10.Security Day 2014

NSA is watching you!!

http://nsa.gov1.info/surveillance/

Die Nationale Sicherheitsdirektive 67

Wie alles begann

Nach Beendigung des Kalten Krieges im Jahr 1990 fiel der Hauptfeind, der Ostblock, als potentieller Gegner weg. Die neue geheimdienstliche Priorität, die Wirtschaftsspionage, wurde von George Bush sen. durch die Nationale Sicherheitsdirektive 67 – herausgegeben vom Weißen Haus am 20. März 1992 – festgelegt. Die freigewordenen Kapazitäten sollen die Echelon-Beteiligten genutzt haben, um die eigenen Verbündeten auf dem Gebiet der Wirtschaft auszuspionieren.

Airbus soll einen milliardenschweren Vertrag mit Saudi-Arabien verloren haben, da die NSA vermutlich durch Echelon herausgefunden hatte, dass Airbus die saudischen Geschäftsleute bei der Auftragsvergabe bestochen hatte.

Die Wirtschaftsspionage wird auch durch die Aussage des ehemaligen CIA-Chefs James Woolsey im Wall Street Journal vom 17. März 2000 bestätigt. Woolsey bemühte sich allerdings darzulegen, die USA hätten lediglich Informationen über Bestechungsversuche europäischer Unternehmen im Ausland gesucht, denn

„die meiste europäische Technologie lohnt den Diebstahl einfach nicht“.

Die Anschläge am 11. September 2001 verändert die Zielsetzung der US-Dienst massiv !
Flächendeckende Rund-Um-Überwachung wird zum Primärziel

http://de.wikipedia.org/wiki/ECHELON

http://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1

Deutschland ist "Partner dritter Klasse“ aber Zielgebiet Nr. 1

Geheime Dokumente offenbaren, dass die NSA systematisch einen Großteil der Telefon- und Internetverbindungsdaten in Deutschland kontrolliert und speichert.

Laut einer internen Statistik werden in der Bundesrepublik monatlich rund eine halbe Milliarde Kommunikationsverbindungen überwacht.

https://netzpolitik.org/2013/sehr-geehrter-innenminister-friedrich-vergessen-sie-prism-hier-ist-was-sie-die-usa-wirklich-fragen-mussen/

http://www.nytimes.com/2013/10/30/world/europe/obama-may-ban-spying-on-heads-of-allied-states.html?hp=&_r=0

Auch Brasilien und Mexiko Zielgebiet Nr. 1

(TS//SI//REL) NSA's Mexico Leadership Team (S2C41) conducted a two-week target development surge effort against one of Mexico's leading presidential candidates, Enrique Pena Nieto, and nine of his close associates. Nieto is considered by most political pundits to be the likely winner of the 2012 Mexican presidential elections which are to be held in July 2012. SATC leveraged graph analysis in the development surge's target development effort.

TOP SECRET//COMINT//REL TO USA, GBR, AUS, CAN, NZL

TOP SECRET//COMINT//REL TO USA, GBR, AUS, CAN, NZL

(U//FOUO) S2C42 surge

(U) Goal

(TS//SI//REL) An increased understanding o
communication methods and associated s
Brazilian President Dilma Rousseff and he

TOP SECRET//COMINT//REL TO USA, GBR, AUS, CAN, NZL

Blick auf die United Nations Plaza und das Hauptquartier der Vereinten Nationen in New York

Palais des Nations in Genf

UNO-City in Wien

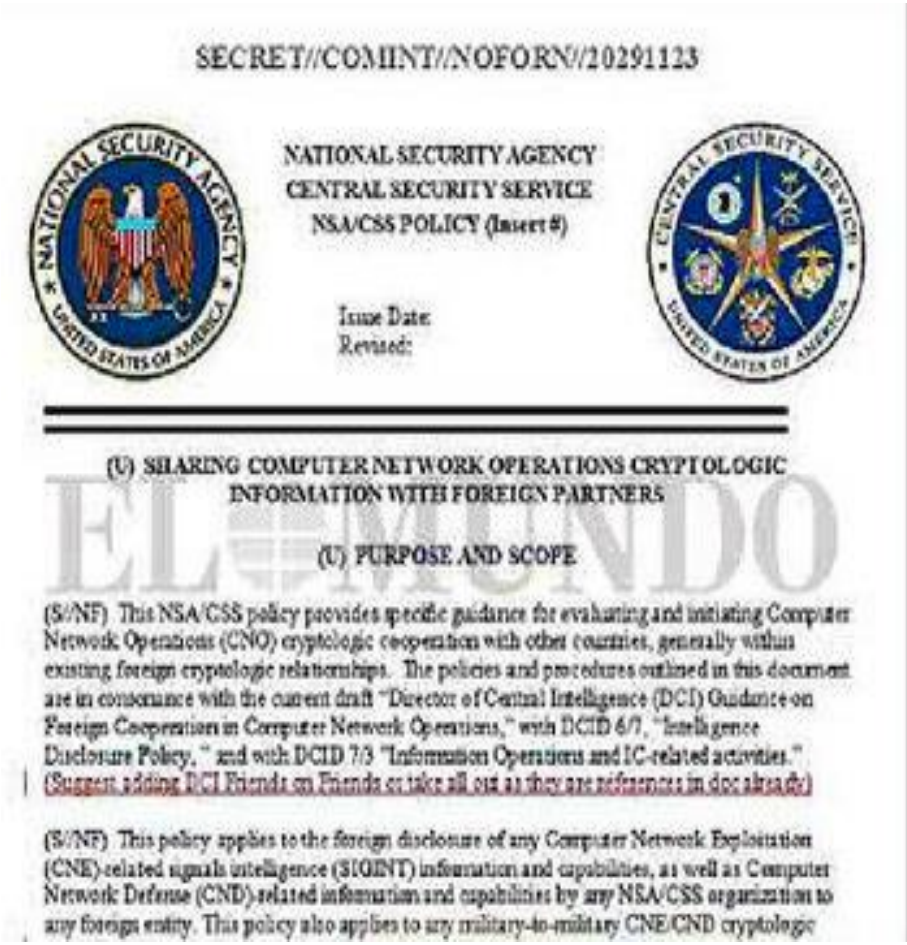
„5 eyes" spionieren Systematisch relevante Ziele in Südamerika aus !

Den Berichten zufolge hat die NSA systematisch auf Telefonate, E-Mails und Kur
brasilianischen Präsidentin und einiger ihrer engsten Berater sowie Minister in i
zugegriffen. Auch der mexikanische Präsident wurde schon im Vorwahlkampf sy

Kanada überwachte mit „Olympia" gezielt Kommunikation des Brasilianischen B
&Energieministeriums

http://g1.globo.com/fantastico/noticia/2013/09/veja-os-documentos-ultrassecretos-que-comprovam-espionagem-dilma.html/

Österreich ?



SECRET//COMINT//NOFORN//20291123

NATIONAL SECURITY AGENCY
CENTRAL SECURITY SERVICE
NSA/CSS POLICY (Insert #)

Issue Date:
Revised:

(U) SHARING COMPUTER NETWORK OPERATIONS CRYPTOLOGIC INFORMATION WITH FOREIGN PARTNERS

(U) PURPOSE AND SCOPE

(S//NF) This NSA/CSS policy provides specific guidance for evaluating and initiating Computer Network Operations (CNO) cryptologic cooperation with other countries, generally within existing foreign cryptologic relationships. The policies and procedures outlined in this document are in consonance with the current draft "Director of Central Intelligence (DCI) Guidance on Foreign Cooperation in Computer Network Operations," with DCID 6/7, "Intelligence Disclosure Policy," and with DCID 7/3 "Information Operations and IC-related activities." (Suggest adding DCI Friends on Friends or take all out as they are references in doc already)

(S//NF) This policy applies to the foreign disclosure of any Computer Network Exploitation (CNE)-related signals intelligence (SIGINT) information and capabilities, as well as Computer Network Defense (CND)-related information and capabilities by any NSA/CSS organization to any foreign entity. This policy also applies to any military-to-military CNE/CND cryptologic

CONFIDENTIAL//NOFORN//20291123

TIER A **Comprehensive Cooperation**	Australia Canada New Zealand United Kingdom
TIER B **Focused Cooperation**	Austria Belgium Czech Republic Denmark Germany Greece Hungary Iceland Italy Japan Luxemberg Netherlands Norway Poland Portugal South Korea Spain Sweden Switzerland Turkey

/http://www.elmundo.es/espana/2013/10/30/5270985d63fd3d7d778b4576.html

Wirtschaftliche Interessenslage wird NICHT bestritten

“Woolsey suggested the CIA might aid American companies both by helping them to defend against industrial espionage and by providing them with intelligence about economic trends”.

James Woolsey (ehem. CIA-Direktor)

Von wem sprechen wir ?

Die NSA wurde von US-Präsident Harry S. Truman in den 1940er-Jahren als Unterabteilung des Department of Defense (Pentagon) der USA geschaffen. Aus der Army Security Agency (ASA) wurde ab 1949 die Armed Forces Security Agency (AFSA) und schließlich am 4. November 1952, dem Tag der Wahl Dwight D. Eisenhowers zum 34. Präsidenten der USA, die NSA offiziell gegründet. Sie wurde mit dem Auftrag, ausländische Nachrichtenverbindungen abzuhören, eingerichtet.

National Security Agency
— NSA —

Staatliche Ebene	Bund
Aufsichtsbehörde(n)	United States Department of Defense
Gründung	4. November 1952
Hauptsitz	Crypto City, Fort Meade, Maryland, USA
Behördenleitung	**DIRNSA** Gen. Keith B. Alexander[1] **Deputy DIRNSA** John C. Inglis[2]
Mitarbeiter	ca. 40.000 (Schätzung, genaue Angaben geheim)
Haushaltsvolumen	ca. 10,8 Mrd. US-Dollar[3][4] (Schätzung, genaue Angaben geheim)
Website	www.nsa.gov

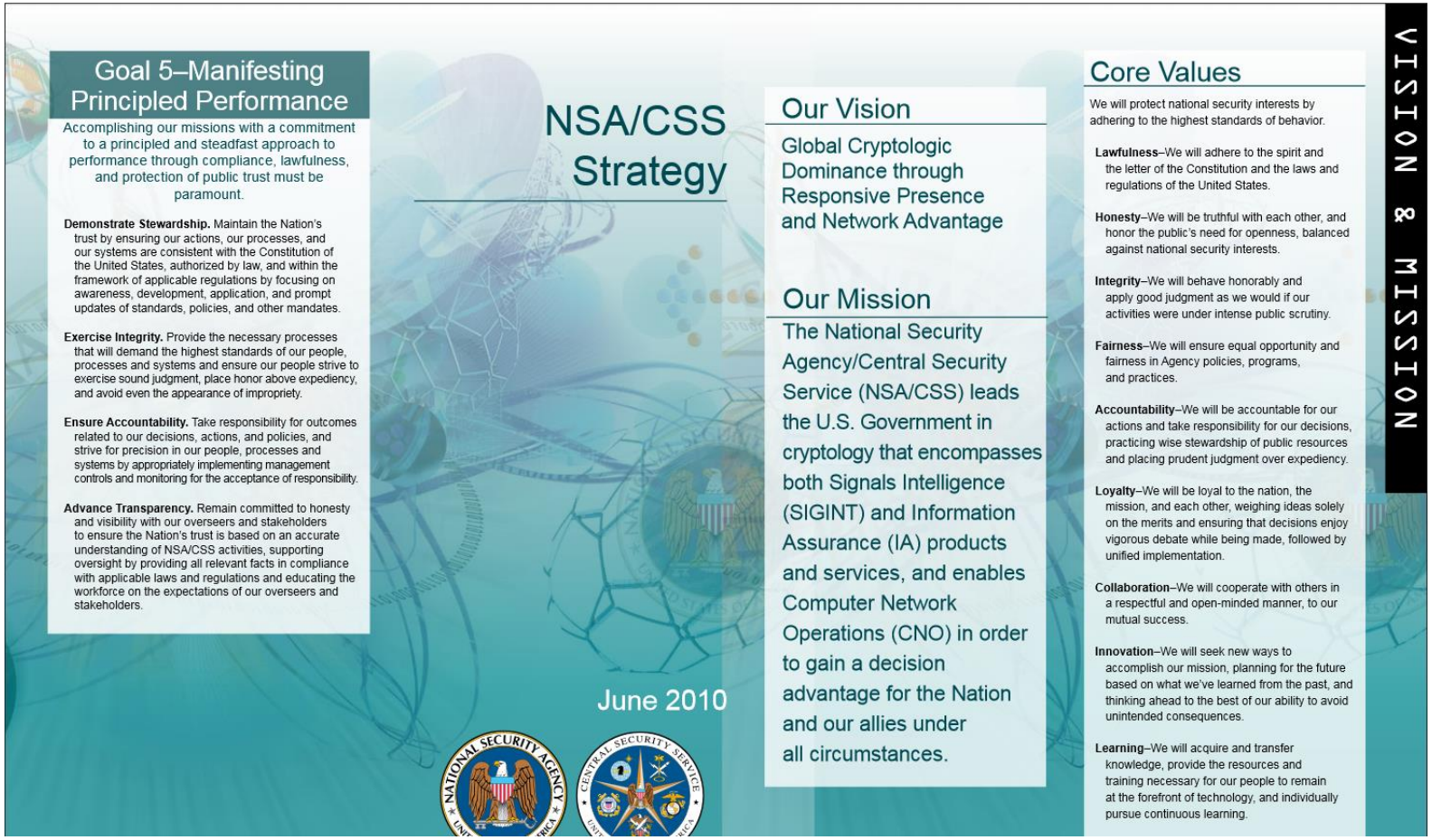
Die **National Security Agency** (**NSA**) ist der größte und finanziell am besten ausgestattete Auslandsgeheimdienst der Vereinigten Staaten.

Die NSA ist für die weltweite Überwachung, Entschlüsselung und Auswertung elektronischer Kommunikation zuständig und in dieser Funktion ein Teil der *Intelligence Community*, in der sämtliche Nachrichtendienste der USA zusammengefasst sind.

Die NSA arbeitet mit Geheimdiensten befreundeter Staaten zusammen.

http://de.wikipedia.org/wiki/National_Security_Agency - www.nsa.gov

Strategie wird klar kommuniziert



Globale kryptographische Vorherrschaft durch Allgegenwertige Präsenz und Netztechnologischen Vorsprung

http://nsa.gov1.info/surveillance/
http://www.nsa.gov/about/_files/nsacss_strategy.pdf

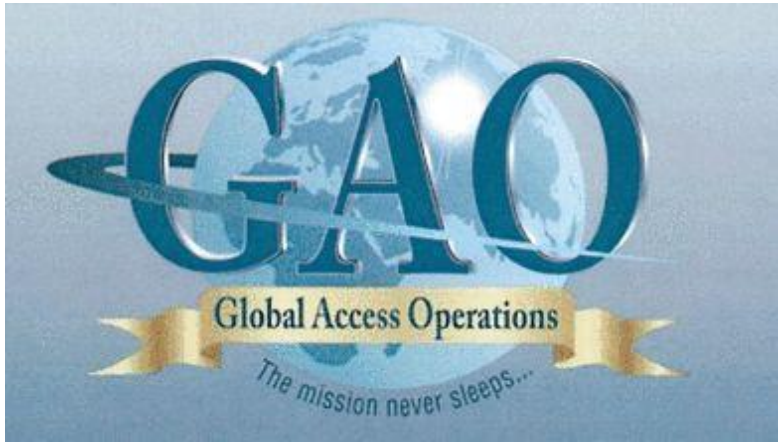
Bevors losgeht..

PRISM war nicht der Anfang von SigInt (Signal Intelligence)

PRISM ist nur EIN Teilprogramm von VIELEN das im Zuge der SigInt entwickelt und eingesetzt wurde bzw wird

Snowdens „Verrat“ offenbart laufend weitere Details zu unterschiedlichen Programmen Und Aktivitäten die immer bessere Rückschlüsse auf die „surveillance strategy“ der USA ermöglichen

Wir erinnern uns:



Boundless Informant
Grenzenloser Informant

Dient dazu, aus der Maße nachrichtendienstlicher signifikante Zusammenhänge herauszufiltern – etwa die Kommunikation einer einzelnen, terrorverdächtigen Person aus einer Fülle von E-Mails und Telefonmetadaten.

Um die verfügbaren Daten noch effizienter auszuwerten, vollzog sich in den Geheimdiensten eine grundsätzliche Veränderung des Denkansatzes:

Neben Inhalten in den Nachrichten (Telefonate, E-Mails, Postings) zu suchen, lieferten bereits die datenmäßig kleinen Zeit- und Ortsstempel von Nachrichten so viele Informationen über eine Person, dass man ein Bewegungsprofil und damit ein Überwachungsprofil aufstellen kann.

.

Boundless Informant

Von *Boundless Informant* erzeugte Weltkarte mit Regionen stärkerer und schwächerer Überwachung (rot – gelb – grün)

Besondere Bedeutung in Deutschland erlangte das Tool, weil die Bundesrepublik in einem von Edward Snowden veröffentlichten Screenshot als einziges europäisches Land gelb eingefärbt war, das für eine starke Überwachung steht.

Ansätze zu dieser Technologie gibt es seit langem, aber ein sinnvoller Umgang mit Big Data, also Datenmengen, wie sie durch Privatpersonen und Firmen heutzutage in Trillionen-Mengen anfallen, war erst ab 2010 möglich.

Aktuell: 2,5 · 1018 Bytes pro Tag = 2.500.000 Terabytes pro Tag

Bis dato galten diese Mengen jedoch bisher wegen ihrer ungeordneten Struktur und schieren Menge als unauswertbar.

Prism-Leakage brachte die Sache in Rollen

Zugriffsprogramme auf Glasfaserkabel wiretapping programs:

Fairview

Stormbrew

Blarney

Oakstar

Blarney:

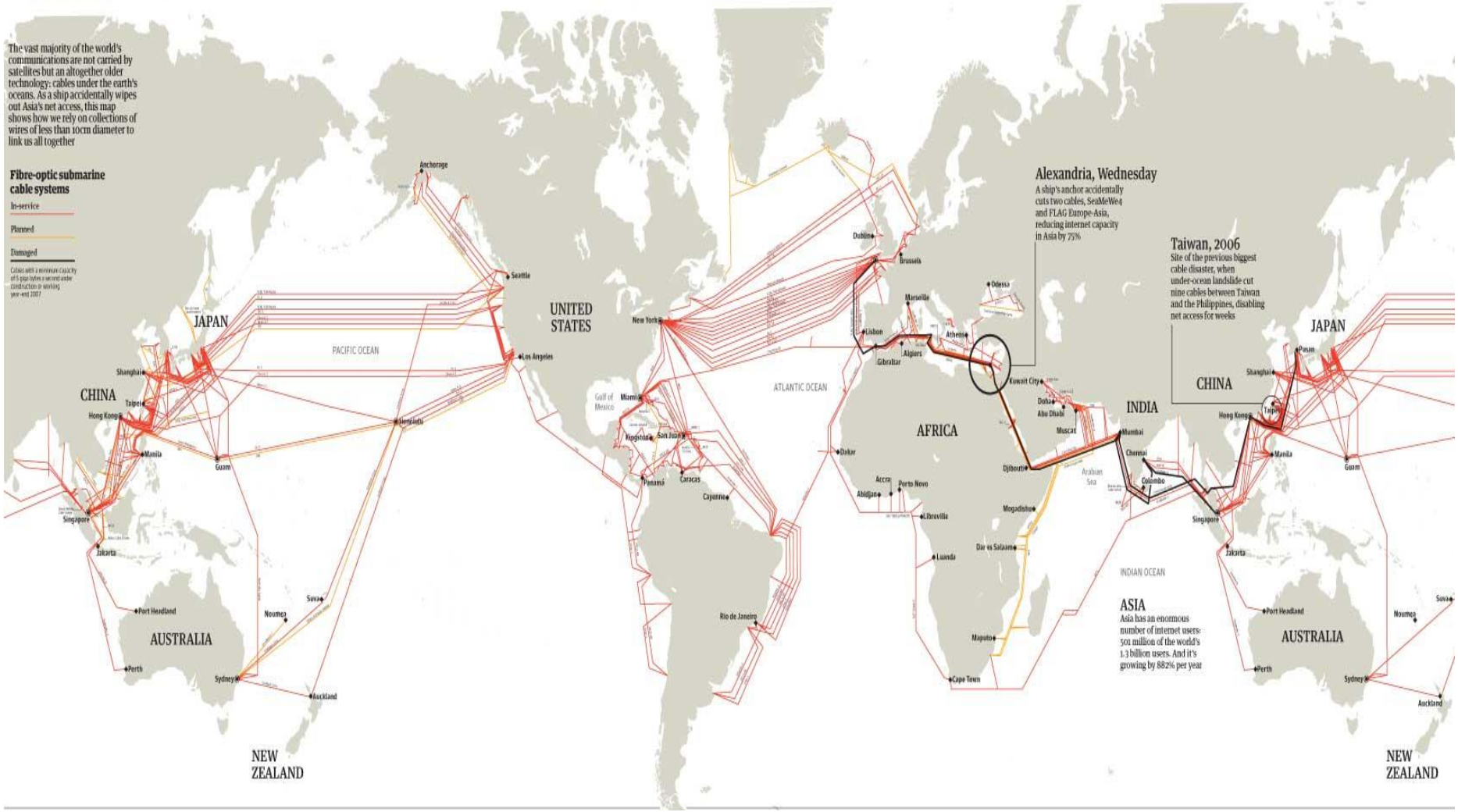
Schon 2004 „leakte“ der AT&T Angestellte und whistleblower Mark Klein das fiber-optic-splitting der NSA bei AT&T.

Diese “Sammlung von Glasfasern” passiert nicht nur auf Kabeln, auf denen die USA direkten Zugriff an einem End- oder Zwischenpunkt hat. Seit den neunziger Jahren bekannt, dass die USA auch fremde Glasfaser-Kabel anzapfen können, unter anderem mit speziellen Spionage-U-Booten wie der USS “Jimmy Carter”.

http://de.wikipedia.org/wiki/USS_Jimmy_Carter_%28SSN-23%29

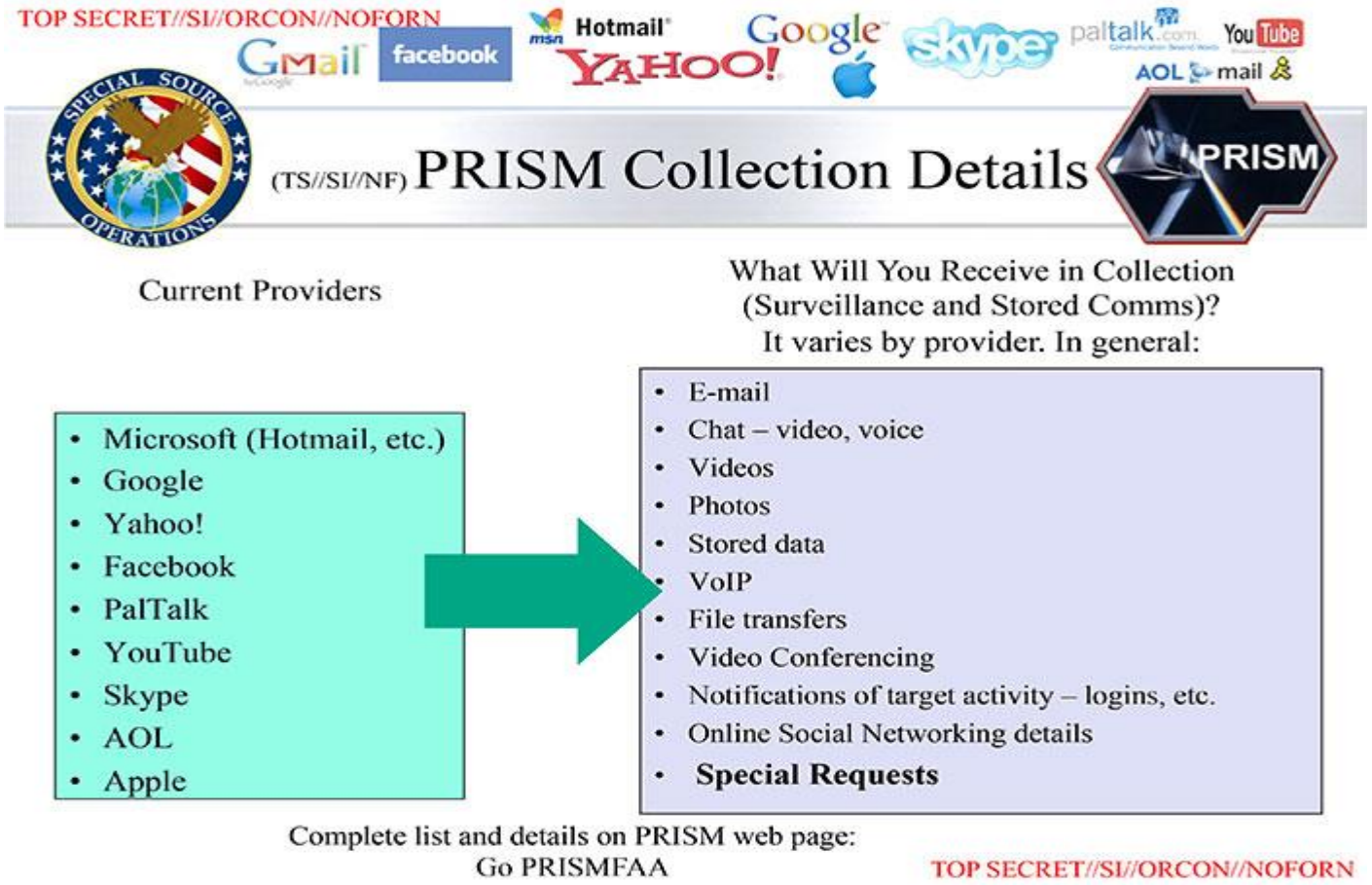
Praktisch: U.S. as Worlds Telecommunications Backbone

The internet's undersea world



http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa

Special Sources Operations



Dürfen NICHT kommunzieren – sind per Gesetz verpflichte JEDE Nachrichtendienstlichen Zugriff geheim zu halten !! Auch Noten amerikanischer Hersteller NICHT mit Behörden zu kooperieren oder ungesetzlich zu handeln sind SINNLOS

Xkeyscore
Datenanalyse und die Echtzeit-Überwachung der erfassten Daten

http://de.slideshare.net/xkeyscore/xkeyscore-nsa-program-presentation

XKeyscore ermöglicht , Inhalte digitaler Kommunikation nach starken Suchkriterien zu durchsuchen (zum Beispiel einer konkreten E-Mail-Adresse), aber auch nach "weichen Kriterien" (etwa der benutzten Sprache oder einem bestimmten Such-String).

Das System erlaubt sowohl die Erfassung von "Ziel-Aktivität in Echtzeit" als auch einen "durchlaufenden Pufferspeicher", der, "ALLE ungefilterten Daten" umfasst, die das System erreichen.

Am Ort der Datenerfassung werden demzufolge ALLE Internetinhalte erfasst und auf Basis ihrer Metadaten indexiert - so dass sie anschließend mit entsprechenden Suchanfragen ausgewertet werden können.

http://de.wikipedia.org/wiki/XKeyscore

Xkeyscore
zum Beispiel ganz Konkret:

http://de.slideshare.net/xkeyscore/xkeyscore-nsa-program-presentation

Weitere Beispiele für das, was XKeyscore aus dem Traffic fischen und noch leisten kann:

Telefonnummern, E-Mail-Adressen, Logins

Nutzernamen, Buddylisten, Cookies in Verbindung mit Webmail und Chats

Google-Suchanfragen samt IP-Adresse, Sprache und benutztem Browser

Jeden Aufbau einer verschlüsselten VPN-Verbindung (zur "Entschlüsselung und zum Entdecken der Nutzer")

Aufspüren von Nutzern, die online eine in der Region ungewöhnliche Sprache nutzen (als Beispiel genannt wird Deutsch in Pakistan)

Suchanfragen nach bestimmten Orten auf Google Maps und darüber hinaus alle weiteren Suchanfragen dieses Nutzers sowie seine E-Mail-Adresse

Zurückverfolgen eines bestimmten online weitergereichten Dokuments zur Quelle

alle online übertragenen Dokumente, in denen zum Beispiel "Osama bin Laden" oder "IAEO" vorkommt, und zwar auch auf "Arabisch und Chinesisch„

"Zeige mir alle verschlüsselten Word-Dokumente in Iran."

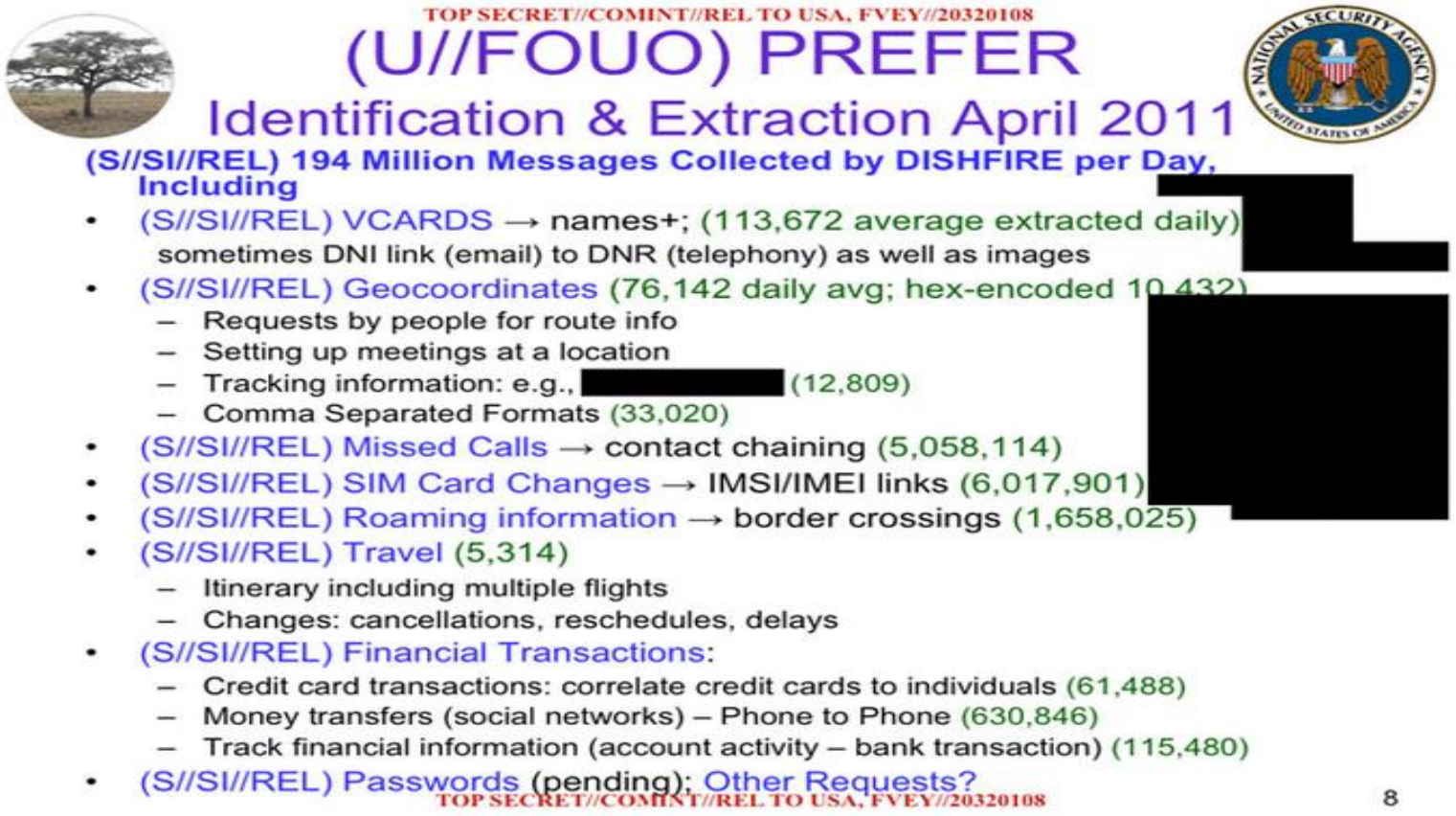
"Zeige mir die gesamte PGP-Nutzung in Iran.".

"Zeige mir alle Microsoft-Excel-Tabellen, mit MAC-Adressen aus dem Irak, so dass ich Netzwerke kartieren kann.„

http://de.wikipedia.org/wiki/XKeyscore

Dishfire&Prefer

Rund 200 Mio SMS / Tag



Alle Inhalte, (Text, Bild) die ich verschicke

Verschickte Visitenkarten und Inhalte

Roaming-User plus Standort-Bestimmung / GeoKoordinaten

Jeder Transaktion (Creditcard, online-banking)

Etc etc

Anschlag auf den Boston-Marathon

Der Anschlag auf den Boston-Marathon war ein Sprengstoffanschlag auf den jährlich am Patriots' Day in Boston stattfindenden Stadtmarathon. Am Montag, dem 15. April 2013, explodierten gegen 14:50 Uhr EDT im Abstand von 13 Sekunden zwei in Rucksäcken versteckte Sprengsätze auf der Zielgeraden des Boston-Marathons. Durch die Explosionen wurden 3 Menschen getötet und 264 weitere verletzt. US-amerikanische Bundesbehörden stuften den Bombenanschlag als terroristischen Akt ein

http://de.wikipedia.org/wiki/Anschlag_auf_den_Boston-Marathon

Das Risiko beim Erdäpfel kochen

"Michele Catalano was looking for information online about pressure cookers. Her husband, in the same time frame, was Googling backpacks"

Wednesday morning, six men from a joint terrorism task force showed up at their house to see if they were terrorists.

Which prompts the question: How'd the government know what they were Googling?

http://www.theatlanticwire.com/national/2013/08/government-knocking-doors-because-google-searches/67864/

Auch auf Facebook wird in ausgewertet:

Der Griesheimer Daniel Bangert hat via Facebook zu einem Spaziergang eingeladen:

Daniel Bangert: "Lebensraum der NSA-Spione etwas aufpeppen"

Man wolle sich den sogenannten Dagger Complex und die "NSA-Spione" einmal aus der Nähe ansehen.

Das US-Militär rief die deutsche Polizei zu Hilfe.

Die kam gleich zweimal.

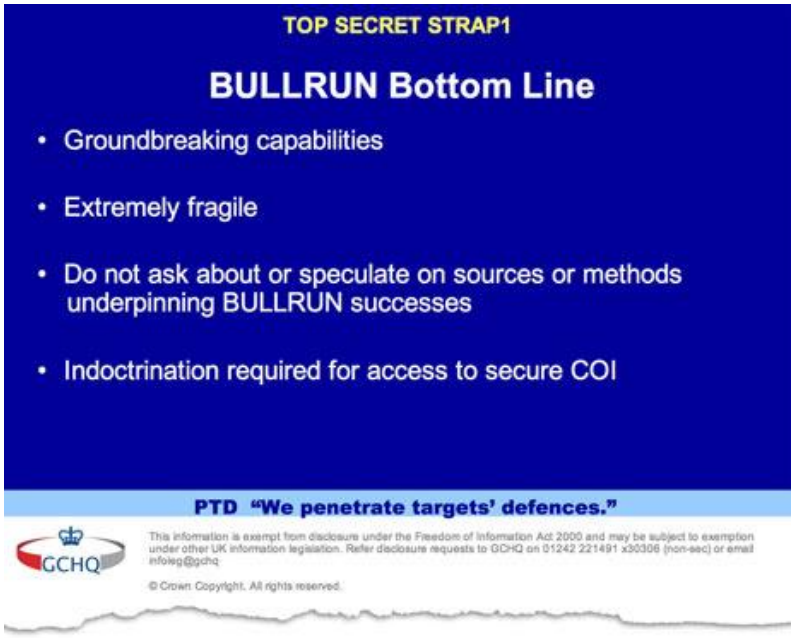
Bundespolizei UND Staatsschutz
Sicher ist Sicher !!

Der Standort gilt als einer der letzten drei Standorte der NSA neben Wiesbaden und Stuttgart – von ursprünglich „schätzungsweise 18 Einrichtungen in der Bundesrepublik“

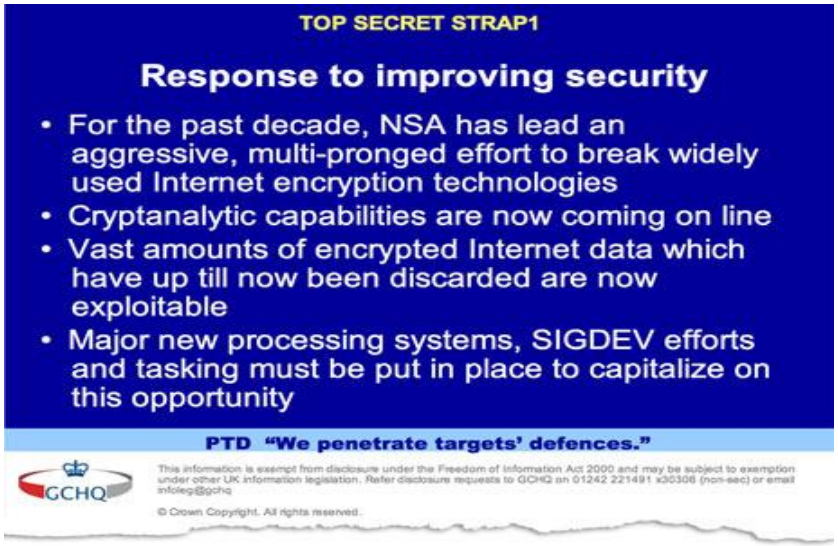
Consolidated Cryptologic Program

BULLRUN

250 Millionen$ schwer dient dazu verdeckten Einfluss auf SecurityAnbieter zu nehmen – darunter sowohl software als auch hardware (etwa crypto-chips)



http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security



Consolidated Cryptologic Program

Ein über 10 Jahre laufendes Entschlüsselungsprogramm hat – laut Eigenangaben NSA – im Jahr 2010 einen Durchbruch erzielt und enorme Datenmengen auswertbar gemacht

Die NSA arbeitet gezielt an der Infiltrierung der weltweiten TK Industrie sowie an einem Weg die Verschlüsselung der von LTE Mobil-Telefonen zu umgehen

Die NSA hat sich Klartext-Zugang zu einem „bedeutenden“ peer-to-peer System für Sprach und Textkommunikation verschafft (Skype ?)

Das US Normungsgremium NIST (National Institute of Standards) wurde gezielt in Arbeitsgruppen manipuliert so das Schwachstellen in Verschlüsselungsstandards- und Protokolle geschaffen wurden

Die NSA kann https bzw SSL gesicherter Kommunikation problemlos entschlüsseln

TAO – Tailored Access Operations
vom Sammler zum Jäger

Über die Struktur und Arbeitsweise der TAO ist verständlicherweise nur recht wenig bekannt:

Remote Operations Center ist der größte Stützpunkt mit etwa 600 Mitarbeitern, innerhalb des Fort Meade Complex in Maryland, USA. Dies ist das 'Herzstück' der TAO

Data Network Technologies Branch, entwickelt die Software, mit der TAO Informationen aufbereitet und analysiert werden.

Telecommunications Network Technologies Branch ist zuständig für das Infiltrieren der Netzwerke

Infrastructure Technologies Branch – sozusagen die System-Administratoren der TAO.

Access Technologies Operations Branch, in Zusammenarbeit mit CIA und FBI kümmert sich die Einheit um "off-net operations" – Rechner vor Ort präparieren, um den TAO Hackern Zugang zu verschaffen.

Budget für CyOps 2013 3,7 Mrd Dollar –4,7 für 2014 gefordert

https://netzpolitik.org/2013/nsa-tailored-access-operations-neue-einblicke-in-die-hacker-einheit/

TAO – Tailored Access Operations
die Staats-Hacker

Kernelement ist dabei *Computer Network Exploitation* – CNE
Das systematische Infiltrieren ausländischer Computernetzwerke,
um so an relevante Informationen zu gelangen =
Einbruch/Hacken von Netzwerkinfrastrukturen

TAO auch eine wichtige Rolle im Kampf gegen die Taliban, al-Qaida und das Ausspähen von Osama Bin-Laden gespielt.

Als die USA 2007 in den Iraq einmarschierten hatten die TAO schon 100 al-Qaida Zellen lokalisiert und die entsprechenden Informationen zur Verfügung gestellt. Allerdings geht es bei TAO um wesentlich mehr, als nur Spionage und Infiltration.

So war die Einheit auch federführend bei der Entwicklung (Zusammen mit der israelischen Armee) des *Stuxnet* und *Flame* Trojaners, zur gezielten Zerstörung bzw. Sabotage des iranischen Atomprogramms.

Auch die bei Operation „Socialist“ verwendete Software „QI“ wird auf TAO zurückgeführt.

Wir halten fest:

Dies waren nur Auszüge unterschiedlicher Programme die von den „5eyes“ Betrieben werden bzw von Snowden gelakt wurden

Es ist klargeworden, dass die US-Dienste im Anlass-Fall und „by Default“ auf alle US-Amerikanischen Unternehmen und deren Lösungen „Einfluss nehmen“

Das sich die Amerikaner eine Position erarbeitet haben - und weiter ausbauen -, die Ihnen die globale Kontrolle über Information und Informations-Infrastrukturen ermöglicht.

I am regularly asked what the average Internet user can do to ensure his security. My first answer is usually : 'Nothing; you're screwed'.

Bruce Schneier

Was können wir tun ?

Es gibt keine „isolierte“ Maßnahme – außer als Einsiedler in den Busch zu kehren –
die etwas gegen diese Möglichkeit der Überwachung ausrichten könnte.

Es braucht eine Fülle von Maßnahmen – gesellschaftlich wie technologisch –
um Europa´s Abhängigkeit zu verringern.

Vor allem aber braucht es dafür:

Das Bewusstsein dieser Sachverhalte und die daraus resultierenden Konsequenzen für
Unsere Gesellschaft und Europa

Menschen die diese Technologien verstehen und in der Lage sind die Zusammenhänge
und Konsequenzen korrekt beurteilen zu können.

Vielen Dank

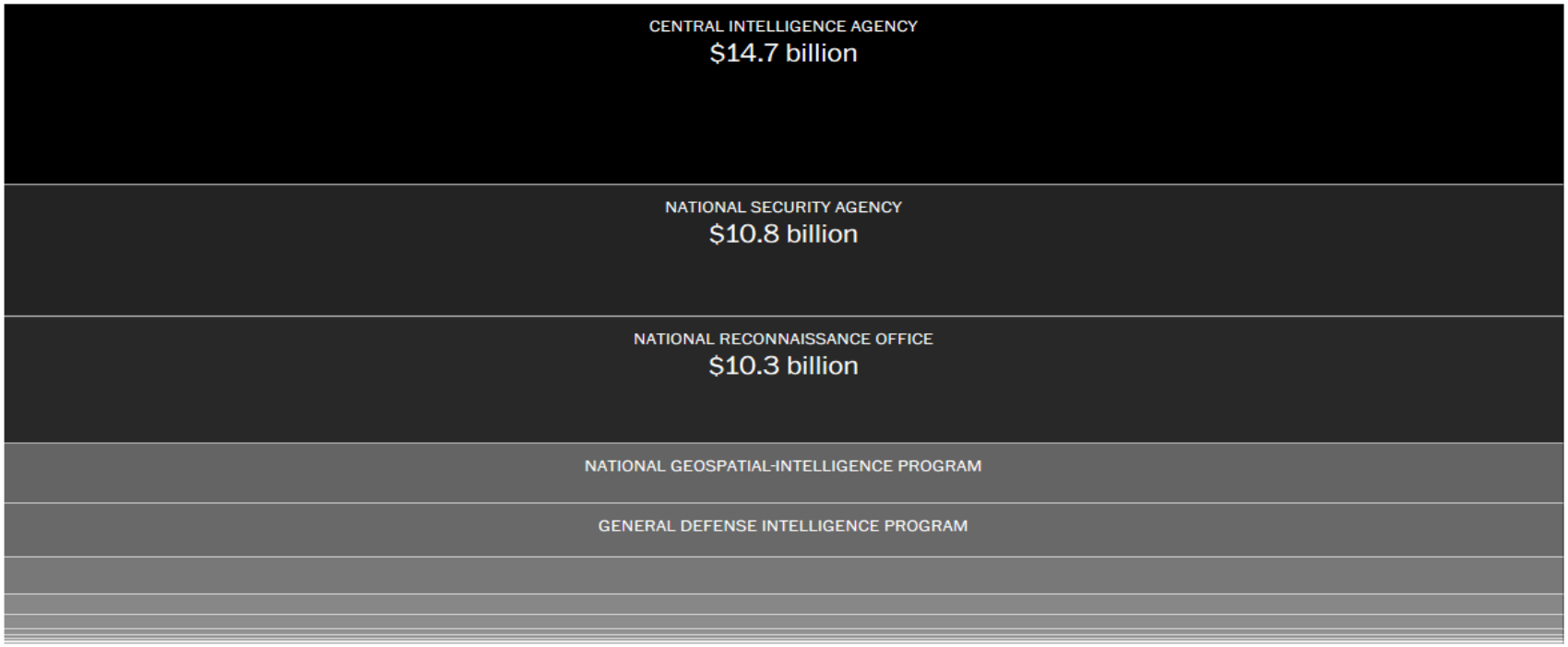
Budget&Funding

The Total Budget

The Washington Post SHARE COMMENT

Funding the intelligence program

The CIA, NSA and National Reconnaissance Office (NRO) receive more than 68 percent of the black budget. The National Geospatial-Intelligence Program's (NGP) budget has grown over 100 percent since 2004.



http://apps.washingtonpost.com/g/page/national/inside-the-2013-us-intelligence-black-budget/420/

Operation Socialist – Bics

Belgacom International Carrier Services

Belgacom gehört zu den großen und wichtigen Telekommunikationsunternehmen Europas, da zu ihren Kunden auch die Europäische Kommission, der Europarat und das Europaparlament gehören

Die *GCHQ* griff dazu gezielt die Computer von 6 hochrangigen Mitarbeiter via *„sinkhole attack“* an und übernahm deren Rechner

Aus einer durch Snowden veröffentlichten Präsentation der GCHQ geht hervor, dass die *GCHQ* kurz davor war, die zentralen GRX RouterSysteme des belgischen Unternehmens zu übernehmen. Und wenn diese Hürde genommen wäre, wollte man darangehen, mit weiteren MIT-Angriffen die Daten von Smartphone-Nutzern abzuschöpfen

Global Information Grid
Gigantische Datenmengen

Das Utah Data Center: BLUFFDALE. Quelle: Wired.

Die Speicherkapazität dieses DataCenters
wird in Yotabyte gemessen:

1,000 gigabytes is a terabyte.
1,000 terabytes is a petabyte.
1,000 petabytes is an exabyte.
1,000 exabytes is a zettabyte.
1,000 zettabytes is a yottabyte.

Umgerechnet auf die Weltbevölkerung entspräche dies einem Datenvolumen von etwa 140 Gigabyte - 1,4 Megabyte pro Person. Damit wird der Schritt in die komplette Überwachung und Speicherung der weltweiten Kommunikation möglich.

Die Datenmenge, die derzeit im Rahmen der US-Überwachung anfällt beträgt 29 PetaBytes pro Tag

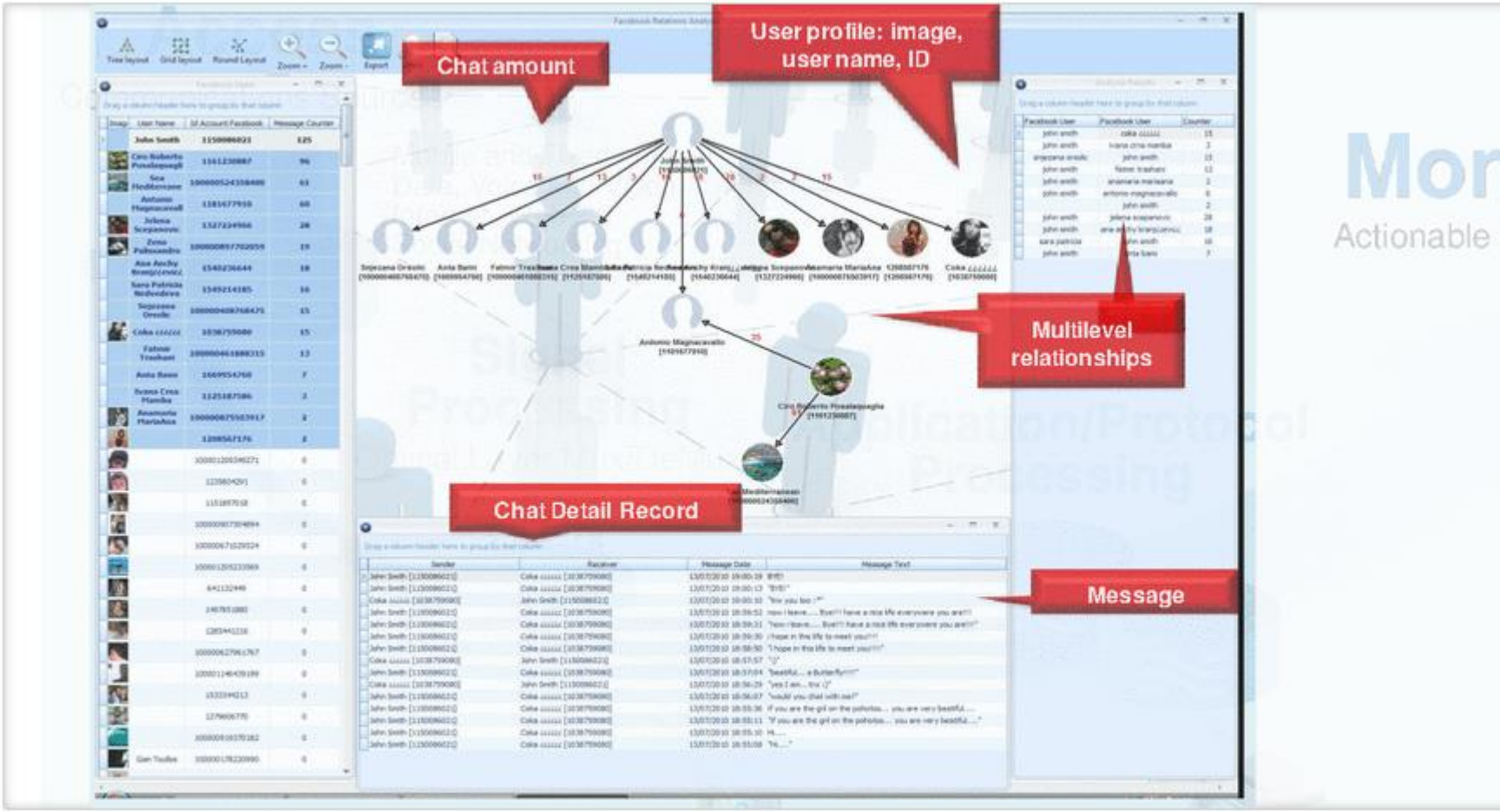
Ein einziges Yottabyte sind 360 Milliarden mal so viele Daten wie alle Stasi-Unterlagen der Gauck Behörde.

In der Gauck-Behörde sind laut eigenen Angaben 111.200 Regalmeter Unterlagen von der Stasi. Bei 25 Millionen Bytes pro Regalmeter sind das 2,8 Terabyte – und geht damit auf eine handelsübliche Festplatte.
Das Global Information Grid der USA speichert unter anderem im Datencenter in Utah eine Datenmenge, die in Yottabytes gemessen wird. Ein einziges Yottabyte sind 360 Milliarden mal so viele Daten wie alle Stasi-Unterlagen.

In Relation der DDR-Einwohnerzahl zur gesamten Weltbevölkerung heute sind das 6,5 Millionen mal mehr Daten – pro Person.

Technologien dafür gibt es zu kaufen

Facebook interception and analysis



Who do you know? Who do you speak to most often? What do you say to your friends? What do they say about you? Glimmerglass advertises the capab traffic and analyse Facebook accounts, uncovering huge amounts of personal information about individuals and the people they know. This is a screens 'Facebook Relations Analysis' software platform.

https://www.documentcloud.org/documents/409165-55-201110-iss-iad-t1-glimmerglass.html#document/p11/a67831

Lavabit - verschlüsselter eMail Dienst !!

UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA

FILED
JUN 10 2013
CLERK, U.S. DISTRICT COURT

IN RE APPLICATION OF THE
UNITED STATES OF AMERICA FOR
AN ORDER PURSUANT TO
18 U.S.C. § 2703(d)

MISC. NO. 1:13 EC 254

Filed Under Seal

ORDER

The United States has submitted an application pursuant to 18 U.S.C. § 2703(d), requesting that the Court issue an Order requiring Lavabit LLC, an electronic communications service provider and/or a remote computing service located in Dallas, TX, to disclose the records and other information described in Attachment A to this Order.

The Court finds that the United States has offered specific and articulable facts showing that there are reasonable grounds to believe that the records or other information sought are relevant and material to an ongoing criminal investigation.

Am 8. August 2013 wurde Lavabit geschlossen und die Seite wurde durch eine Nachricht ersetzt, dass der Betreiber nicht erklären DÜRFE, warum er den Dienst beendet habe. Er sammele Spenden, um am United States Court of Appeals for the Fourth Circuit – einem Bundesberufungsgericht – für seine verfassungsgemäß zustehenden Rechte zu kämpfen.[6]

Von wem sprechen wir ?

Government Communications Headquarters (GCHQ)hat die Aufgabe der Sicherung der elektronischen Kommunikation und Computersysteme des Vereinigten Königreichs.

Dies wird durch die Entwicklung eigener Chiffren (auch Kryptoalgorithmen genannt) sichergestellt. CESG erfand in den 1970er Jahren die Public-Key-Kryptographie, hielt dies aber bis ins Jahr 1997 geheim. Später wurde dieses Verfahren unter dem Namen RSA von Ronald L. Rivest, Adi Shamir und Leonard Adleman nochmals entdeckt.

GCHQ betreibt in engster Zusammenarbeit mit der amerikanischen National Security Agency und anderen angelsächsischen Organisationen (sogenannte UK/USA/CA/AU/NZ-Allianz) ein weltumspannendes System zur technischen Nachrichtengewinnung = „five eyes“

Government Communications Headquarters
— GCHQ —

GCHQ

Aufsichtsbehörde(n)	Foreign and Commonwealth Office
Gründung	1919 als Government Code and Cypher School
Hauptsitz	Cheltenham
Behördenleitung	Sir Iain Lobban
Website	www.gchq.gov.uk

Britische Programme

Tempora:

„Mastering the Internet“
„Global Telecoms Exploitation“
und fortführend (Muscular, Genie….)

Unter dem Namen Tempora überwacht die britische Regierungsbehörde Government Communications Headquarters (GCHQ) den **kompletten** Telekommunikations- und Internet-Datenverkehr, den sie bekommen kann. Mindestens alle Internet-Knotenpunkte und Kabel, die durch das Vereinigte Königreich gehen. Der komplette Inhalt wird für mindestens drei Tage gespeichert, Verbindungsdaten mindestens einen Monat lang.

Zum gesetzlichen Auftrag der britischen Geheimdienste gehört explizit das „economic well-being“ der britischen Wirtschaft !

Tempora ist der erste „ich speichere alles“ (Full take) Ansatz

d.h. JEDES Datenpaket das über Britische Infrastrukturen läuft oder von Ihnen erfasst wird - Wird gespeichert !

http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa

Ja – dürfen´s den das ?

TOP SECRET // COMINT // NOFORN//20291130

Relationships & Authorities

- Leverage unique key corporate partnerships to gain access to high-capacity international fiber-optic cables, switches and/or routers throughout the world
- Collection on U.S. soil is conducted under three different authorities:
  - Transit Authority: Collection of foreign intelligence communications which originate and terminate in foreign countries, but traverse U.S. territory
  - Foreign Intelligence Surveillance Act (FISA): Court ordered collection (NSA/FBI/FISA Court)
  - FISA Amendment Act of 2008 (FAA): Surveillance in the US when the target is reasonably believed to be foreign

TOP SECRET // COMINT // NOFORN//20291130

3

Yes we (S)can !

Foreign Intelligence Surveillance Act of 1978

Long title	An Act to authorize electronic surveillance to obtain foreign intelligence information.
Colloquial acronym(s)	FISA
Enacted by the	95th United States Congress
Effective	October 25, 1978
Citations	
Public Law	95-511
Stat.	92 Stat. 1783
Codification	
Title(s) amended	50 U.S.C.: War and National Defense
U.S.C. sections created	Chapter 36 § 1801 *et seq.*
Legislative history	

- **Introduced in the Senate as** S. 1566 **by** Edward Kennedy (D–MA) **on** May 18, 1977
- **Committee consideration by:** Senate Select Committee on Intelligence, Committee on the Judiciary
- **Passed the Senate on** March 20, 1978 (95-1)
- **Passed the House on** September 7, 1978 (246-128)
- **Reported by the joint conference committee on** October 5, 1978; **agreed to by the Senate on** October 9, 1978 (Without objection) **and by the House on** October 12, 1978 (226-176)
- **Signed into law by President** Jimmy Carter **on** October 25, 1978

Major amendments

USA PATRIOT Act
Protect America Act of 2007
FISA Amendments Act of 2008

V • T • E

https://en.wikipedia.org/wiki/Foreign_Intelligence_Surveillance_Act