

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 milliarden schweren 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 of communication methods and associated s
Brazilian President Dilma Rousseff and her



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 Kurz
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
&Energeministeriums

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 or 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 |

Iceland
Italy
Japan
Luxenberg
Netherlands
Norway
Poland
Portugal
South Korea
Spain
Sweden
Switzerland
Turkey

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.

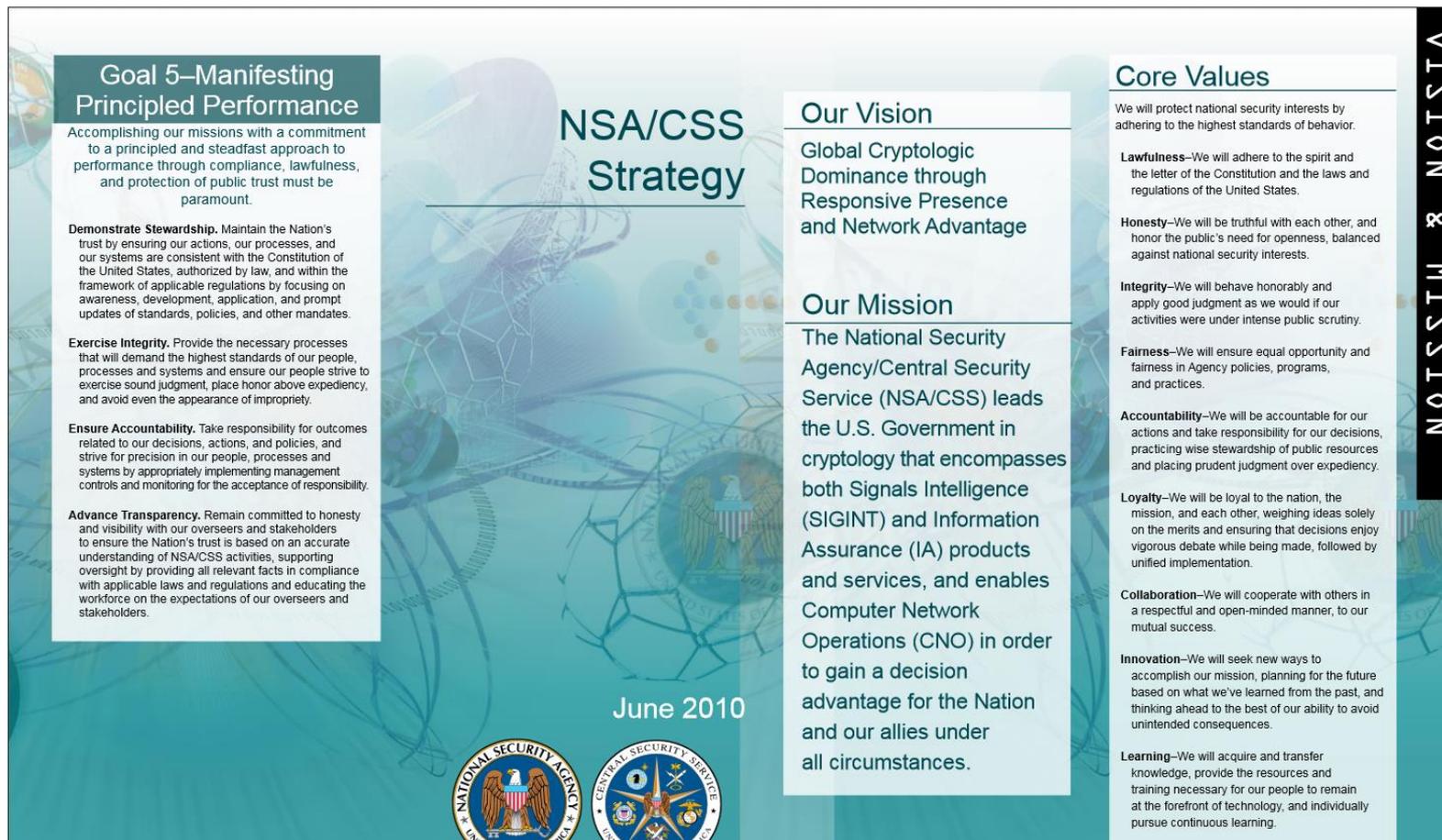
| National Security Agency — NSA — | |
|---|--|
|  | |
| Staatliche Ebene | Bund |
| Aufsichtsbehörde(n) | United States Department of Defense |
| Gründung | 4. November 1952 |
| Hauptsitz | Crypto City, Fort Meade, Maryland, USA |
| Behördenleitung | DIRNSA Gen. Keith B. Alexander ^[1] Deputy DIRNSA 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.

Strategie wird klar kommuniziert



The image shows the cover of the NSA/CSS Strategy document. It features a blue and white color scheme with a background of abstract geometric patterns and a globe. The title 'NSA/CSS Strategy' is prominently displayed in the center. Below the title, the date 'June 2010' is visible. At the bottom, the official seals of the National Security Agency (NSA) and the Central Security Service (CSS) are shown. The document is organized into several key sections: Goal 5, Core Values, Our Vision, and Our Mission. A vertical banner on the right side reads 'VISION & MISSION'.

Goal 5—Manifesting Principled Performance

Accomplishing our missions with a commitment to a principled and steadfast approach to performance through compliance, lawfulness, and protection of public trust must be paramount.

Demonstrate Stewardship. Maintain the Nation's trust by ensuring our actions, our processes, and our systems are consistent with the Constitution of the United States, authorized by law, and within the framework of applicable regulations by focusing on awareness, development, application, and prompt updates of standards, policies, and other mandates.

Exercise Integrity. Provide the necessary processes that will demand the highest standards of our people, processes and systems and ensure our people strive to exercise sound judgment, place honor above expediency, and avoid even the appearance of impropriety.

Ensure Accountability. Take responsibility for outcomes related to our decisions, actions, and policies, and strive for precision in our people, processes and systems by appropriately implementing management controls and monitoring for the acceptance of responsibility.

Advance Transparency. Remain committed to honesty and visibility with our overseers and stakeholders to ensure the Nation's trust is based on an accurate understanding of NSA/CSS activities, supporting oversight by providing all relevant facts in compliance with applicable laws and regulations and educating the workforce on the expectations of our overseers and stakeholders.

NSA/CSS Strategy

June 2010

Our Vision

Global Cryptologic Dominance through Responsive Presence and Network Advantage

Our Mission

The National Security Agency/Central Security Service (NSA/CSS) leads the U.S. Government in cryptology that encompasses both Signals Intelligence (SIGINT) and Information Assurance (IA) products and services, and enables Computer Network Operations (CNO) in order to gain a decision advantage for the Nation and our allies under all circumstances.

Core Values

We will protect national security interests by adhering to the highest standards of behavior.

Lawfulness—We will adhere to the spirit and the letter of the Constitution and the laws and regulations of the United States.

Honesty—We will be truthful with each other, and honor the public's need for openness, balanced against national security interests.

Integrity—We will behave honorably and apply good judgment as we would if our activities were under intense public scrutiny.

Fairness—We will ensure equal opportunity and fairness in Agency policies, programs, and practices.

Accountability—We will be accountable for our actions and take responsibility for our decisions, practicing wise stewardship of public resources and placing prudent judgment over expediency.

Loyalty—We will be loyal to the nation, the mission, and each other, weighing ideas solely on the merits and ensuring that decisions enjoy vigorous debate while being made, followed by unified implementation.

Collaboration—We will cooperate with others in a respectful and open-minded manner, to our mutual success.

Innovation—We will seek new ways to accomplish our mission, planning for the future based on what we've learned from the past, and thinking ahead to the best of our ability to avoid unintended consequences.

Learning—We will acquire and transfer knowledge, provide the resources and training necessary for our people to remain at the forefront of technology, and individually pursue continuous learning.

VISION & MISSION

Globale kryptographische Vorherrschaft durch Allgegenwertige Präsenz und Netztechnologischen Vorsprung



Bevors losgeht..



PRISM war nicht der Anfang von SigInt (Signal Intelligence)

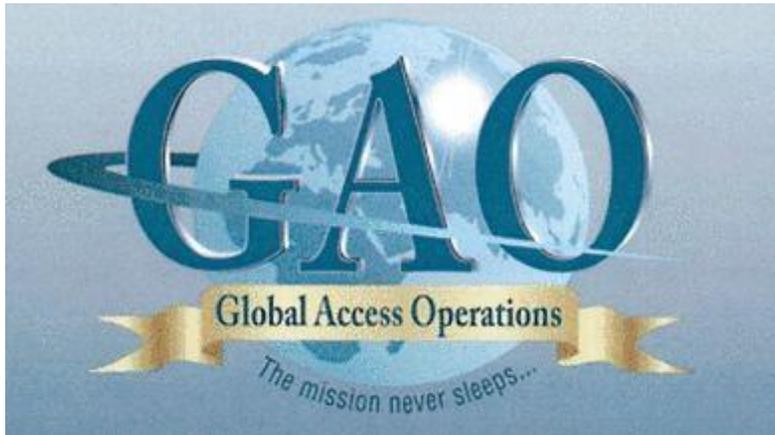
PRISM ist nur EIN Teilprogramm von VIELEN das im Zuge der SigInt entwickelt und eingesetzt wurde bzw wird

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:

Global Cryptologic Dominance through
Responsive Presence and Network Advantage





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: $2,5 \cdot 10^{18}$ 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”](#).

Praktisch: U.S. as Worlds Telecommunications Backbone

TOP SECRET//SI//ORCON//NOFORN

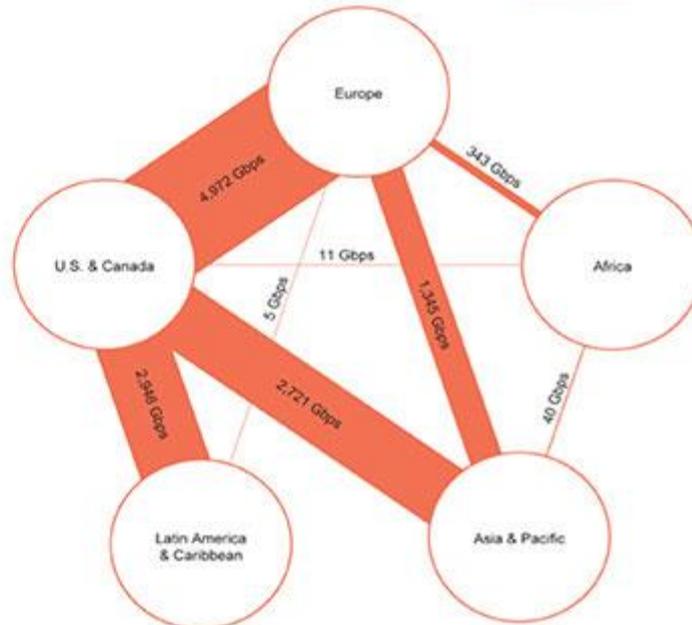


(TS//SI//NF) Introduction

U.S. as World's Telecommunications Backbone



- Much of the world's communications flow through the U.S.
- A target's phone call, e-mail or chat will take the **cheapest** path, **not the physically most direct** path – you can't always predict the path.
- Your target's communications could easily be flowing into and through the U.S.



International Internet Regional Bandwidth Capacity in 2011

Source: Telegeography Research

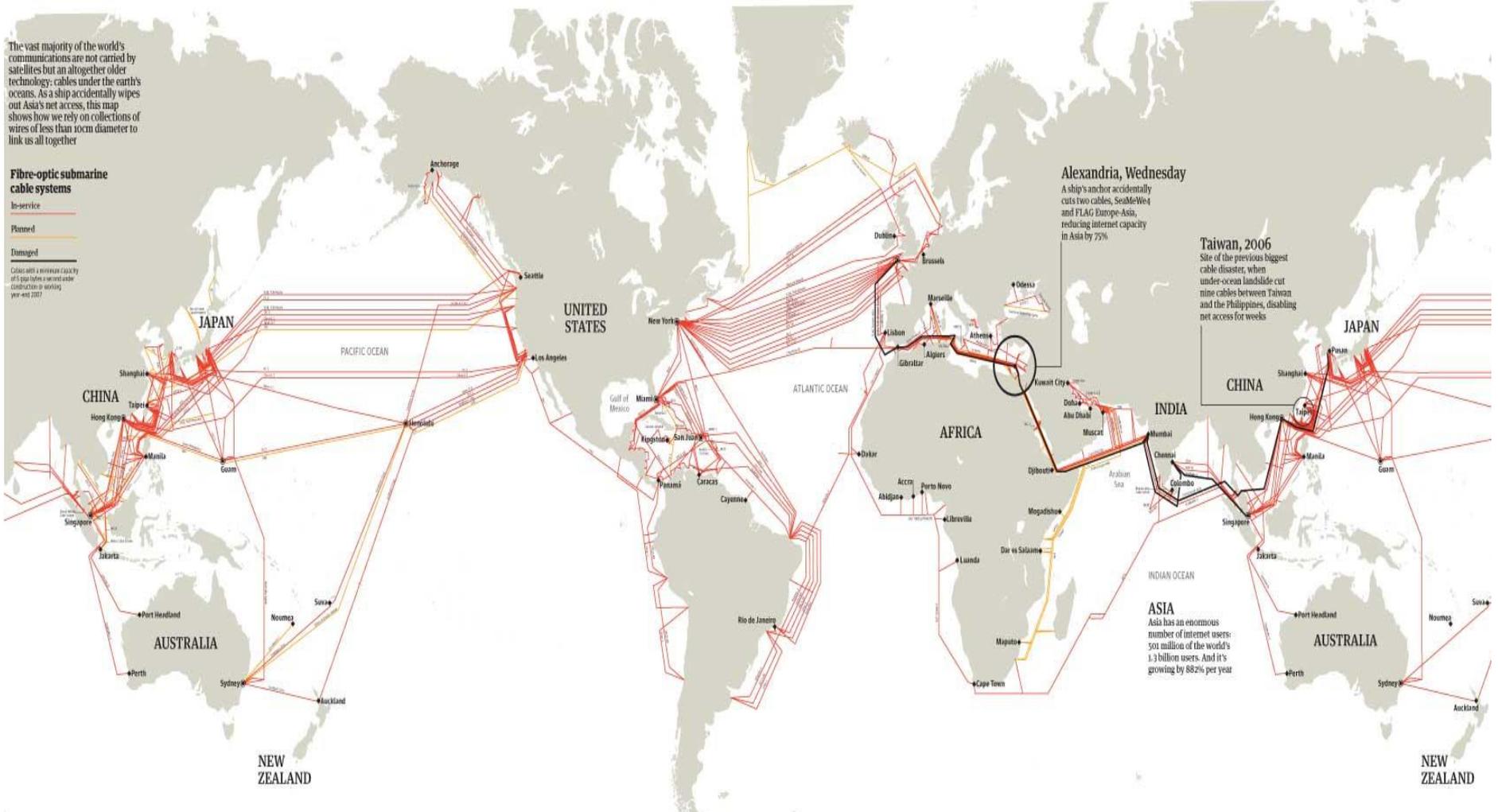
TOP SECRET//SI//ORCON//NOFORN

The internet's undersea world

The vast majority of the world's communications are not carried by satellites but an altogether older technology: cables under the earth's oceans. As a ship accidentally wipes out Asia's net access, this map shows how we rely on collections of wires of less than 10cm diameter to link us all together

Fibre-optic submarine cable systems
 In-service
 Planned
 Damaged

Cables with a maximum capacity of 1.5 petabits a second are indicated by a wavy line
 Construction in working year-end 2017



Alexandria, Wednesday
 A ship's anchor accidentally cuts two cables, SeaMe-We4 and FLAG Europe-Asia, reducing internet capacity in Asia by 75%

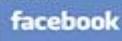
Taiwan, 2006
 Site of the previous biggest cable disaster, when under-ocean landslide cut nine cables between Taiwan and the Philippines, disabling net access for weeks

ASIA
 Asia has an enormous number of internet users: 500 million of the world's 1.3 billion users. And it's growing by 88% per year

Special Sources Operations



TOP SECRET//SI//ORCON//NOFORN



(TS//SI//NF)

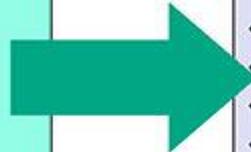
PRISM Collection Details



Current Providers

What Will You Receive in Collection
(Surveillance and Stored Comms)?
It varies by provider. In general:

- Microsoft (Hotmail, etc.)
- Google
- Yahoo!
- Facebook
- PalTalk
- YouTube
- Skype
- AOL
- Apple



- E-mail
- Chat – video, voice
- Videos
- Photos
- Stored data
- VoIP
- File transfers
- Video Conferencing
- Notifications of target activity – logins, etc.
- Online Social Networking details
- **Special Requests**

Complete list and details on PRISM web page:
Go PRISMFAA

TOP SECRET//SI//ORCON//NOFORN

Dürfen NICHT kommunizieren – sind per Gesetz verpflichtete JEDE Nachrichtendienstlichen Zugriff geheim zu halten !! Auch Noten amerikanischer Hersteller NICHT mit Behörden zu kooperieren oder ungesetzlich zu handeln sind SINNLLOS



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.



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.,,

Dishfire&Prefer

Rund 200 Mio SMS / Tag



TOP SECRET//COMINT//REL TO USA, FVEY//20320108

(U//FOUO) PREFER



Identification & Extraction April 2011

(S//SI//REL) 194 Million Messages Collected by DISHFIRE per Day, Including

- (S//SI//REL) VCARDS → names+; (113,672 average extracted daily) sometimes DNI link (email) to DNR (telephony) as well as images
- (S//SI//REL) Geocoordinates (76,142 daily avg; hex-encoded 10,432)
 - Requests by people for route info
 - Setting up meetings at a location
 - Tracking information: e.g., [REDACTED] (12,809)
 - Comma Separated Formats (33,020)
- (S//SI//REL) Missed Calls → contact chaining (5,058,114)
- (S//SI//REL) SIM Card Changes → IMSI/IMEI links (6,017,901)
- (S//SI//REL) Roaming information → border crossings (1,658,025)
- (S//SI//REL) Travel (5,314)
 - Itinerary including multiple flights
 - Changes: cancellations, reschedules, delays
- (S//SI//REL) Financial Transactions:
 - Credit card transactions: correlate credit cards to individuals (61,488)
 - Money transfers (social networks) – Phone to Phone (630,846)
 - Track financial information (account activity – bank transaction) (115,480)
- (S//SI//REL) Passwords (pending); Other Requests?

TOP SECRET//COMINT//REL TO USA, FVEY//20320108

8

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

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?

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)

TOP SECRET STRAP1

BULLRUN Bottom Line

- Groundbreaking capabilities
- Extremely fragile
- Do not ask about or speculate on sources or methods underpinning BULLRUN successes
- Indoctrination required for access to secure COI

PTD "We penetrate targets' defences."

 This information is exempt from disclosure under the Freedom of Information Act 2000 and may be subject to exemption under other UK information legislation. Refer disclosure requests to GCHQ on 01242 221491 x30306 (non-sec) or email infoleg@gchq

© Crown Copyright. All rights reserved.

TOP SECRET STRAP1

Response to improving security

- For the past decade, NSA has lead an aggressive, multi-pronged effort to break widely used Internet encryption technologies
- Cryptanalytic capabilities are now coming on line
- Vast amounts of encrypted Internet data which have up till now been discarded are now exploitable
- Major new processing systems, SIGDEV efforts and tasking must be put in place to capitalize on this opportunity

PTD "We penetrate targets' defences."



This information is exempt from disclosure under the Freedom of Information Act 2000 and may be subject to exemption under other UK information legislation. Refer disclosure requests to GCHQ on 01242 221491 x0308 (non-sec) or email infoleg@gchq

© Crown Copyright. All rights reserved.

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

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.



10.Security Day 2014

Vielen Dank

Budget&Funding

The Total Budget

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.

CENTRAL INTELLIGENCE AGENCY
\$14.7 billion

NATIONAL SECURITY AGENCY
\$10.8 billion

NATIONAL RECONNAISSANCE OFFICE
\$10.3 billion

NATIONAL GEOSPATIAL-INTELLIGENCE PROGRAM

GENERAL DEFENSE INTELLIGENCE PROGRAM

Budget Deficit:
1,267 Billion -19% +877%

Receipts 2.567 Trillion +19% +8%

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

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.



Das Utah Data Center: BLUFFDALE. Quelle: [Wired](#).

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 Datacenter 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

The screenshot displays the Facebook Relations Analysis software interface. It features a central network graph with nodes representing users and edges representing relationships. Red callout boxes highlight key features: 'Chat amount' (a red box pointing to the graph), 'User profile: image, user name, ID' (a red box pointing to a user profile), 'Multilevel relationships' (a red box pointing to a complex network structure), and 'Message' (a red box pointing to a chat detail record). The interface includes a sidebar with a list of users, a top navigation bar with options like 'Tree layout', 'Grid layout', and 'Round Layout', and a bottom section for 'Chat Detail Record' showing a table of messages.

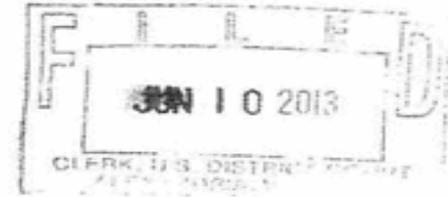
| Sender | Receiver | Message Date | Message Text |
|------------------------|------------------------|--------------------------|--|
| John Smith [130098621] | Cika [130098621] | 13/01/2012 18:00:28 (8) | "Hi" |
| John Smith [130098621] | Cika [130098621] | 13/01/2012 18:00:13 (9) | "Hi" |
| Cika [130098621] | John Smith [130098621] | 13/01/2012 18:00:10 (10) | "Hi you too :)" |
| John Smith [130098621] | Cika [130098621] | 13/01/2012 18:00:52 (11) | "Hi I have... But I have a nice life everywhere you are!!" |
| John Smith [130098621] | Cika [130098621] | 13/01/2012 18:00:31 (12) | "Hi I have... But I have a nice life everywhere you are!!" |
| John Smith [130098621] | Cika [130098621] | 13/01/2012 18:00:30 (13) | "Hope in the life to meet you!!" |
| John Smith [130098621] | Cika [130098621] | 13/01/2012 18:00:30 (14) | "I hope in the life to meet you!!" |
| Cika [130098621] | John Smith [130098621] | 13/01/2012 18:01:07 (15) | "Hi" |
| John Smith [130098621] | Cika [130098621] | 13/01/2012 18:01:04 (16) | "Sweet! - a Butter-fun!!" |
| Cika [130098621] | John Smith [130098621] | 13/01/2012 18:00:29 (17) | "Yes I am... the :)" |
| John Smith [130098621] | Cika [130098621] | 13/01/2012 18:00:07 (18) | "Would you chat with me?" |
| John Smith [130098621] | Cika [130098621] | 13/01/2012 18:00:36 (19) | "If you are the girl on the photos... you are very beautiful..." |
| John Smith [130098621] | Cika [130098621] | 13/01/2012 18:00:11 (20) | "If you are the girl on the photos... you are very beautiful..." |
| John Smith [130098621] | Cika [130098621] | 13/01/2012 18:00:10 (21) | "Hi..." |
| John Smith [130098621] | Cika [130098621] | 13/01/2012 18:00:08 (22) | "Hi..." |

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 capabilities of its 'Facebook Relations Analysis' software platform.



Lavabit - verschlüsselter eMail Dienst !!

UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA



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 sammelte 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 —



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

MASTERING THE INTERNET (MTI)

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 !



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 <i>et seq.</i> |

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