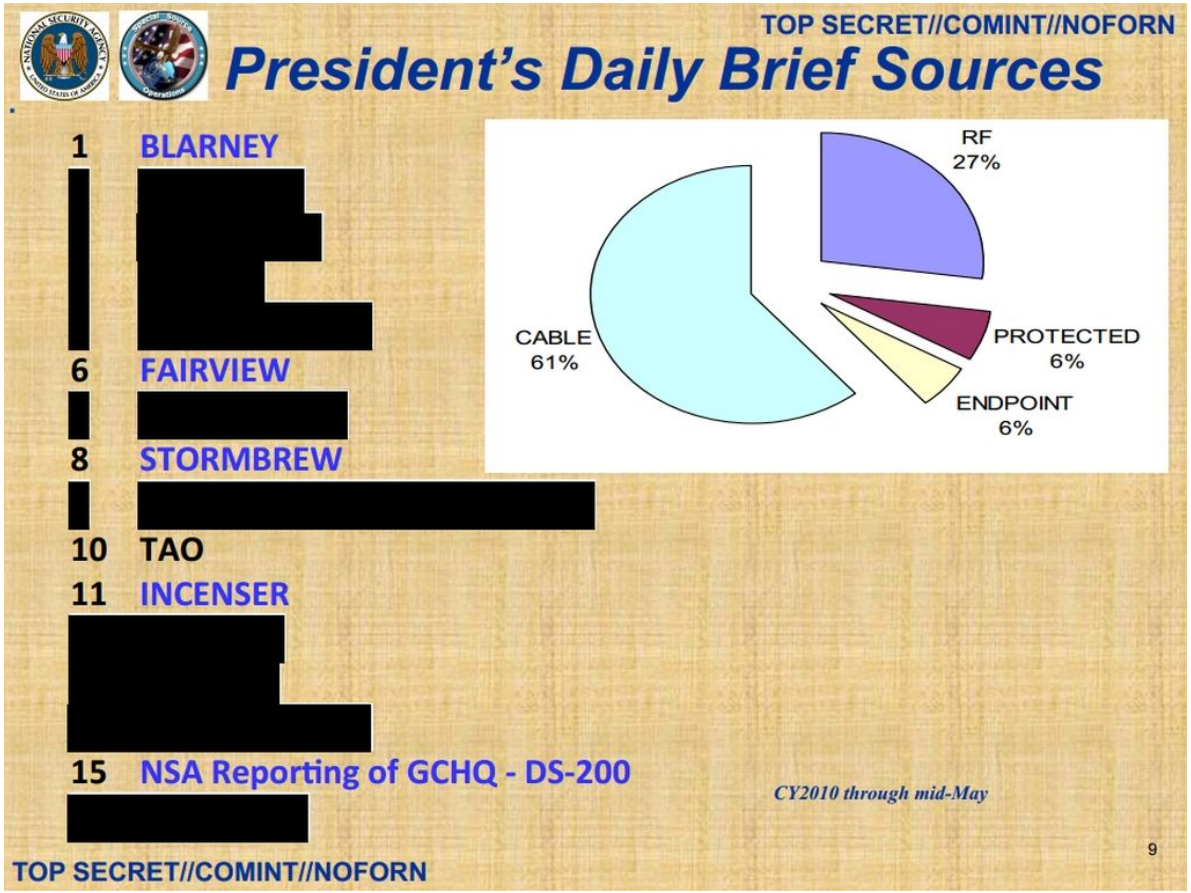


**Abbildung :** Überblick über laufende Programme (nicht Operationen) an den Präsidenten

# TAO Team Texas

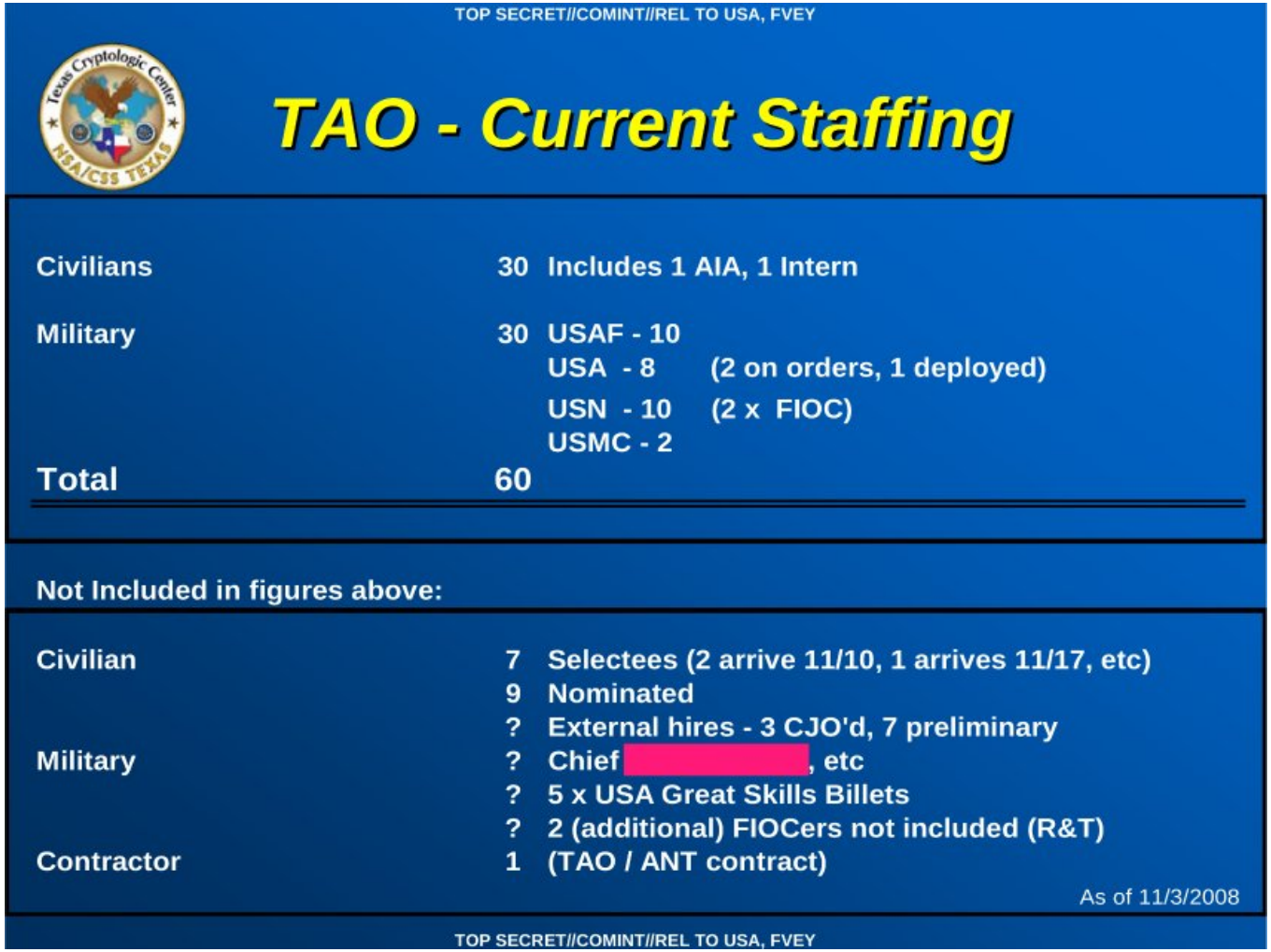


**Abbildung :** Ausstattung des TAO Teams

# Operationen des TAO Team Texas

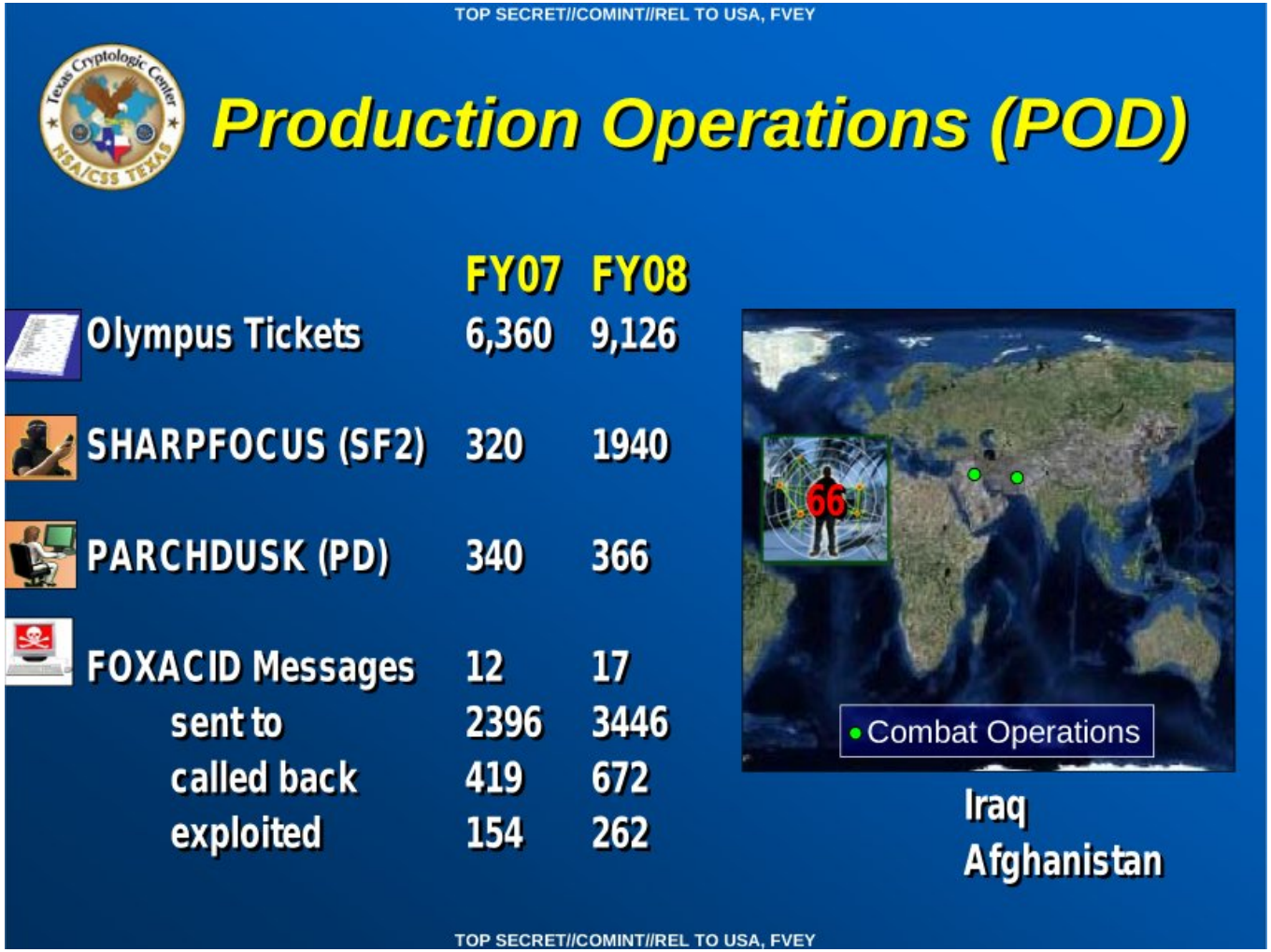


**Abbildung :** Operationen des TAO Teams

# Erfolge der NSA

Die Programme/Operationen der NSA in Bezug auf die Verhinderung von Terrorkaktivitäten ('Counter terrorism') – für die sie eigentlich aufgelegt und bezahlt worden sind, sind im wesentlichen komplett gescheitert[28].

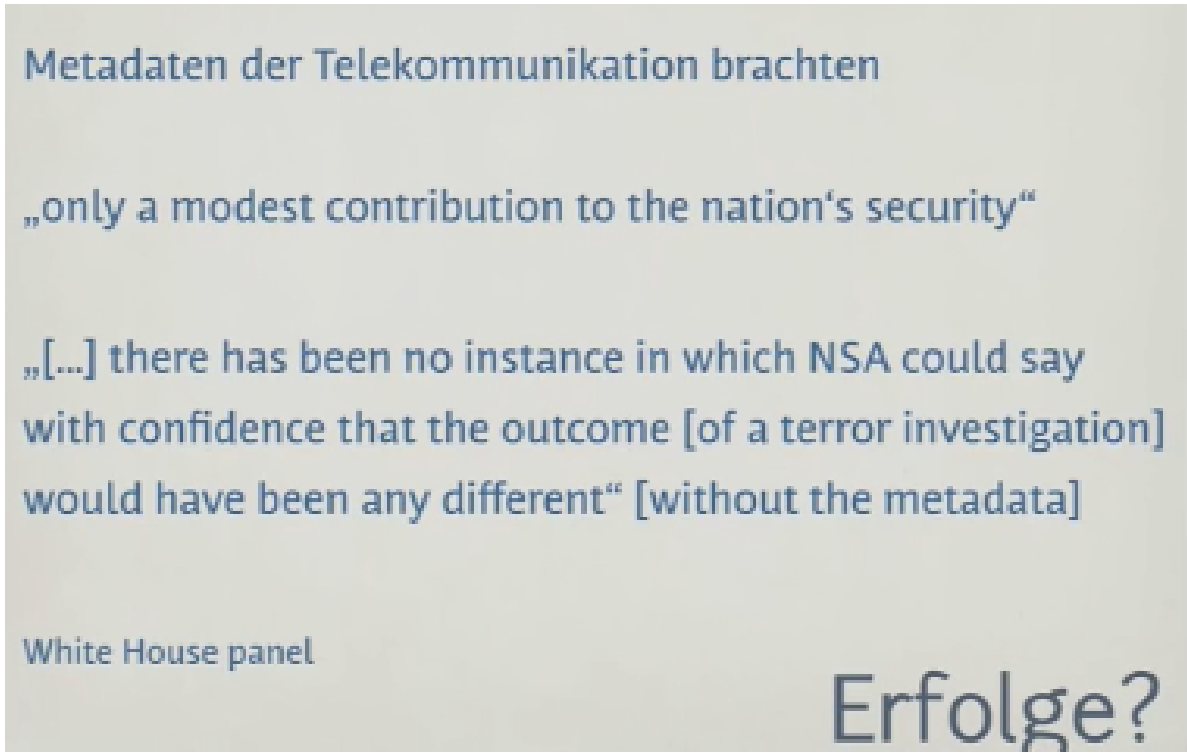


**Abbildung :** Erfolgsbilanz des Anti-Terrorkampfs [Quelle: Constanze Kurz / CCC]

[28] http://www.zeit.de/politik/ausland/2014-01/us-botschaft-bengasi-senat-bericht

# Quellen

- NSA: https://www.nsa.gov/
- CIA: https://www.cia.gov
- FBI: www.fbi.gov/
- FISA: www.fas.org/irp/agency/doj/fisa/

- NSA CES: https://www.nsa.gov/careers/opportunities_4_u/students/undergraduate/msep.shtml
- NSA GAO: http://www.gao.gov/products/NSIAD-96-6

- Wikipedia: http://en.wikipedia.org/wiki/National_Security_Agency
- FISA: http://www.theguardian.com/commentisfree/2013/jun/19/fisa-court-oversight-process-secrecy
- FIfF: http://media.ccc.de/browse/tags/Vortrag.html
- Müller-Maguhn: https://buggedplanet.info/
- ETSI LI: http://www.etsi.org/technologies-clusters/technologies/security/lawful-interception
- Black Hat: http://www.blackhat.com/presentations/bh-usa-03/bh-us-03-baloo.pdf
- Ernst Möchel: https://moechel.com/
- NSA Programm-Namen: http://namingschemes.com/NSA_surveillance_tools
- Cryptome: http://cryptome.org/2014/01/nsa-codenames.htm