

Umesh Heendeniya
P. O. Box 5104
Spring Hill, FL-34611
(508)-630-6757
umeshheendeniyavsthefbi@gmail.com
Thursday, October 18, 2018
via certified mail

David M. Hardy
Chief, Record/Information Dissemination Section, Records Management Division
Federal Bureau of Investigation (FBI)
170 Marcel Drive
Winchester, VA 22602-4843
(540) 868-4500 | foiparequest@ic.fbi.gov
(540) 868-4997, (540) 868-4391 (Fax).

**Re: Request for information pursuant to The Privacy Act (PA)-- 5 U.S.C. §552a-- and
The Freedom of Information Act (FOIA)-- 5 U.S.C. §552.**

Dear FBI Public Records Officer:

Pursuant to The Privacy Act (PA)-- 5 U.S.C. §552a-- and The Freedom of Information Act (FOIA)-- 5 U.S.C. §552-- I seek access to and copies of all records about me which you have in your possession. If any of the information/records/data requested is redacted, please indicate under what specific statutory exemption(s) this was done. However, I will expect you to release the non-exempt, segregable portions to me as the law requires. Please indicate the name, title, and contact information of the person/official to whom I can appeal the redaction, and the appeal procedure available to me under the law.

But first, I will provide a little background information that may assist you in finding the records and data that I seek. From approx. Sept., 2010 to April, 2013, I was following the Muslim faith while living in Massachusetts. From approx. Sept. 2010 to approx. early Fall, 2012, I had an online, long distance, romantic relationship with a lady, whose name-- on information and belief-- was [REDACTED]. On information and belief, Ms. [REDACTED] lived in **Isfahan** (the name of the city is alternatively spelled as **Esfahan**), **Iran**. The email addresses she used, that I was aware of, were [REDACTED].

During this time period, Ms. [REDACTED] and I communicated using numerous communication technologies, including but not limited to, Skype chat and video, Yahoo Instant

Messenger chat and video, email, U.S. postal mail, long distance cell-phone and land-line communication, various social media platforms, etc.

Then, approximately one year after she and I broke-off our long distance relationship, the former NSA contractor Edward Snowden's whistle-blowing took place in June, 2013. As you can imagine, I was horrified and deeply concerned by the fact that some of mine and Ms. [REDACTED]'s romantic communication that involved nude video, and sexually explicit, intimate and very private conversations that were only supposed to be between me and her (and NOT to be seen or heard by any other person), were probably seen and heard by various U.S. law enforcement agency officers/agents and various U.S. intelligence agency officers, and were now in the possession of various U.S. Government Agencies such as The FBI, The NSA, The DHS, etc.

In addition, I have strong reasons to believe that from approx., Sept., 2010 to approx. Sunday, May 18, 2014 (including when I was communicating with Ms. [REDACTED]), I was subjected to surveillance-- both physically and electronically-- by agents, troopers, deputies, and/or officers of the Joint Terrorism Task Force (JTTF) based in Massachusetts, and possibly other law enforcement agencies (such as The Middlesex County Sheriffs Office, The Berkshire County Sheriffs Office, and The Massachusetts State Police).

Also, I have strong reasons to believe that from approx., Monday, May 19, 2014 to the present, I was subjected to and continue to be subjected to both physical and electronic surveillance by agents, troopers, deputies, and/or officers of the Joint Terrorism Task Force (JTTF) based in Florida, and possibly other law enforcement agencies (such as The Hernando County Sheriffs Office and The Florida State Police).

Having given the background information contained in the prior 3 paragraphs, I note that The Privacy Act and The Freedom of Information Act (FOIA/PA) require federal agencies to acknowledge requests promptly and to respond in good faith; thus, I would appreciate your cooperation.

If any of the below requested information is redacted, please indicate under what specific statutory exemption(s) this was done. However, I will expect you to release the non-exempt, segregable portions to me as the law requires. Please indicate the name, title, and contact information of the person/official to whom I can appeal the redaction, and the appeal procedure available to me under the law.

If any of the requested information is denied, as you are probably aware, The Privacy Act and The Freedom of Information Act (FOIA/PA) require federal agencies to state the basis for any claim that the 'requested records are exempt' and to provide a specific statutory citation to the claimed exemption. However, I will expect you to release all of the non-exempt, segregable portions to me as the law requires. Additionally, as a requester, I have the right to a written statement explaining with particularity the reasons for a conclusion by the agency that the records are exempt. Please indicate the name, title, and contact information of the person/official to whom I can appeal the denial of particular records, and the appeal procedure available to me under the law. Naturally, I will expect you to release all of otherwise exempt material.

I seek access to and copies of all records and data about me which you have in your possession, including, but not limited to:

- (1). All information [including, but not limited to; inter-agency and intra-agency email, voice-mail, text messages, facsimile, social media posts, letters and memoranda, field notes, reports, content of all face-to-face communication, administrative subpoenas (including National Security Letters), search warrants, etc.; that were hand-written, typed, voice recorded, and/or recorded by imaging devices such as cameras, video recorders, etc.; by FBI officials/personnel, ATF officials/personnel, DHS/USCIS/ICE officials/personnel, Department of Defense officials/personnel, government and private-contract officials/personnel associated with intelligence activities and collection of data in furtherance of intelligence activities, and any and all other federal, state, county, and municipal law enforcement and corrections officers/agents].**
- (2). Files, documents (i.e., letters, field-notes, memoranda, and reports), records, data (including audio and video data), and all records/information/data obtained by using various legal authorities (such as, for example, FISA, Section 702 of the FISA Act, Section 215 of the USA PATRIOT Act, Executive Order 12333, etc.).**
- (3). Files, documents (i.e., letters, field-notes, memoranda, and reports), records, data (including audio and video data), and all records/information/data prepared by any federal, state, county, and/or municipal agency/officer that are in the possession and/or control of the FBI, including but not limited to, the following:**
 - (i). Field notes, Form-302's, and other reports and memoranda prepared as a consequence**

of the physical surveillance of me between Sept. 01, 2010 to the present.

- (ii). Threat Assessment Report(s) or similar document(s) prepared by the FBI and/or any other federal, state, county, or municipal agency officer/official.
- (iii). Memorandum of Activities (MoA) or similar document(s) prepared by the FBI and/or any other federal, state, county, or municipal agency officer/official.
- (iv). Intelligence Assessment(s) or similar document(s) prepared by the FBI and/or any other federal, state, county, or municipal agency officer/official.
- (v). Reports, field-notes, and memoranda received from other law enforcement and corrections officers/agencies.
- (4). Files, documents (i.e., letters, field-notes, memoranda, and reports), records, data (including audio and video data), and all records/information/data that were intercepted and/or collected and/or examined and/or stored that pertain to:
 - (i). My Skype chats/messaging and video communication.
 - (ii). My Yahoo Instant Messenger chats/messaging and video communication.
 - (iii). All of my email accounts in the Yahoo and Google/Gmail email systems.
 - (iv). My social media accounts such as Facebook, Twitter, Google-Plus, MySpace, and Orkut.
 - (v). My electronic document/file repositories such as Scribd, SlideShare, Box, Youtube, Dropbox, Google Drive, Microsoft Skydrive, and DocStoc.
 - (vi) My chats/messaging and video communication that involved the following messaging accounts:
 - (a). Yahoo: umesh1989.
 - (b). AOL: umesh1989 and umesh1989@yahoo.com.
 - (c). ICQ: umesh1989@yahoo.com and ICQ #593270360.
 - (d). MSN: umesh1989@yahoo.com.
 - (e). Google Talk: umesh.heendeniya.
 - (f). Skype: umesh.heendeniya.
- (5). Interception and/or collection and/or examination of my cellphone communication (including international phone calls) and my land-line phone communication (including international land-line phone calls).
- (6). Electronic surveillance using means such as GPS technology, sting ray type technology, and means that utilize the signal/connection of my smart-phone such as SS7 Signaling System No. 7.
- (7). Files, documents (i.e., letters, field-notes, memoranda, and reports), records, data (including audio and video data), and all records/information/data that were

intercepted and/or collected and/or examined and/or stored using the following methods and technologies:

- (i). Data from Cell Towers (such as, for example: 'Cellphone Location Data' a/k/a 'Cell Site Location Information (CSLI)', Cell Location Data, Cell-Site Records, Cell Tower Dumps).
- (ii). Data from Trap and Trace device(s) and Pen Register(s).
- (8). Surveillance and collection of records/data/information using Cell-Site Simulators/IMSI Catchers such as Stingray and similar technologies.
- (9). Any and all records and data "obtained" by the Federal Bureau of Investigation's Remote Operations Unit (ROU) or similar department, by accessing my computers, tablets, and smart-phones.
- (10). Files, documents (i.e., letters, field-notes, memoranda, and reports), records, data (including audio and video data), and all records/information/data pertaining to me that were obtained by using various surveillance programs identified/named and briefly described in the double-sided 44 pages that are attached and demarcated as EXHIBITS 1-3.
- (11). Records and data (including audio and video data) shared with the FBI either directly or indirectly (or shared *via* the NSA intermediary) by the FVEY Five Eyes alliance partners pertaining to me. These records and data were intercepted and/or collected, and/or examined, and/or stored by the FBI, ATF, DHS/USCIS/ICE, NSA, FVEY Five Eyes alliance partners between September 01, 2010 to the present.
- (12). If I am listed in the FBI's Violent Gang and Terrorist Organization File (VGTOF) computer database, then all records and data in VGTOF that contain my name, my date of birth, my social security number, or my address.
- (13). All records and data contained in the files of your agency (in either paper format or electronic format) and specifically under my name and/pr identifier assigned to my name. The records sought shall include but not be limited to, your agency's compiled file(s) containing: (i) Investigation and investigatory reports, (ii) Reports and evidentiary and scientific information and findings, (iii) Final and closing investigation reports, (iv) Reports and information from all other federal and state governmental agencies which were acquired by your agency during any investigation, (v) Any and all

information, data, and reports not otherwise exempt by statutes or regulations (adopted by your agency consistent with the above referenced statutes).

- (14). All records and data that pertain to me in any manner, that are in the following data management or records systems: The computer case tracking systems, the Legal Information Office Network System ("LIONS"), the Tracking Assistance for the Legal Office Network ("TALON"), the Central Records System (CRS), the Electronic surveillance ("ELSUR") indices, the 'N-Force' case management system, the Treasury Enforcement Communications System ("TECS"), TECS II, the National Crime Information Center (NCIC), the USPIIS Security Investigations Service Center records, the Mail Theft and Financial Crimes Database ("FCD"), the Inspection Service Integrated Information System ("ISIIS"), the Automated Targeting System (ATS), the National Automated Immigration Lookout System II (NAILS II), the Central Index System (CIS), the Deportable Alien Control System (DACS), the National Security Entry Exit Registration System (NSEERS), the Interagency Border Inspection System (IBIS), the Computer Linked Application Information Management System (CLAIMS), the Non-immigrant Information System (NIIS), the Criminal Alien Investigation System (CAIS), the Enforcement Case Tracking System (ENFORCE) Removal Module (EREM), the Western Identification Network (WIN), the National Law Enforcement Telecommunications System (Nlets), the Terrorist Screening Database (TSDB), the No-Fly List, the Terrorist Screening Records System (TSRS), the Consular Lookout and Support System (CLASS), the Terrorist Screening Center Encounter Information (TSCEI), the DHS Watchlist Service (WLS), and the USCIS Fraud Detection and National Security (FDNS).

I would like to receive the information on paper, or in electronic form as Adobe PDF format documents. However, in the case of any audio and/or video data/information, please place those in CDs and/or DVDs.

To assist you with your search for the records I seek, I'm providing my identification information as well as my home address, which are given below:

Name: **Umesh Heendeniya.**

Sex: **Male.**

D.O.B.: [REDACTED]

Social Sec. No.: [REDACTED]

Home Address: [REDACTED]. I have

lived at this address from mid-May, 2014, after relocating from Massachusetts.

P. O. Box Address: **P. O. Box 5104, Spring Hill (Hernando County), FL-34611.** I have had this post office box from approx. January, 2015 to the present.

When I lived in Massachusetts, from Sept., 2010 to mid-2014, I lived at 2 addresses, and they are given below:

188 Stearns Road, Marlborough (Middlesex County), MA-01752.

and

321 River Street, North Adams (Berkshire County), MA-01247.

Please mail all of the above requested information, that's made under The Privacy Act and The Freedom of Information Act (FOIA/PA), to:

**Umesh Heendeniya
P. O. Box 5104
Spring Hill, FL-34611.**


In order to help determine my status to assess fees, you should know that I am an individual seeking information for personal use and not for commercial use. I request a waiver of all fees for this request since the disclosure of the information I seek is not primarily in my commercial interest, and is likely to contribute significantly to public understanding of the operations or activities of the government, thus making the disclosure a matter of public interest.

If I don't receive the requested information from you-- *per* The Privacy Act and The Freedom of Information Act (FOIA/PA) -- by Wednesday, November 14, 2018, I will take that to mean that 'The Federal Bureau of Investigation' and its officials/personnel are refusing to provide me the requested information, and that thereby, they are informing me that they are refusing to comply with The Privacy Act and The Freedom of Information Act (FOIA/PA) requirements.

If you have any questions regarding this request, please contact me by my email, which is: umeshheendeniyavsthefbi@gmail.com (do not contact me by phone). I look forward to receiving your prompt reply, and I thank you in advance for your assistance.

Sincerely,

Dated : Oct. 18, 2018.



Umesh Heendeniya

umeshheendeniyavsthefbi@gmail.com

I hereby certify that on this 18th day of October, 2018.

Personally appeared before me the signer and subject of the above document, who signed or attested to the same in my presence, and presented the following form of identification as proof of his identity:

☒ Driver's License or Govt. Identification Card.

☐ U.S. Passport.

☐ U.S. Military ID Card.

☐ State Identification Card.

☐ Social Security Card.

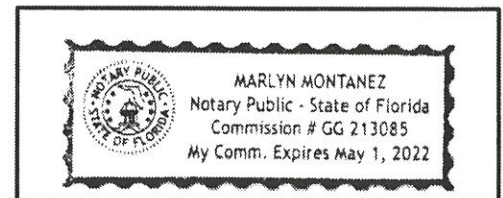
☐ Birth Certificate.

☐ Other: _____
(Provide description)

Notary Public: Marlyn Montanez
(Print Name)

My Commission Expires: 5/1/2022

Notary Public Signature: Marlyn Montanez



Reserved for Notary Seal

U.S Department of Justice

Certification of Identity

FORM APPROVED OMB NO. 1103-0016
EXPIRES 10/31/13

Privacy Act Statement. In accordance with 28 CFR Section 16.41(d) personal data sufficient to identify the individuals submitting requests by mail under the Privacy Act of 1974, 5 U.S.C. Section 552a, is required. The purpose of this solicitation is to ensure that the records of individuals who are the subject of U.S. Department of Justice systems of records are not wrongfully disclosed by the Department. Requests will not be processed if this information is not furnished. False information on this form may subject the requester to criminal penalties under 18 U.S.C. Section 1001 and/or 5 U.S.C. Section 552a(i)(3).

Public reporting burden for this collection of information is estimated to average 0.50 hours per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Suggestions for reducing this burden may be submitted to the Office of Information and Regulatory Affairs, Office of Management and Budget, Public Use Reports Project (1103-0016), Washington, DC 20503.

Full Name of Requester ¹ Umesh [REDACTED] HeendeniyaCitizenship Status ² Permanent Resident Social Security Number ³ [REDACTED]

Current Address [REDACTED] Florida [REDACTED]

Date of Birth [REDACTED] Place of Birth Sri Lanka

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct, and that I am the person named above, and I understand that any falsification of this statement is punishable under the provisions of 18 U.S.C. Section 1001 by a fine of not more than \$10,000 or by imprisonment of not more than five years or both, and that requesting or obtaining any record(s) under false pretenses is punishable under the provisions of 5 U.S.C. 552a(i)(3) by a fine of not more than \$5,000.

Signature ⁴ [REDACTED] Date Oct. 18, 2018**OPTIONAL: Authorization to Release Information to Another Person**

This form is also to be completed by a requester who is authorizing information relating to himself or herself to be released to another person.

Further, pursuant to 5 U.S.C. Section 552a(b), I authorize the U.S. Department of Justice to release any and all information relating to me to:

Print or Type Name

¹ Name of individual who is the subject of the record(s) sought.

² Individual submitting a request under the Privacy Act of 1974 must be either "a citizen of the United States or an alien lawfully admitted for permanent residence," pursuant to 5 U.S.C. Section 552a(a)(2). Requests will be processed as Freedom of Information Act requests pursuant to 5 U.S.C. Section 552, rather than Privacy Act requests, for individuals who are not United States citizens or aliens lawfully admitted for permanent residence.

³ Providing your social security number is voluntary. You are asked to provide your social security number only to facilitate the identification of records relating to you. Without your social security number, the Department may be unable to locate any or all records pertaining to you.

⁴ Signature of individual who is the subject of the record sought.

EXHIBIT 1



Journalism in the Public Interest

Receive our top stories daily

Subscribe

[Home](#) [Investigations](#) [Data](#) [MuckReads](#) [Get Involved](#) [About Us](#)

Surveillance

The NSA Revelations All in One Chart

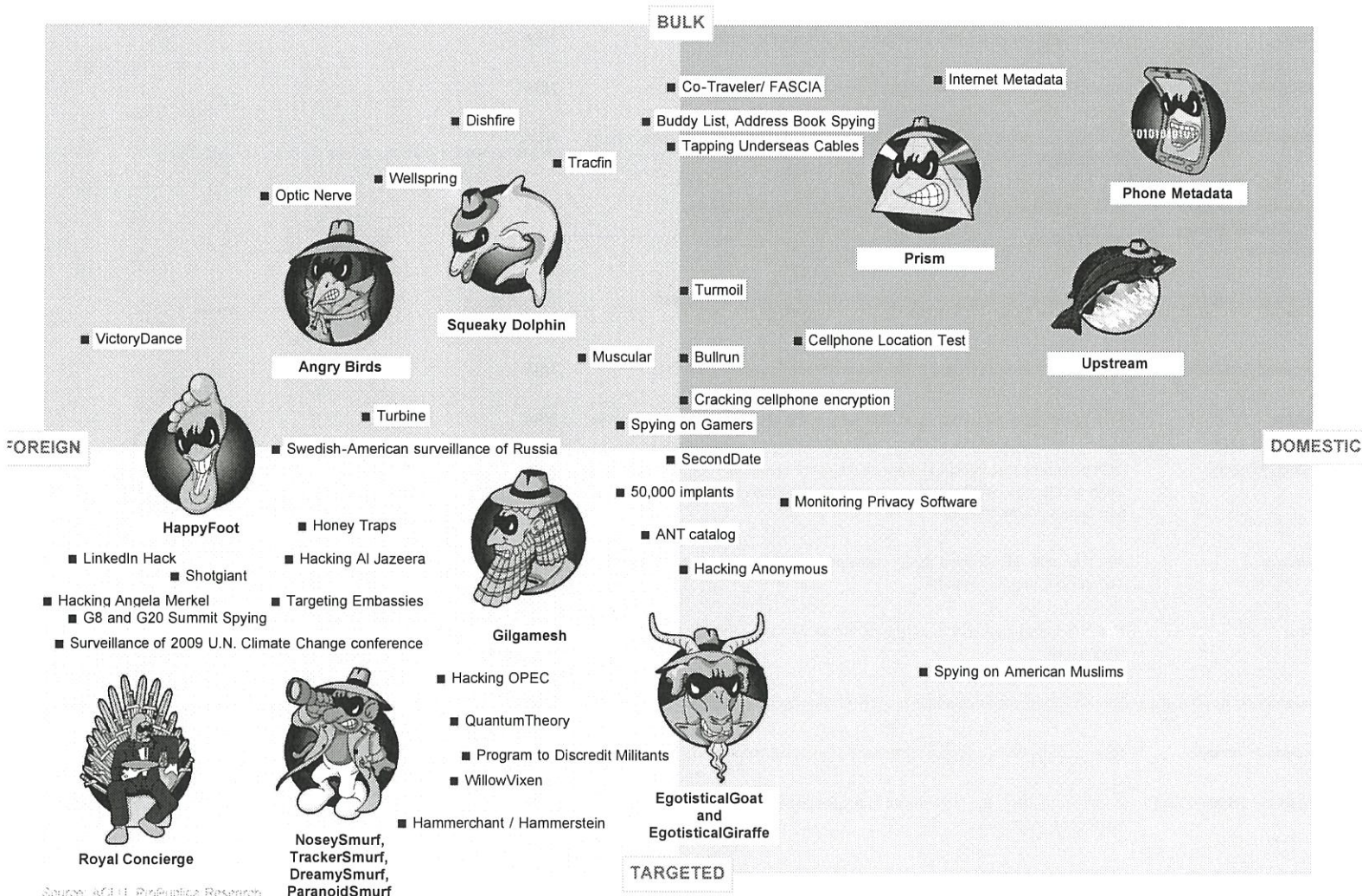
By Julia Angwin and Jeff Larson, ProPublica, illustrations by Alberto Cairo, special to ProPublica
Published June 30, 2014

Tweet

This is a plot of the NSA programs revealed in the past year according to whether they are bulk or targeted, and whether the targets of surveillance are foreign or domestic. Most of the programs fall squarely into the agency's stated mission of foreign surveillance, but some – particularly those that are both domestic and broad-sweeping – are more controversial.

Just as with the New York Magazine approval matrix that served as our inspiration, the placement of each program is based on judgments and is approximate.

For more details, read our [FAQ](#) or listen to our [podcast](#). Also, take our [quiz](#) to test your NSA knowledge.



Source: NSA, ProPublica Research

Program Name	Description	Agency	Bulk?	Targeted?	Foreign?	Domestic?
VictoryDance	The NSA tested a technique for using drones to map "the Wi-Fi fingerprint of nearly every major town in Yemen."	NSA				

Hammerchant / Hammerstein	NSA programs to spy on data sent through voice over IP calls and Virtual Private Networks.	NSA
ANT catalog	Various techniques - with names like IronChef and DropoutJeep - used to inject surveillance software into Apple, Cisco, Dell and other products.	NSA
Cracking cellphone encryption	The NSA has the capability to defeat a widely-used cellphone encryption technology.	NSA
Optic Nerve	A British program to bulk collect images from Yahoo webcam chats: "it would appear that a surprising number of people use webcam conversations to show intimate parts of their body to the other person."	NSA
Swedish-American surveillance of Russia	A Swedish-American effort to spy on Russian leadership.	NSA
Gilgamesh	An NSA program to geolocate people's SIM cards via Predator drones.	NSA
Buddy List, Address Book Spying	An NSA effort to collect hundreds of millions of contact lists from email and instant messaging accounts.	NSA
Hacking Anonymous	A British spy unit to monitor hacktivists such as the group Anonymous.	NSA
Co-Traveler/ FASCIA	The NSA collected 5 billion records a day of cellphone locations worldwide.	NSA
Hacking OPEC	NSA and GCHQ programs to infiltrate the OPEC oil cartel	NSA and GCHQ
Tracfin	Tracfin amasses gigabytes of data about credit card purchases.	NSA
Wellspring	An NSA program to collect images from emails for facial recognition.	NSA
Honey Traps	A British spy effort to conduct covert Internet investigations, including sexual "honey-traps."	NSA
Surveillance of 2009 U.N. Climate Change conference	NSA surveillance of the 2009 U.N. Climate Change conference.	NSA
Spying on Gamers	The NSA and GCHQ monitored games including World of Warcraft.	NSA and GCHQ
Targeting Embassies	An NSA operation targeting the Italian embassy in Washington D.C.	NSA
Dishfire	An NSA program to collect up to 200 million text messages a day worldwide.	NSA
QuantumTheory	NSA programs that inject spyware onto targets' computers through so-called "man on the side" attacks. Variants include QuantumInsert, QuantumBiscuit, and QuantumSmackdown.	NSA
Muscular	The NSA and GCHQ have jointly operated a program to intercept data from Yahoo and Google networks.	NSA and GCHQ
Prism	The Prism program collects data from the servers of U.S. technology companies.	NSA
Hacking Angela Merkel	The NSA targeted German Chancellor Angela Merkel's cellphone.	NSA
Hacking Al Jazeera	NSA hacked into Al Jazeera's internal communications system.	NSA
Cellphone Location Test	In 2010 and 2011, the NSA tested bulk collection of location data from Americans cellphones.	NSA
Tapping Underseas Cables	Companies - including BT, Vodafone, and Verizon Business - gave GCHQ access to their underseas cables.	NSA
Angry Birds	NSA and GCHQ efforts to intercept information transmitted by phone apps, including Angry Birds.	NSA and GCHQ
Royal Concierge	A GCHQ program to monitor hotel reservations for "governmental hard targets."	NSA

Monitoring Privacy Software	The NSA collected information about users of privacy software including visitors to two Massachusetts Institute of Technology computers.	NSA
SecondDate	A so-called man-in-the-middle attack for "mass exploitation" of traffic "passing through network choke points" as well as "surgical target selection."	NSA
NoseySmurf, TrackerSmurf, DreamySmurf, ParanoidSmurf	The Smurf programs get inside iPhones and Android devices, turning on microphones, tracking location, and managing power.	NSA
Internet Metadata	A program, ended in 2011, to sweep up domestic Internet metadata such as the To and From fields in emails.	NSA
EgotisticalGoat and EgotisticalGiraffe	The Egotistical animal programs are techniques to track users of Tor anonymizing software.	NSA
Program to Discredit Militants	An NSA effort to spy on targets' online sexual activity.	NSA
LinkedIn Hack	Engineers at a Belgian telcom were infected with malware, via a technique called Quantuminsert, when they pulled up their LinkedIn profiles.	NSA
Bullrun	Joint NSA and GCHQ effort to undermine and weaken cryptography standards and tools.	NSA and GCHQ
Shotgiant	An NSA program to break into Chinese-owned Huawei networks and products.	NSA
WillowVixen	An NSA technique to deploy malware by sending out emails that trick targets into clicking a malicious link.	NSA
Turmoil	A large network of clandestine surveillance "sensors" to collect data from satellites, cables, and microwave communications around the world.	NSA
Turbine	A network of active command and control servers around the world that can be used for "industrial scale exploitation."	NSA
Squeaky Dolphin	A British effort to monitor YouTube video views, URLs "liked" on Facebook and Blogger visits.	NSA
Spying on American Muslims	FBI monitored e-mail of 200 Americans including prominent Muslims such as a former Bush Administration official, two professors, an attorney and the leader of a Muslim civil rights group.	NSA
Upstream	The Upstream program collects communications transiting the Internet via commercial partners codenamed Fairview, Stormbrew, Blarney, and Oakstar.	NSA
50,000 implants	An NSA map of the 50,000 computers worldwide it has implanted with surveillance malware	NSA
G8 and G20 Summit Spying	The NSA conducted surveillance during the 2010 G8 and G20 summits in Canada.	NSA
Phone Metadata	The well-known and controversial program to collect phone call records - aka metadata - of nearly all Americans.	NSA
HappyFoot	An NSA effort to use Web cookies and data from phone apps to identify users' devices and physical locations.	NSA

EXHIBIT 2

Short list of NSA,GQHC and other Governments Surveillance Program Names and Functions...A Must Read

Published on April 19, 2016

Michael Holt | 

Federal Government Veterans Administration IT Cybersecurity Whistleblower, Not a Extremist ,Terrorist or Radical

Posted for Public Health, Welfare and Safety under FOIA

For now, you can check out ProPublica's FAQ on the NSA's Surveillance Programs. And also be sure to check out the Electronic Frontier Foundation's timeline of NSA Domestic Spying, which reveals how persistent and common the issues we're running into now really are.

Updated 2/11/2015: Added entries for EONBLUE,

~~*Updated 4/14/2014:*~~ *Updated TAO, UPSTREAM Programs – separated into SIGAD w/ sub-sections on FORNSAT, Upstream collection, MYSTIC, & Tempora.*

Added entries for DISHFIRE, GILGAMESH, SHENANIGANS, Section 215 FISC

order, Special Collection Service, CO-TRAVELER, CHALKFUN, TAPERLAY,

FASCIA, Treasure Map, Royal Concierge, 30-08 warrants, CSIS, CSEC,

HAPPYFOOT, Squeaky Dolphin, Smurfs, ANT, Implants, TURBINE,

QUANTUMHAND, SECONDDATE, FOXACID,

QUANTUMCOPPER/QUANTUMSKY, Menwith Hill.

~~*Updated 11/7/2013:*~~ *Added entries for MUSCULAR, INCENSER, MAINWAY,*

Executive Order 12333, Parallel Construction

~~*Updated 8/2/2013:*~~ *Updated entry on X-KeyScore with new information. Added entries for Trafficthief, Pinwale, MARINA, and Tailored Access Operations.*

30-08 warrants – The warrant required by Section 21 of the CSIS Act which states that the agency must receive the approval of a federal judge to actively investigate a potential threat to national security. In the past these warrants were permitted while it was presumed the targeting and surveillance would be carried out by the Canadian intelligence agencies (CSIS and CSEC) within Canadian borders. What occurred however was that CSEC, with the approved warrant, then let other intelligence agencies from the Five Eyes perform the jobs of targeting Canadian citizens.

ANT – AKA Advanced or Access Network Technology and home to the infamous ANT Catalog, ANT is a sub-division of the TAO that acts as the NSA's own in-house version of Radio Shack. They specialize in computer engineering hacks that can exploit back doors in corporate networking devices or imbed "implants" so deep inside a computer's memory that it's nearly impossible to remove. Part of their inventory are various programs specifically tailored to certain networking routers or hard drives. One example is FEEDTROUGH, an implant that can break through the firewalls of popular corporate security company Juniper Networks. It imbeds itself so well in the software architecture that it can remain in place, smuggling hidden NSA

surveillance and programs into the computer, even if the computer is wiped and reset.

ANT have access to software which can exploit the products of a whole host of international and US-based companies including Western Digital, Seagate, Maxtor and Samsung. [Read more.](#)

Boundless Informant – A data-mining tool used by the NSA for recording and analyzing the amount of metadata collected globally. The program displays information in a heat map (with green being countries least subjected to surveillance and yellow, orange, and red being the most) and allows agents to check in real time what data has been collected from a particular country. Agents can then go through and see the specific details of that collected data.

CHALKFUN – A search tool used with the FASCIA repository to discover past or current location of mobile phones. Similar to **TAPERLAY**.

Example of a CHALKFUN query

CSIS – The Canadian Security Intelligence Service is the Canadian intelligence service focused on HUMINT and foreign espionage. It was founded in 1984 and is overseen by the Security Intelligence Review Committee. It, alongside CSEC, is an active partner in the Five Eyes relationship and routinely shares intelligence with its counter-parts in the United States.

CSEC – The Communications Security Establishment Canada is the branch of the Canadian intelligence service which works with foreign SIGINT and protects government communications. Established shortly after World War 2, the agency's existence was only admitted after a Fifth Estate expose in 1974. It was an active partner in the ECHELON project and routinely shares intelligence information with the other Five Eyes countries. Since 2001 and the passing of the Anti-Terrorism Act, the agency has only grown and can now monitor foreign communications that begin or end in Canada, similar to the NSA's own policy.

CO-TRAVELER – A tool used for tracking targeted individuals and marking any unknown associates that may cross their path. Most communication devices, when powered on, give off a signal that registers with a provider and/or goes through a cell tower. NSA programs scoop up this metadata globally, amounting to about 5 billion records a day, and dump it in the FASCIA repository. From there, CO-TRAVELER analyses the metadata and using a device's Global Cellphone-Tower Identifier (GCID) tracks a targeted individual's movements through a city or region. What CO-TRAVELER watches for specifically is the consistency of other GCIDs or devices moving with the primary target across a distance. This way the NSA can map potential associates of a targeted individual or establish relationships and movement patterns. CO-TRAVELER is sophisticated in its mapping abilities, with the ability to track when a new device connects to a network after another disappears for the last time, discover waypoints of common activity between certain devices, and predict a target's potential movements with mapping technology similar to turn-by-turn navigation systems. [Read more.](#) [Summary of DNR and DNI Co-Travel Analytics.](#) [WaPo: How the NSA is tracking people right now.](#)

DISHFIRE – A program which sweeps up all SMS text messages, including those of

untargeted individuals; that is persons or smartphones not currently under surveillance.

The specific collection method is unknown, but it has been collecting a high volume of text messages for some time. In April 2011, the program was collecting and storing around 194 million text messages a day. The reach of the program is global, with only US numbers being removed or minimized within the collection. DISHFIRE works in conjunction with subprogram known as ‘Prefer’, which analyzes messages for automated or “System Generated” texts and uses those alongside metadata to extract information. For example, the Prefer subprogram extracted more than 5 million missed-call alerts, which can be officially used for contact-chaining analysis (figuring out relations between people and when they contact each other). Border crossings were pinpointed through the 1.6 million roaming alerts, and geolocation data was acquired through simple requests for meetings or travel directions. The combination of collected SMS metadata and Prefer’s system generated information gives the NSA and its partners a wealth of historical information for agents to leaf through once an individual becomes targeted.

ECHELON – The popular term for the software system used in the collection and analysis of signals intelligence, under the directive of the Five Eyes countries. Originally created to monitor military and diplomatic communications of the Soviet Union and Eastern Bloc countries in the Cold War, it relied on intercepting signals produced by high frequency radio, public switched telephone networks, or satellites by the way of microwave links. It did this by employing a number of ground stations, such as RAF Menwith Hill, positioned around the world to tap into downlinks and major communication hubs. Since the rise of fiber-optics, phone line and satellite transmissions have been relied upon less for moving internet traffic and general communication, making the old ECHELON ground station system somewhat obsolete, and giving rise to a new era of signal interception. Now, the collection of signals intelligence relies on tapping directly into the fiber-optic hubs, such as **BLARNEY** or **FAIRVIEW**.

Edward Snowden – A thirty year old IT specialist contracted to the NSA through the private consulting firm Booz Allen Hamilton. He had access to a multitude of internal NSA documents which detailed surveillance programs being used to collect data on Americans. He obtained a number of these documents in secret and leaked them to blogger and journalist Glenn Greenwald who, in conjunction with the British newspaper The Guardian, are slowly publishing these documents for the public. On May 20th he fled the United States for Hong Kong, performing interviews to reveal his intentions, before departing for Moscow on June 23rd. On June 14th he was charged with espionage and theft of government property and is currently seeking asylum in Ecuador.

EONBLUE –

EvilOlive – AKA One-End Foreign (1EF) solution, it was a program introduced in December 2012 and was described as “broadening the scope” of what metadata the NSA could collect. This would include all the information of say an email, without the actual content of the email itself. The 1EF solution refers to how the metadata collected

always has at least one end of the communication coming from outside of the US. This program, and a partner program called ShellTrumpet, apparently opened the floodgates for the NSA, increasing data intercepts by 75 percent.

Executive Order 12333 – The executive order signed by Ronald Reagan which defines the responsibilities of the US intelligence agencies and directs other federal agencies to co-operate with their demands. Full text found [here](#).

FASCIA – The NSA repository containing trillions of device location data from all over the world including Americans, compiled by a wide range of collection methods. As many as 5 billion records a day move into repository a day and about 27 terabytes worth over 7 months. FASCIA deals only with location metadata and not the content of calls or devices themselves. It acts as a kind of pool of data which other search and database programs then sift through automatically or when an agent queries. This “pool” is at the center of the bulk data collection debate, with NSA officials calling the service essential and legal because it does not target any specific individual. Read on what exactly FASCIA contains.

FISA – The Foreign Intelligence Surveillance Act, first enacted in 1978, is the law which covers both the physical and electronic surveillance of foreign powers or individuals. It was meant to protect US citizens from being monitored without a specific warrant from a FISA court, which would only be assigned if there was evidence showing probable cause that the person monitored was interacting with a foreign power or terrorist organization. The FISA court is entirely secret and is subject to no oversight, hearing only the NSA or FBI’s testimony and evidence before issuing a warrant. In 2008, this act was amended in the FISA Amendments Act or FAA, which made it easier for the NSA to acquire the data of US citizens in bulk and without a warrant. Currently, the NSA only has to submit an annual general procedures document to the court which outlines how they go about eavesdropping without a warrant. Once the FISA court approves these guidelines, the NSA is then free to send directives to telephone and internet companies requesting any and all data on whomever the NSA decides, including US citizens, with no further input from the FISA court. As well, every thirty days, the FISA court is given an aggregate number of database searches on US domestic phone records. Read more details.

FISA Amendments Act (FAA) – OR New FISA. This act, passed by Congress in 2008 in light of George W. Bush’s own surveillance program, and renewed in late 2012, amended FISA so a warrant was no longer required by the NSA to monitor and eavesdrop on any call, email, or online chat *involving* a US citizen. Individual warrants are still required if the specific target is a US citizen or a telephone call is entirely domestic. This means that while Americans still have the protection of a warrant if they themselves are the subject of an investigation, they do not have this same protection if any of their data or communications go outside the US or to a foreign national. The result is that the NSA collects the data of Americans in bulk, monitoring communications that may only be tangibly related to or several degrees removed from a case. Surveillance of foreign persons still does not require any suspicion of a terrorist connection or criminal activity. In a hearing before the Senate Judiciary Committee in

"Indeed, the dragnet surveillance of Americans' international communications was one of the purposes of the Act. In advocating changes to FISA, the executive made clear that its aim was to enable broader surveillance of communications between individuals inside the United States and non-Americans abroad. See Hayden Testimony (stating, in debate preceding passage of FAA's predecessor statute, that certain communications "with one end in the United States" are the ones "that are most important to us"). Moreover, in advocating for the FAA, executive officials expressly sought the authority to engage in dragnet rather than individualized surveillance"

This amendment also granted legal immunity to private corporations who cooperated with the NSA in its surveillance efforts.

FOXACID – The NSA servers which QUANTUMHAND and SECONDDATE redirect to. FOXACID is part of the QUANTUM system which allows the NSA to spoof a target computer into believing it is on a certain website or connected to a certain server when it is really under NSA control and surveillance. It does this with split-second pings of data that come back quicker than the target's original pings, and by redirecting an unsuspecting user's traffic away from their intended server mid-connection.

GCHQ – The Government Communication Headquarters is the British intelligence agency tasked with signals intelligence and information assurance operations. Information collected by the GCHQ through their surveillance programs, like Tempora, are considered the largest of the Five Eyes, as they are freely able to collect information on the citizens of other foreign countries, and have little to no protections against the surveillance of their own citizens. As a member of the Five Eyes, the GCHQ and the NSA are closely linked, sharing much of the information which flows through their surveillance programs, as well as analysts used to sift through this information. This also ensures that while the NSA could potentially be blocked from collecting information on an individual US citizen, it can freely obtain that information from the GCHQ, who do not have the same restrictions.

GILGAMESH – A geolocation system attached to Predator drones. GILGAMESH works by spoofing the abilities of a cellphone tower, allowing a targeted individual's device to connect to it and in the process allowing the operators to discover the location of the individual to within 30 feet. The individual holding the connected SIM card or handset is then presumed to be the same individual they are targeting.

HAPPYFOOT – A program designed to search for data traffic generated by apps that incidentally transmit a device's location, such as for social media or game app purposes. Sometimes apps, in the process of performing their function like posting online or communicating with a developer's server, have to transmit metadata that includes the devices relative GPS location. HAPPYFOOT jumps on these keywords and data as they appear to map devices to locations, which can later be used to infer relations between devices or people.

Implants – A piece of software or hardware specially designed to be installed on a targeted computer or device and remain active without being detected. They are similar to computer viruses in this way but the majority of implants do not seek to spread or do damage. Instead they are primarily for surveillance, watching packets or computer

activity, and data interception. An example of a software implant would be

DROPOUTJEEP for Apple iPhones. An example of a hardware implant would be FIREWALK, used to filter Gigabit Ethernet traffic.

INCENSER – A program revealed alongside MUSUCLAR, INCENSER’s exact purpose is not yet known but it is described as being closely related to MUSCULAR.

MAINWAY – A database and data analysis tool, first uncovered in 2006, which focuses specifically on the metadata of the billions of telephone records which pass through the major telephony companies (AT&T and Verizon). It was initiated about seven months after the 9/11 attacks and has since compiled over two trillion pieces of phone records, which, as of June 2013, is stored for five years. The program has come under some legal pressure before, with the White House evoking the State Secrets Privilege to keep them at bay. The program was not approved by the FISA court and does not record call contents, only call metadata (date, numbers, recipients, length). The FISA court, as of August 29th 2013, released an opinion stating in relation to MAINWAY that “metadata that includes phone numbers, time and duration of calls is not protected by the Fourth Amendment, since the content of the calls is not accessed.” and that the program would be authorized under Section 215 of the Patriot Act. It has since been renewed in 90 day intervals multiple times.

MARINA – A database that works in conjunction with X-Keyscore, it seems to act as a sort of run-off database, holding metadata and full user content after it has expired in the main X-Keyscore database. It can hold this content for up to five years. **See X-Keyscore.**

Menwith Hill – A satellite signal interception base in Northern England, Menwith Hill is a major component of the TURBINE system and is jointly operated by the NSA and GCHQ. Menwith Hill is home to up to five QUANTUM programs intended to attack and exploit targeted computers and mobile devices.

Metadata – On an electronic device, every picture taken, text sent, call made, or any other data “action” has a hidden, underlying set of data associated with it. That data, used mainly for device-to-device communication and programming reasons, can list various things about the action you just performed. For an email it can be the sender and recipient’s name or email address, the date and time it was made, the servers it passed through to be delivered, and the type of content in the email. For a photo it can be the location the photo was taken at, the type of camera that took it, and the photo’s date and time. *The Guardian* posted this example of metadata from a single tweet, and while they highlighted details like the name, location, language, etc. you can also see other information included such as the actual text of the tweet, its embedded url, your following/follower/listed amount, and various ID numbers that could be used to trace that particular bit of information.

All of this is what is considered “metadata” and it is this information which the NSA has been vacuuming up from undersea cables and fiber-optics for a number of years. This metadata acts as a sort of library reference card for your actual data, giving the broad details (book’s name, author, shelf number, year of publication, etc.), but not actual content.

One of the main crux of the current debate is over whether collecting metadata alone is an invasion of privacy, whether it could be used to really watch you as an individual, or reveal private information about your life. From these examples we can see that, for example, while the NSA may not know that you texted Sally saying you snuck out of the house to meet Chad in the park after dark, they can easily infer from your text metadata that you may be out after your bed time. Or if you have been attempting to self-diagnose an illness or find a support group for a physical or emotional issue through Google or any number of online searches, the metadata from your internet browser is now safely stored somewhere in the NSA's servers, ready to be called upon at a moment's notice.

Recently German Green party politician Malte Spitz made six months of his telephone metadata available to the news site Zeit Online. From this data they created an easily navigable map of Mr. Spitz's movements as well as details of his calls, SMS, and internet connectivity time.

MoonLightPath – Metadata processing program similar to EvilOlive and ShellTrumpet which is expected to go online sometime in September 2013.

MUSCULAR – Source of the now infamous pencil diagram and NSA smiley, MUSCULAR is the backdoor entry to PRISM's friendly front door knocking. It originated as a partnership between the NSA and the GCHQ to intercept data between the servers of major internet companies like Google and Yahoo without their knowledge. Whereas PRISM is executed with the compliance of internet companies through US law, MUSCULAR instead taps directly into the connections between major data hubs overseas, snatching up information as it is synchronized between "clouds". These clouds are essentially data warehouses; large server banks which contain and share much of the information customers input into Google or Yahoo sites. For efficiency reasons, the entirety of a customer's data, including emails, address books, search history, audio, video and any pertaining metadata, (what may be defined as "their account") is passed between the servers as that data is accessed. Though one may be checking their contacts from the US, their line of connection to that information could pass to one of these servers outside the US. Or if one is travelling overseas, the information can be provided by a server closer to your location than one in the continental US. All this data housed and moving around outside US territory is particularly tempting to agencies like the NSA as it is outside the jurisdiction of the FISA regulations, so data on US citizens can be gathered without check or oversight. Once data is leached from the fiber optic lines or the servers themselves, it is placed into a buffer area for three to five days where it is screened and processed for useful information.

NSA – The National Security Agency is the US intelligence branch focused on signals intelligence and counter-intelligence, as well as the protection of government intelligence and information systems. They are mandated to collect and analyze as much foreign data as possible, including through clandestine methods. It has a long history of various surveillance methods going back through the Cold War and into the warrantless wiretap days of George W. Bush. The recent construction of its new data

center in Utah could see it be in possession of some of the largest storage and computing power in the world.

Parallel Construction – The process whereby law enforcement officials receive tips or information from NSA intelligence gathering to secure an arrest, before then “reconstructing” the investigative trail so as to hide the origins of the actual evidence from judicial review. This process has been performed for years by members of the DEA, FBI, CIA, DHS, and IRS to imprison and put pressure on various individuals. A division of the DEA, called the Special Operations Division (SOD), deals with handling FISA evidence and sharing it with various departments, while being beyond judicial review itself. The primary concern is that the process bypasses the defendant, prosecutor, and/or judge’s ability to review the origin and validity of evidence, particularly in pretrial, while also dolling out information intended for national security and terrorism purposes solely for use in criminal prosecutions. **This lack of oversight could leave criminal cases open to entrapment, bias, or simple mistakes.**

Comment: Everyone should take note

“Remember that the utilization of SOD cannot be revealed or discussed in any investigative function,” a document presented to agents reads. The document specifically directs agents to omit the SOD’s involvement from investigative reports, affidavits, discussions with prosecutors and courtroom testimony. Agents are instructed to then use “normal investigative techniques to recreate the information provided by SOD.”

Read more on Parallel Construction [here](#). See the EFF’s piece on ‘Intelligence Laundering’ [here](#). This process is currently under investigation by the DoJ.

Pinwale – A subset database of X-Keyscore which collects “interesting” content, most likely chosen by being filtered for specific dictionary or colloquial terms, which can then be stored and searched for up to five years. See **X-Keyscore**.

PRISM – The internal codename for one of many of the NSA’s surveillance programs, initiated in 2007 and under the jurisdiction of the FISA court. It is distinct from other NSA surveillance programs like BLARNEY, FAIRVIEW, OAKSTAR, and STORMBREW in that it does not deal with the “upstream” from underseas internet or fiber-optic cable, but works directly with private companies and their internal data servers to extract customer information. These private companies include Microsoft, Google, Apple, Yahoo!, Facebook, PalTalk, Facebook, Skype, and AOL. The information extracted can include emails, videos, voice or video chats, photos, VoIP calls, activity logs (log ins, setting changes, etc.), social networking details, and any other stored data. There has been some debate over how much “direct access” PRISM has to the servers of these private companies, ie whether PRISM can access internal data servers without the knowledge of those servers’ parent company. What appears to occur however is that when an NSA agent makes a query through PRISM, the company extracts any specific data relevant to the query and places it into a “dropbox” side-server, which PRISM then extracts and saves within the NSA’s own databases. The validity of this method is still under dispute.

Project Chess – A program set up in February 2011 between the owners of Skype (pre-Microsoft purchase) and the NSA which allowed security officials more direct and easy access to user information.

QUANTUMHAND – A malware attack known as the man-on-the-side technique, QUANTUMHAND detects when a computer attempts to connect to Facebook and signals back fake Facebook packets to the computer. To the user it looks like they are on the normal Facebook page when they are actually on an NSA imitation which siphons their internet and hard drive data as long as they're connected. See FOXACID.

QUANTUMSKY/QUANTUMCOPPER – QUANTUMSKY was first developed in 2004 and designed as a way of blocking access to certain specified sites.

QUANTUMCOPPER can corrupt a user's downloads and was first tested in 2008.

Royal Concierge – A GCHQ program for tracking the hotel reservations of travelling diplomats and retrieving information like booking time and location. It does this by skimming foreign cellphone and internet data for reservation confirmation texts or emails commonly sent out by the high-end hotels (for example, a hotel sending an email to a government domain like gov.xx would be flagged). The GCHQ alone is said to have some 350 upscale hotels around the world monitored for the comings and goings of government officials. Once the GCHQ knows of a reservation in advance it can be better prepared for more direct surveillance (such as wiretapping).

SECONDHAND – A malware attack known as the man-in-the-middle technique, SECONDHAND sits between a computer and the internet server it's trying to connect to and diverts the computer's traffic from the intended destination to an NSA FOXACID server. Once the user is connected to the NSA server, their computer can be infected with implants or sent other malicious data that can be used to harvest the hard drive data over time.

Section 215 FISC order – The section of the Foreign Intelligence Surveillance Court's order that defines the specifics of what telephony meta data can be collected. It is the order which periodically must be renewed by the FISC after review. On April 3rd, 2008, the section read,

Telephony meta data includes comprehensive communications routing information, including but not limited to session identifying information (e.g., originating and terminating telephone number, communications device identifier, etc.), trunk identifier, telephone calling card numbers, and time and duration of call.

Telephony meta data does not include the substantive content of any communication, as defined by 18 U.S.C. § 2510(8), or the name, address, or financial information of a subscriber or customer.

On August 19th, 2008 it was modified to,

Telephony meta data includes comprehensive communications routing information, including but not limited to session identifying information (e.g., originating and terminating telephone number, International Mobile Subscriber Identity (IMSI) numbers, International Mobile Station Equipment Identity (IMEI) etc.), trunk identifier, telephone calling card numbers, and time and duration of call. Telephony meta data does not include the substantive content of any communication, as defined by 18 U.S.C. § 2510(8), or the name, address, or financial information of a subscriber or customer.

and has been renewed since. h/t emptywheel.

Section 215 of the Patriot Act – Section 215 is the specific article in the Patriot Act, passed after 9/11 and renewed in 2011, that allows the FBI to order the turnover of “any tangible thing” relating to an investigation as long as they are business records (ie

Section 702 of the FISA Amendments Act – Section 702, renewed for five years in late 2012, is what allows the NSA to collect data on a wide scale, including foreign communications between the US and other countries, as long as the target is overseas. Warrants issued under the FISA Amendments Act (FAA) by the FISA court last up to 12 months at a time and specifically authorize the bulk collection of data, which can include communications of US citizens or people inside the US. The difference being that if they wanted to *intentionally* target one of those two groups, they would need another more specific warrant.

ShellTrumpet – An apparent partner program to EvilOlive, it was introduced either prior to or in December 2012, filtering incoming information for metadata. By the end of the month it had “processed its One Trillionth metadata record”, with almost half of that processed in 2012 alone.

SHENANIGANS – A CIA operation that uses a pod attached to aircraft to suck up information from any wireless routers, computers, smartphones, or other devices within range. Can be used to “fingerprint”, ie retain device and communication metadata, a region, as successfully shown in operation VICTORYDANCE, conducted in Yemen in 2012. Related to **GILGAMESH**. [Read more.](#)

SIGAD – Or “Signals Intelligence Address”, SIGADs are sources of information which the NSA can penetrate or extract data. SIGADs can be physical like TIMBERLINE and GCHQ Bude, or software like PRISM or MYSTIC. There are currently 10 known major SIGADs used by the NSA: DANCINGOASIS, FAIRVIEW, MYSTIC, OAKSTAR, RAMPART-A, RAMPART-M, RESOLUTETITAN, STORMBREW, TIMBERLINE, and WINDSTOP. Three (FAIRVIEW, STORMBREW, and TIMBERLINE) are located in the US. We do not know what they all do or whether that is the complete list, but most are involved in some kind of signals or data interception. For example, STORMBREW is the code-name for a SIGAD which sits on 27 telephone links known as OPC/DPC pairs (Originate and Destination points that transfer traffic from one provider’s network to another’s), collecting phone data that passes through those links. FAIRVIEW is a similar SIGAD which collects data from 860 OPC/DPC pairs. But these are not the only kind, as there are many types of SIGADs at the NSA’s disposal:

==Upstream collection – Upstream can be defined as the communication information flowing at the speed of light through undersea and fiber-optic cables serving as the backbone of the internet. It is how all online traffic crosses local, state, and national boundaries. Due to how the infrastructure of the internet is set up, almost all major internet traffic flows through the US or the UK at some point. Particularly for underseas cables, a large amount of them make landfall on the US and UK coasts. BLARNEY, OAKSTAR, and STORMBREW are examples of SIGADs which collect upstream data and stores it in databases like FASCIA. This gives the NSA a wide access to global internet and telephone communication data, which is later sifted through by agents on programs like X-Keyscore or by automated flagging programs like Pinwale or CO-TRAVELER. Details on the information the NSA is collecting. [Click here for more details on undersea cable tapping.](#) [Click here for a Google Maps-esque view of the](#)

world's underseas cables. Click here for more information on undersea cables

specifically.

==**FORNSAT** – A network of 13 stations operated by the NSA and its British partners, located around the world to intercept foreign satellite signals. The network is a mixture of new stations and leftovers from the ECHELON program. The most prominent stations are TIMBERLINE, located in Sugar Grove, W.VA, and GCHQ Bude, or Carboy, on the Cornwall coast. “Timberline and Carboy intercept high-priority communications traffic moving through communications satellites parked over the Atlantic. Together, these two stations covered much of a region that was of interest to [US] during the Cold War.” Many developing countries and governments still rely on satellites for data and telephone communication which is easily scooped up by these listening posts. The GCHQ Bude location also taps into many of the undersea internet cables just as they make landfall on the coast. Those cables include the Apollo (USA), TAT-3 (USA), CANTAT-1 (Canada), TAT-8 (USA and France – last used in 2002), TAT-14 (USA and Europe), AC-2 (USA), EIG (Europe and India) and GLO-1 (West Africa) lines. It was recently revealed the GCHQ Bude station was using access to these cables to collect data on a wide range of targets from the German government, to United Nations officials, American businesses, and foreign energy corporations. More on TIMBERLINE/Sugar Grove. More on GCHQ Bude.

==**MYSTIC** – A voice interception program which is designed to collect every single call routed from a certain country and storing the billions of calls it collects in a database for up to 30 days. The database works on a rolling buffer, removing older calls as newer ones come in. This enables the NSA to review the entirety of a phone conversation up to a month after it has taken place and without requiring that a target be marked in advanced. Although not every call is listened to, millions of voice clippings are said to be moved into long storage every month. MYSTIC became fully operational against its first country by 2011 and in last year's secret intelligence budget five other countries were identified as providing “comprehensive metadata access and content,” through MYSTIC, with another expected by last October. American communications with foreign persons can get swept in these collections to, and because they are done so incidentally, as per the NSA, the same protections that apply in the US do not apply abroad. These types of calls with one end in America were once deemed by former director Michael Hayden as “the most important” to the NSA during bulk collection. WaPo has a description of data collection under MYSTIC.

==**Tempora** – The GCHQ's equivalent of the NSA's upstream programs. However, instead of vacuuming up just metadata like its US cousins, Tempora also pulls actual data from at least 200 different undersea and fiber-optic cables, including such data as phone calls, emails from Gmail, Yahoo!, and Outlook, Google and Yahoo! searches, and direct messages sent through Facebook and Twitter. This amounts to an estimated 21 million gigabytes of intercepted data per day, requiring 300 GCHQ and 250 NSA analysts to sift through it all.

Smurfs – Many of the intelligence gathering programs the NSA infect cellphones with are given the names of Smurfs corresponding with their function. Nosey Smurf has the

ability to turn a phone's microphone on remotely. Tracker smurf is a high precision geolocation tool. Dreamy Smurf can activate a phone that is sleeping or turned off, allowing other functions to then be used. These programs hide themselves in the phone firmware architecture with capabilities codenamed Paranoid Smurf. Smurfs are known to function on both iPhone and Android devices.

Special Collection Service – A unit run by a CIA and NSA partnership which performs wiretapping operations in American embassies in over 80 foreign locations. The most notable location revealed was Berlin, but 19 other European locations were cited, including Rome, Paris, Geneva, Madrid and Prague. SCS teams work undercover as accredited diplomats within “shielded” areas of American embassies. They use listening devices to intercept almost all types of communication including cellular signals, wireless networks and satellite communication. They operate on the upper floors of the embassy, near the rooftop, where antennas and other equipment can be camouflaged by aesthetic and design features. The eavesdropping could possibly extend beyond the embassy itself, with many SCS teams operating close to government buildings and business sectors which would be operating on local cell towers or radio links. [Read more.](#)

Spinneret – Metadata processing program similar to EvilOlive and ShellTrumpet which is expected to go online sometime in September 2013.

Squeaky Dolphin – A monitoring program designed by the GCHQ and showcased to the NSA in 2012. Designed as a “broad real-time monitoring of online activity” including everything from YouTube videos to Facebook likes or links shared and blog visits. It is first major extension of surveillance into social media realms which it has classically only drawn metadata from, all of which is performed without the target corporation's consent. Squeaky Dolphin would map a network of trends such as which videos were popular for certain cities and also allow agencies to extract specific user information. The GCHQ revealed how they already exploited unencrypted Twitter data to identify users and target them for propaganda. Such kind of real-time surveillance is only possible by tapping directly into undersea internet cables and fiber-optic hubs, access the GCHQ and NSA have through their SIGAD programs worldwide.

SSO – Special Source Operations. A division within the NSA focused entirely on programs dealing with US corporate communications. Home to PRISM and other surveillance programs.

Stellar Wind – One of the first NSA programs dedicated to collecting email metadata on both foreigners and Americans, appearing soon after the 9/11 attacks. Initially not authorized by any court authority, it was discontinued in March 2004. On July 14th, 2004, the Department of Justice and NSA took the program to the FISA courts who reauthorized the program but limited the datalinks the NSA could access and who could access that data. This program continued two years into the Obama administration and it is unknown if it was discontinued or not.

TAO – AKA Tailored Access Operations. The NSA's hacking central, responsible for the many “implants” which can be installed on a target computer and used for

surveillance or data modification. The agency has rapidly grown over the past six to eight years, hiring new personal to design hundreds of new implant software for everything from network routing devices to mobile phones. TAO fills the NSA's need for a more "active" form of surveillance and the TAO's stated mission is to "aggressively scale" their hacking operations.

TAPERLAY – A search tool used with the FASCIA repository to find the registered location of a mobile device, its provider, and the country where the phone was originally located. Similar to CHALKFUN.

Trafficthief – A subset database to X-Keyscore, it holds metadata from strong selectors (email address) most likely after they have passed their time limit (for metadata, 30 days) in the main X-Keyscore database. See **X-Keyscore**.

Transient Thurable – The GCHQ's version of metadata processing program, and new arm of the X-Keyscore surveillance program. Described as having been a modified version of the NSA's own programs, with its metadata flowing into NSA repositories since 13 August 2012.

Treasure Map – A program which is said to provide the NSA with "a near real-time, interactive map of the global Internet.". Relying on a holy trinity of Internet routing data (SIGAD), commercial information (PRISM), and Signals Intelligence, it allows agents to map, analysis, and explore computer networks all over the world. It collects between 30 and 50 million unique Internet provider addresses across WiFi networks and geolocation data, with one PowerPoint slide boasting it can map any device, anywhere, all the time." Officials insist it is only targeted at foreign and Defense Department networks and is not used for surveillance but to study computer networks. The amount of data from IP addresses is actually too much at times, and thus the NSA is not able to retain all data all the time. "Packaged Goods" is a program used in conjunction with Treasure Map to track traceroutes through the internet, and with the program the NSA has gained access to "13 covered servers in unwitting data centers around the globe".

TURBINE – A newly created program used to efficiently manage the many thousands of implants the NSA has in operation. TURBINE is intended to work as a sort of brain, automating much of the setting up and installing of implants on target computers, procedures that were manual before 2009. As one secret document stated. "For example, a user should be able to ask for 'all details about application X' and not need to know how and where the application keeps files, registry entries, user application data, etc." This automation has the side effect of vastly increasing the NSA's implant attack profile from thousands to millions. Because they don't need an agent on hand for every implant, many more targets can be hit at once, the back and forth stream of information largely handled by TURBINE. The system works in conjunction with a program called TURMOIL, which scans internet data packets for communications between two targeted computers. Once it discovers that, it gives TURBINE a heads-up, allowing an automatic implant attack to occur.

UKUSA Agreement – A secret treaty between the British GCHQ and the American NSA intelligence departments first negotiated in March 1946, later expanded to include

Canada in 1948 and Australia and New Zealand in 1956 (colloquially known as the “Five Eyes”). It allows the free sharing of intelligence, particularly of signal intercepts, between the five nations, assigning each to monitor a particular section of the globe, with an emphasis on the Soviet Union and Eastern European countries during the Cold War, but which has expanded to include the People’s Republic of China, South-East Asia, and Latin America. This program later led to the creation of the ECHELON signal collection and analysis program.

X-Keyscore – Described as the “widest reaching” system for working with online intelligence, X-Keyscore is the program which allows the NSA to search various tiered databases for both metadata and actual user content. Analysts search by using either a strong selector (an email address) or soft selectors (content; phone numbers, browser history, log ins, IP address) which can then return information on a designated target with no pre-authorization or oversight (though the process is described as “auditable”). X-Keyscore can be described as a mass pool of information, collecting both unfiltered metadata and almost all other internet activity such as the From/To/CC/BCC and contents of an email, Facebook chats and private messages, browser history, contact lists, and lists of IP addresses that have visited a targeted website. Due to the massive amount of data being collected (850 billion call events and 150 billion internet records by 2007, up to 20 trillion transactions by last year, with about 1.7 billion in emails, phone calls, and other types of communications collected every day), content only remains on the main X-Keyscore server for three to five days, while metadata is stored for 30 days. Other tiered databases, internally known as Trafficthief, Pinwale, and MARINA, can save “interesting” content from the main X-Keyscore server for up to five years. X-Keyscore is also noted to work on tracking and cracking VPNs, encrypted content, and “exploitable machines”. It is a system which is distributed over 700 servers across 150 global sites, and is claimed to have captured up to 300 terrorists using information gleaned from intelligence. [Click here for the slides and more details on X-Keyscore.](#)

From the various programs listed, one can tell that there is very little the NSA will not do to collect data. Every possible method is in use. While they extract corporate user data from the front (PRISM) they are also hoarding it secretly from the backend as well (MUSCULAR). While they scoop up all cellular and internet data (FASCIA, CO-TRAVELER, MYSTIC, FORNSAT) they also target users with malware attacks to infect their computers individually, posing as a US corporation while they do it (QUANTUMHAND). The Washington Post has a run-down of how the NSA deals with its data.

Comment: The United States and other government sponsored mass surveillance programs are a trillion dollar business where citizens around the world are the product. I seek vindication for illegal termination after blowing the whistle over huge federal government cybersecurity vulnerability's.

Please pass on to White House, Senate, Congressional, State and Local Reps, Friends and Family.

The White House recently created a "Cybersecurity Panel task with securing America,

but the appointees are Corporate and IT executives guilty of breaking all our privacy laws.....President Obama awards the newly created Cybersecurity Panel 4 trillion dollars for 2017....Wow. question: For what? The government already owns the internet, service, telephone and cell phone provider around the world.

EXHIBIT 3

Electrospace.net

Signals Intelligence

Communications Security

Top Level Telecommunications

NSA Nicknames and Codewords

(Updated: January 11, 2017)

Below is a listing of nicknames and codewords related to US Signals Intelligence (SIGINT) and Communications Security (COMSEC). Most of them are from the National Security Agency (NSA), some are from other government or military agencies.

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

> There's a separate listing of NSA's TAO Division Codewords

NICKNAMES are generally unclassified. NSA uses single word nicknames, but at other agencies they usually consist of two separate words, with the first word selected from alphabetical blocks that are assigned to different agencies by the Joint Staff. Usually, nicknames are printed using all capital letters.

CODEWORDS are always classified and always consist of a single word. Active codewords, or their three-letter abbreviations, which identify a classification compartment always need to be shown in the classification or banner line. Normally, codewords are printed using all capital letters.

It's not always clear whether we see a nickname or a codeword, but terms mentioned in public sources like job descriptions can be considered unclassified nicknames.

Similar lists are available on this website for GCHQ, CSE and BND. See also the lists of abbreviations of SIGINT and COMSEC, and general telephony and internet terms.

Please keep in mind that a listing like this will always be work in progress!

(this list has been copied on some other websites and forums, but only this one is being updated frequently)


Welcome to Electrospace.net!

Here you can read about:

- Signals Intelligence (SIGINT),
 - Communications Security (COMSEC),
 - Information Classification,
- and also about the equipment, from past and present, which make that civilian and military leaders can communicate in order to fulfill their duties.

The main focus will be on the United States and its National Security Agency (NSA), but attention will also be paid to other countries and subjects.

Any comments, additions, corrections, questions or suggestions will be very appreciated! There's no login or registration required for commenting.

 twitter.com/electrospace

 [info \(at\) electrospace.net](mailto:info@electrospace.net)

As of February 3, 2017:

NEW PGP Public Key fingerprint:
ECEC FF63 D036 F415 A0BF A436
661A AC96 B451 5E04

The postings on this weblog are updated frequently as new information about the NSA is still being revealed. Therefore, revisit this weblog and check the articles for updates!

A

ABNER I - General-purpose cryptanalytic computer (delivered to the US Army's ASA in 1952) *

ACIDWASH - Covert access point for a mobile phone network in Afghanistan, part of the MYSTIC program * *

ACORN - Compartment for Top Secret COMINT information (1950-1951) *

ACCORDIAN - Type 1 Cryptographic algorithm used in a number of crypto products

AETHER - ONI tool "to correlate seemingly disparate entities and relationships, to identify networks of interest, and to detect patterns" *

AGILITY - NSA internet information tool or database

AGILEVIEW - NSA internet information tool or database

AIRGAP - Database which deals with priority DoD missions, and/or for access to the public internet *

AIRHANDLER (AH) - Processing system for wireless (geolocation) data collected by a Predator drone platform, like AST-221A *

AIRSTEED - Cell phone tracking program of the Global Access Operations (GAO) *

AIRWOLF - ?

ALAMITO - The mission of Mexico at the United Nations in New York *

ALBATROSS - Soviet cipher system of the 1940s and maybe 1950s

ALPHA - Retired SIGINT Exchange Designator for Great Britain

ALTEREGO - A type of Question-Focused Dataset based on E.164

AMBERJACK - SIGINT/EW collection and exploitation system

AMBLE - Retired SIGINT product codeword

AMBULANT (AMB) - SI-ECI compartment related to the BULLRUN program

ANARCHIST - Joint NSA-GCHQ program to intercept video from Israeli drones from an RAF facility on Cyprus *

ANCHORY - NSA software system which provides web access to textual intelligence documents

APALATCHEE - The EU mission in New York

APERIODIC - SI-ECI compartment related to the BULLRUN program

APEX - See Abbreviations listing

APPLE1 - Upstream collection site

APPLESAUCE - Civilian(CIA)-run station on Cyprus (1950s)

APRIL FLOWERS - SSO access capability supporting the Athens Olympics in 2004 *

APRIL STRAWBERRY - Small-scale program that researched vulnerabilities in computer networks running critical infrastructure *

APSTARS - NSA tool that provides "semantic integration of data from multiple sources in support of intelligence processing" *

AQUADOR - Merchant ship tracking tool

ARCA - SIGINT Exchange Designator for ?

ARGON - Satellite mapping program

ARGYLEALIEN - Method to cause a loss of data by exploiting zeroization of hard-drives *

ARKSTREAM - Implant used to reflash BIOS, installed by remote access or intercepted shipping

ARMADA SWEEP - Ship-based collection system for electronic communications data *

ARMOR - System related to the Predator drone *

ARTEMIS - SIGINT and Direction Finding system, probably for cell phones

ARTIFICE - Corporate partner for domestic long-distance cable access (presumably Verizon/MCI) *

ASPHALT - Software modem, increasing the volume of satellite signals *

ASPHALT-PLUS (A-PLUS) - See above

ASSOCIATION - NSA database for cell phone metadata, derived from FASCIA *

ATALANTA - EU anti-piracy operation

ATLAS - Cryptanalytic computer using magnetic drum storage technology, built by Engineering Research Associated (ERA, delivered to the US Navy for 1 million US dollar in 1950) *

AUNTIE - SI-ECI compartment related to the BULLRUN program

AURORAGOLD (AG) - Repository of data about international GSM/UMTS networks *

AUTO ASSOCIATION - Second party database

AUTOSOURCE - NSA tool or database

AQUACADE - A class of SIGINT spy satellites (formerly RHYOLITE)

AZUREPHOENIX - Cable tapping facility operated in cooperation with a trusted 3rd

Index of all postings

Recent Posts

Trump's "beautiful" Oval Office phones and what was changed on them

The 5-year anniversary of this weblog

The presidential communications equipment under Barack Obama

Obama used a cybersecurity link for the first time to warn Russia

A perspective on the new Dutch intelligence law

Wikileaks publishes classified documents from inside German NSA inquiry commission

Data sharing systems used within the Five Eyes partnership

With NSA contractor Martin arrested, other leakers may still be at large

Secret report reveals: German BND also uses XKEYSCORE for data collection

"It's actually straight up interesting but also weird how weirdly, wonderfully detailed this blog about hyper secure communications is."

— Gizmodo.com

Pages

Home

INDEX

Links

Abbreviations and Acronyms

NSA Nicknames and Codewords

NSA's TAO Division Codewords

NSA's organizational designations

NSA's Legal Authorities

NSA Glossary

The US classification system

SIGINT Activity Designators (SIGADs)

GCHQ Codewords and Abbreviations

Party agency, part of the RAMPART-A program *

[back to top](#)

B

BACCHUS - ASA-provided electromechanical cipher equipment for South Korean forces (1953)

BALLOONKNOT - TAO computer hacking project *

BAMBOOSPRING - ?

BANCROFT - KY-67 voice encryption system

BANISTER - The Columbian trade bureau in New York *

BANYAN - NSA tactical geospatial correlation database?

BANYAN - Database for (landline) telephone metadata, derived from FASCIA *

BASECOAT - Program targeting the mobile phone network on the Bahamas (sigad: US-3310A) *

BASILHAYDEN - Joint GCSB-NSA operation (proposed) to tap communications between the Chinese consulate and its passport office in Auckland, New Zealand (GCSB codename: FROSTBITE) *

BASTE - Retired SIGINT product codeword

BATON - Type 1 Block cipher algorithm, used with many crypto products

BAYBRIDGE - Codeword related to data exchange at NSA's European Cryptologic Center (ECC) *

BEAMER - ?

BEGGAR SHADOW - Navy airborne SIGINT missions

BELLTOPPER - NSA database *

BELLVIEW - SIGINT reporting tool

BIGDIPPER - Billing records data flow within BR FISA collection under FAIRVIEW *

BIG LOOK - ELINT systems on Navy EC-121s to detect SAM radars (Vietnam War)

BIGOT - List of personnel cleared for access to highly sensitive information or operations

BIG RIB - airborne telemetry collection program using RB-57 aircraft based in Adana, Turkey (1965-?)

BINOCULAR - Former NSA intelligence dissemination tool

BIRCHWOOD - Upstream collection site

BITTERSWEET - first "advisory warning" (COMINT-provided alert) plan for airborne SIGINT missions (1952)

BLACKBOOK - ODNI tool for large-scale semantic data analysis *

BIRDWATCHER - Automated survey system *

BLACKFOOT - The French mission at the United Nations in New York *

BLACKHAWK - Program for surveillance of the Turkish mission at the UN in New York

BLACKHEART - Collection through FBI implants *

BLACKMAGIC - NSA database or tool

BLACKNIGHT - Filtering or selection tool *

BLACKPEARL - NSA database with SIGINT 5-tuple (TCP/IP), identified routers, routing protocols, and SIGINT access points, maybe also case notations * * *

BLACKWATCH - NSA reporting tool

BLARNEY - Program for intercepting foreign phone and internet communications within the US under FISA authority (since 1978)*

BLAZING SADDLES - CSE tool? *

BLEAKINQUIRY - Metadata database of potentially exploitable VPNs *

BLUEANCHOR - Partner providing a network access point for the YACHTSHOP program

BLUEFISH (BLFH) - Compartment of the KLONDIKE control system

BLUESASH - Network used by NTOC operational analysts *

BLUE SKY - Airborne COMINT program in Far East (1952-?)

BLUESNORT - TURMOIL type or site? *

BLUESTREAM - Cryptologic collection system aboard US Navy ships

BLUEZEPHYR - Sub-program of OAKSTAR

BOGART - General-purpose cryptanalytic computer from the early 1950s using transistors *

BOOKISHMUTE - NSA hacking tool or code included in the Shadow Brokers leak *

BOOTY - Retired SIGINT product codeword

BORGERKING - Something related to Linux exploits *

BOUNDLESSINFORMANT - DNI and DNR metadata visualization tool

BOURBON - Joint NSA and GCHQ program for breaking Soviet encryption codes (1946-?)*

CSE Codewords and Abbreviations


BND Codewords and Abbreviations

Telephony Abbreviations

Internet abbreviations

About

Total Pageviews

 **2,534,498**

Popular Posts

How Obama's BlackBerry got secured

New phones aboard Air Force One

INCENSER, or how NSA and GCHQ are tapping internet cables

The US Classification System

DRTBOX and the DRT surveillance systems

Unnoticed leak answers and raises questions about operation Eikonal

Leaked documents that were not attributed to Snowden

Labels

Air Force One (1) Apple (1) BlackBerry (1) BND-Selectors (1) Boeing (1) BoundlessInformant (8) Brazil (1) Britain (1) Canada (1) Classification (9) CSEC (2) Cyber (1) Eikonal (4) FBI (1) France (2) GCHQ (6) General Dynamics (1) Germany (17) Gold Phone (1) GSM (2) Hotline (5) ISAF (1) Israel (2) IST (4) Kremlin (1) Metadata (5) Netherlands (7) New Zealand (1) Non-Snowden-leaks (2) North Korea (1) **NSA (43)** NSA Partnerships (20) Obama (4) POTUS (10) PRISM (8) Red Phone (5) Russia (1) SatCom (2) Section 215 (2) Sectra (1) Secure voice (5) Situation Room (1) Snowden (4) STE (4) STU-II (1) STU-III (1) Trump (1) UMTS (2) US (1) USA (4) USSR (2) Vatican (1) VoIP (1) White House (7) Wireless (7) XKeyscore (1)

Search This Blog

BOXINGRUMBLE - Network attack that was countered by QUANTUMDNS *

BRAZEN - NSA access to the public internet, in 2004 replaced by OUTPARKS *

BRICKTOP - Project to learn about new malware by intercepting e-mail from several security companies (2009) *

BRIDE - Second codename for what eventually became VENONA *

BROKENRECORD - NSA tool

BROADSIDE - Covert listening post in the US embassy in Moscow

BROOMSTICK - ?

BRUNEAU - The Italian embassy in Washington DC *

BRUTUS - Tool or program related to MARINA *

BUCKSHOT YANKEE - Operation to remove the computer worm Agent.btz from infected classified and unclassified DoD networks (2008-2009) *

BUFFALOGREEN - The name ORANGECRUSH was known to Polish partners *

BUGCATCHER - Internet (DNI) transit cable access under the FAIRVIEW program *

BULLDOZER - PCI bus hardware implant on intercepted shipping

BULLRUN - An NSA COI for decryption of network communications

BULLSEYE - NSG High-Frequency Direction-Finding (HF-DF) network (now called CROSSHAIR)

BYEMAN (BYE) - Retired SCI control system for overhead collection systems (1961-2005)

Blog Archive

- ▼ 2017 (3)
 - ▼ February (1)
 - Trump's "beautiful" Oval Office phones and what wa...
 - January (2)
- 2016 (14)
- 2015 (20)
- 2014 (30)
- 2013 (33)
- 2012 (10)

US Red Phones



Sequence of the real Red Phones, not for the Washington-Moscow Hotline, but for the US Defense Red Switch Network (DRSN). The phones shown here were in use from the early eighties up to the present day and most of them were made by ElectroSpace Systems Inc. They will be discussed on this weblog later.

For the record, you see:

- ElectroSpace MLP-1
- ElectroSpace MLP-1A (since 1983)
- ElectroSpace MLP-2
- Raytheon IST (since 1992)
- Telecore IST-2 (since 2003)

US Classification Levels

Color codes for the classification levels used by the government and the armed forces of the United States:

C

CADENCE - NSA tasking tool and database, probably for internet communications

CAJABLOSSOM - Automated system for analysing and profiling internet browsing histories

CAKEBREAD - Codename for Osama bin Laden

CALIX - System used at the Waihopai satellite intercept station *

CALYPSO - Remote SATCOM collection facility

CAMBERDADA - Project using SIGINT collection to learn about new malware *

CANDYGRAM - Laptop mimicking GSM cell tower, sends out SMS whenever registered target enters its area, for tracking and ID of targets

CANYON - Class of COMINT spy satellites (1968-1977)

CANOE - Compartment for Top Secret COMINT information (1952-1953) *

CANNON LIGHT - Counterintelligence database of the US Army

CANYONDUST - Ground-based 24/7 INMARSAT geolocation capability *

CAPRICORN - (former?) database for voice data *

CARBOY - Second Party satellite intercept station at Bude, England

CARBOY II - Units of ECHELON which break down satellite links into telephone and telegraph channels

CARILLON - Complex of five IBM-370 (or 360, later four IBM 3033s) high performance computers strapped together at Fort Meade, for a mostly traffic analytic process (1973)

CARPAT - NSA contact chaining algorithm *

CASport - NSA user authorization service

CATALYST - Computer system capable of automatically analyzing the massive quantities of data gathered across the entire intelligence community *

CENTER ICE - Data center for the exchange of intelligence regarding Afghanistan among the members of the 14-Eyes/SSEUR *

CENTERMASS - NSA tool or database

CENTRICDUD - Tool that can read and write bytes in the CMOS of a targeted Windows computer *

CERF CALL MOSES1 - Contact Event Record Format - for certain telephony metadata *

CERNET - Open Source information used for the TREASUREMAP tool *

CHALET - First codename for CHALET/VORTEX class SIGINT satellites (the codename was changed after 1979 leak)

CHALKFUN - Analytic tool, used to search the FASCIA database *

CHAOS - CIA domestic spying operation (1967-1973)

CHARGER HORSE - Communication net for afloat direct SIGINT support detachments (Vietnam War, 1969-?)

CHASEFALCON - Major program of the Global Access Operations (GAO) *

CHATTERII - Communications tool (connecting to 3rd Party agencies?)

CHEER - Retired SIGINT product codeword

CHENEY - Soviet cipher system, probably of the 1950s

[back to top](#)

Top Secret/SCI

Top Secret

Secret

Confidential

Unclassified

CHEROKEE - (former) handling instruction: limited to senior officials
 CHESS - Compartment of TALENT KEYHOLE for the U-2 spy plane
 CHEWSTICK - NSA tool or database
 CHIMNEYPOOL - Framework or specification of GENIE-compliance for hardware/software implants
 CHIPPEWA - Some communications network, involving Israel *
 CHUTE - Retired SIGINT product codeword
 CIMBRI - Probably a metadata database *
 CINEPLEX - Analytical tool *
 CIRCUIT RAPTOR - System for processing data from circuit switched telephone networks *
 CLARIFYMIND - Pilot program for secure wireless communications *
 CLASSIC - ?
 CLASSIC BULLSEYE - Worldwide ocean SIGINT surveillance or direction finding system (1960's-?)
 CLASSIC TROLL - System that increases the probability of SIGINT intercept by 500%, supporting tactical and national requirements
 CLASSIC WIZARD - Satellite ocean surveillance system for ELINT
 CLEARSIGHT - Processing system related to COURIERSKILL *
 CLEVERDEVICE - Upstream collection site
 CLIFFSIDE - Trans-Pacific cable access site under the FAIRVIEW program *
 CLOISTER - NSA language center in College Park staffed with contractor native speakers of Russian and Eastern European languages (1960s and 70s) *
 CLOUD - NSA database
 CLOUD - DSP program implementing graph algorithms in a cloud computing environment *
 CLOUDSHIELD - System that terminates a client-side connection to a malicious server and blocks the server's response *
 COASTLINE - NSA tool or database
 COBALTFALCON - Sub-program of OAKSTAR
 COBRA FOCUS - Counter-terrorism SIGINT fusion center at NSA-G, first for operations in Iraq, later expanded to other regions * *
 COGNOS - NSA tool or database
 COLERIDGE - Soviet cipher system of the 1940s
 COMFY LEVI - C-130s with roll-on SIGINT suites (1968-?)
 CORDOBA - Type 2 Cryptographic algorithm used in a number of crypto chips
 COMBAT SENT - Reconnaissance operation
 COMMONGROUND - System used at the Waihopai satellite intercept station *
 COMMONVIEW - Internal NSA monitoring tool *
 CONCERTO - NSA's internal personnel system, with most personnel information in HR
 CONCERTO and name, SSN and clearances in SECURITY CONCERTO *
 CONFIRM - NSA database for personnel access
 CONTRAOCTAVE - NSA telephony tasking database * Used to determine 'foreignness' *
 CONVERSION QUEST - Part of SHAREDQUEST relating to antenna command and control *
 CONVEYANCE - Voice content ingest processor *
 COPILOT - System that automatically scans digital data for things like language, phone and creditcard numbers and attachments *
 COPPER DUNE - Operation against Al Qaida on the Arabian Peninsula (AQAP) in Yemen
 COPSE - Compartment for Top Secret COMINT information (1949-1950) *
 CORALINE - NSA satellite intercept station at Sabana Seca at Puerto Rico (closed)
 CORALREEF - Database for VPN crypto attack data *
 CORONA - A series of photographic surveillance satellites (1959-1972)
 CO-TRAVELER - Set of tools for finding unknown associates of intelligence targets by tracking movements based upon cell phone locations *
 COURIERSKILL - Filtering or selection tool *

These color codes are used to mark the classification level of (digital) documents and files and also of the communication devices used for their transmission.

Subscribe to this weblog!

Hotlinks

- The Dutch virtual Crypto Museum
- Website about Crypto Machines
- Steven Aftergood's Secrecy News
- Intelligence expert Matthew Aid
- Bruce Schneier on Security
- The weblog Empty Wheel
- Weblog of Matthijs R. Koot
- Leaked documents: IC Off the record
- Der Spiegel's 53 & 36 documents
- Netzpolitik live blogs: NSA Inquiry
- The Snowden Surveillance Archive
- NSA Observer - FVEY Docs
- Spy back: ICWATCH
- The Cryptome
- > Many more links

Contact

For questions, suggestions and other remarks about this weblog in general or any related issues, please use the

COWBOY - The DICTIONARY computer used at the Yakima station of ECHELON *

COWBOY - FISA authorized collection under the FAIRVIEW program (sigad: US-984T)

*

CRAFTY SHACK - Analytics documentation *

CRANKSHAFT - Codename for Osama bin Laden

CREAM - Compartment for Top Secret COMINT information (1946-1947) *

CREDIBLE - Transport of intelligence materials to partner agencies

CREST - Database that automatically translates foreign language intercepts in English

*

CRISSCROSS - Database of telecommunications selectors, operated by the CIA and also used by DOJ, DOD and NSA

CROSSBEAM - GSM module mating commercial Motorola cell with WagonBed controller board for collecting voice data content via GPRS (web), circuit-switched data, data over voice, and DTMF to secure facility, implanted cell tower switch

CROSSHAIR - NSG High-Frequency Direction-Finding (HF-DF) network (formerly BULLSEYE)

CRUMPET - Covert network with printer, server and desktop nodes

CULTWEAVE - Smaller size SIGINT database *

CULTWEAVE II - Database for VOICESAIL metadata *

CYBERCOP - Cyber attack visualisation tool

CYBERQUEST (CQ) - Cyber threat discovery mission? (since 2008)*

CYBERTRANS - A common interface to a number of underlying machine translation systems *

CYCLONE Hx9 - Base station router, network in a box using Typhon interface

CYR - Intelligence exchange agreement between DIA and the Israeli military intelligence directorate (1968) *

following e-mail address: info (at) electrospace.net

For sending an encrypted e-mail message, you can use the PGP Public Key under this ID: B4515E04

You can also communicate through Twitter: @electrospace or XMPP/Jabber chat by using the address electrospace (at) jabber.de

The title picture of this weblog shows the watch floor of the NSA's National Security Operations Center (NSOC) in 2006. The URL of this weblog recalls Electrospace Systems Inc. the company which made most of the top level communications equipment for the US Government. All information on this weblog is obtained from unclassified or publicly available sources.

[back to top](#)

D

DAFF - Codeword for products of satellite imagery

DAMEON - Remote SATCOM collection facility

DANCER - Project initiated in 1965 to employ South Vietnamese as linguists in US SIGINT operations

DANCINGOASIS (DGO) - SSO program collecting data from fiber optic cables between Europe and the Far East (since 2011) *

DANDERSPRITZ - Software tool that spoofs IP and MAC addresses, intermediate redirector node

DANGERMUSE - Tactical SIGINT collecting system for like cell phone calls

DARDANUS - Remote SATCOM collection facility

DARKQUEST (DQ) - Automated FORNSAT survey system * that can for example identify the presence of a VPN *; part of SHAREDQUEST *

DAUNT - Compartment for Top Secret COMINT information (1959-1960) *

DAYSEND - Program at NSA's communications complex receiving intercepts files (1973)

DECKPIN - NSA crisis cell activated during emergencies

DEEPDIVE - XKEYSCORE version that can process internet traffic at data rates of 10 gigabit per second *

DELLA - Special-purpose cryptanalytic computer machine from the early 1950s *

DELTA - Former SCI control system for intercepts from Soviet military operations

DEMONSPIT - Dataflow for bulk telephony metadata acquired from major Pakistani telecom providers *

DENIM - Retired SIGINT product codeword

DESOTO - Processing system related to FAIRVIEW Transit collection under FAA 704 & 705b *

DESPERADO - NSA software tool to prepare reports

DEWSWEEPER - Technique to tap USB hardware hosts *

DIANA - ASA-provided one-time-pad system for South Korean forces (1953)

DIKTER - SIGINT Exchange Designator for Norway

DINAR - Compartment for Top Secret COMINT information (1961-1965) *

DIONYSUS - Remote SATCOM collection facility

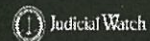
DIRESCALLOP - Method to circumvent commercial products that prevent malicious software from making changes to a computer system

DISCOROUTE - NAC/GCHQ repository for router configuration files from CNE and passive SIGINT, like for example telnet sessions * *

**END ILLEGAL
IMMIGRATION
NOW!**

SIGN THE PETITION

to tell your governor
to enforce our nation's
immigration law



DISHFIRE - NSA database for text messages (SMS)
 DISTANTFOCUS - A pod for tactical SIGINT and precision geolocation (since 2005) *
 DISTILLERY - Tactical collection system(?) *
 DISTILLERY - Stream-based platform for executing hacking identification applications *
 DIVERSITY - SIGINT Exchange Designator for ?
 DOBIE - The South African consulate and mission at the UN in New York *
 DOGCOLLAR - A type of Question-Focussed Dataset based on the Facebook display name cookie
 DOGHUT - Upstream collection site
 DOUBLEARROW - One of NSA's voice processing databases? *
 DRAGGABLEKITTEN - An XKEYSCORE Map/Reduce analytic *
 DRAWSTRING - Project to "remote" more intercept facilities because of budget cuts (1973-?)
 DREADNOUGHT - NSA operation focused on Ayatollah Khamenei *
 DRTBOX - System for processing data from mobile communication networks
 DRUG - Third codename for what eventually became VENONA *
 DRUID - SIGINT Exchange Designator for third party countries
 DRYAD - A US military numeral cipher/authentication system
 DRYTORTUGAS - Analytic tool
 DUALTIRE - System used at the Waihopai satellite intercept station *
 DUSKPALLET - SSO interception program for GSM networks in Kenya (US-3270), part of the MYSTIC program *
 DYNAMO - SIGINT Exchange Designator for Denmark
 DYNO - Classified codename for the Galactic Radiation And Background (GRAB) Low-Earth Orbit ELINT satellite (1960-1962 launches)

[back to top](#)

E

EAGLE - Upstream collection site under the FAIRVIEW program *
 EASYCHAIR (EC) - CIA research project for developing resonant cavity covert listening devices (bugs)
 ECHELON - Sub-program of FROSTING directed against INTELSAT satellites *
 ECHO - SIGINT Exchange Designator for Australia
 ECRU (EU) - Compartment of the ENDSEAL control system
 EDEN - Upstream collection site under the FAIRVIEW program, maybe in New York City *
 EIDER - Compartment for Top Secret COMINT information (1955-1959) *
 EIKANOL (or: EIKONAL) - Joint NSA-BND operation to tap a fiber-optic cable of Deutsche Telekom in Frankfurt, part of the RAMPART-A program
 EINSTEIN - Cell phone network intercepting equipment used by SCS units
 EINSTEIN - Intrusion detection system for US government network gateways (deployed in 2004)
 EINSTEIN 2 - Second version of the EINSTEIN program for detecting malicious network activity
 EINSTEIN 3 - Third version of the EINSTEIN program that will monitor government computer traffic on private sector sites too *
 ELEGANTCHAOS - Large scale FORNSAT data analysis system *
 EMERALD - Alternate codename for operation WHARPDRIVE(?) *
 ENDSEAL (EL) - SCI control system
 ENDUE - A COI for sensitive decrypts of the BULLRUN program
 ENTOURAGE - Directional finder for line of bearing for GSM, UMTS, CDMA, FRS signals, works with NEBULA active interrogator within GALAXY program
 EPICSHALTER - Data backup system to recover information from particular NSA sites, designed by Edward Snowden *
 EQUATION (Group) - Nickname given by Kaspersky to a highly advanced computer hacking group, suspected of being tied to NSA *
 ETCHINGSPIN - SSO mobile telephone interception program, part of the MYSTIC program *
 EVENINGEASEL - Program for surveillance of phone and text communications from Mexico's cell phone network (sigad: US-3411), part of the MYSTIC program *
 EVILOLIVE - Internet geolocation tool
 EVOLVED MUTANT BROTH - Second party database
 EXPLORER I/II/III - Intercept operations using unmanned equipment on hilltops during the Vietnam War (1970-1972)

EYESPY - System that scans data for logos of companies, political parties and other organizations, as well for pictures with faces for facial recognition *

[back to top](#)

F

FACELIFT - Codeword related to NSA's Special Source Operations division *

FACTOR - NSA program targeting North Vietnamese maritime infiltration (1970-?)

FAIRVIEW - Domestic cable tapping program in cooperation with AT&T (since 1985)*

FAIRVIEWCOTS - System for processing telephony metadata collected under the FAIRVIEW program *

FALLENORACLE - NSA tool or database

FALLOUT - DNI metadata ingest processor/database

FALLOWHAUNT (FH) - System used at the Waihopai satellite station, New Zealand, part of SHAREDQUEST *

FARLEY - (SIGINT exchange designator?)

FARMER - Projected general-purpose computer for both cryptanalysis and traffic analysis (1950s)

FARNDAL - ? *

FASCIA - DNR metadata ingest processor/database *

FASCIA II - Ibidem with a dedicated HCS partition *

FASCINATOR - Series of Type 1 encryption modules for Motorola digital-capable voice radios

FASTBAT - Telephony related database?

FASTFOLLOWER - Tool to identify foreign agents who might tail American case officers overseas by correlating cellphone signals

FASTSCOPE (FS) - NSA database for flight lists and manifests, including passenger names *

FIFTYEXCLAIM - Cover term representing NSA's contract with Computer Sciences Corporation (CSC) for mission support in Bad Aibling, Germany *

FIRE ANT - Open Source visualisation tool

FIREBIRD - Cable tapping facility operated in cooperation with a trusted 3rd Party agency, part of the RAMPART-A program *

FIREFLY - NSA key generation scheme, used for exchanging EKMS public keys

FIRETRUCK - SIGINT tool or database

FISHBOWL - NSA program for securing commercial smartphones

FISHWAY - Data batching & distribution system used for FAIRVIEW and BLARNEY collection * *

FLARE - Retired SIGINT product codeword

FLATLIQUID - TAO operation against the office of the Mexican president *

FLEMING - The embassy of Slovakia in Washington DC *

FLINTLOCK - The DICTIONARY computer used at the Waihopai station of ECHELON *

FLOWBEE - Project of NSA's Research Directorate for reducing the volumes of metadata collected from high-speed links (2008) *

FLUTE - System used at the Waihopai satellite intercept station *

FOREMAN - Tactical SIGINT database? Used to determine 'foreignness' *

FOURSCORE - (former?) database for fax and internet data *

FOXAMI - (SIGINT exchange designator?)

FOXTRAIL - NSA tool or database *

FRIAR - Cable station of AT&T at the East coast under the FAIRVIEW program *

FRIARTUCK - VPN Events tool or database (CSEC?)

FREEFLOW-compliant - Supported by TURBULENCE architecture

FRESNELEFFECT - System used at the Waihopai satellite intercept station *

FRETING YETI - Mobile gateway identification analytic *

FRONTO - Retired SIGINT Exchange Designator for ?

FROSTBITE - GCSB codename for operation BASILHAYDEN

FROSTBURG - Connection Machine 5 (CM-5) supercomputer, used by NSA from 1991-1997

FROSTING - Umbrella program for collecting and processing emanations from communication satellites (est. 1966)*

FROTH - Compartment for Top Secret COMINT information (1953-1954) *

[back to top](#)

G

GALACTICHALO - Remote SATCOM collection facility
 GALAXY - Find/fix/finish program of locating signal-emitting devices of targets
 GALLOWAY - System related to the Predator drone *
 GAMBIT - Prototype web portal for the AMOD (Analytical Modernization) QFD (Question Focused Dataset) strategy (2011)
 GAMMA (G) - Compartment for highly sensitive communication intercepts
 GAMUT - NSA collection tasking tool or database
 GARLICK - The NSA satellite intercept station at Bad Aibling (Germany)
 GATEKEEP - Processing system for internet cable tapping *
 GATEKEEPER - User account management system to apply for and maintain access to many NSA Databases *
 GAVEL - Retired SIGINT product codeword
 GEMINI - Remote SATCOM collection facility
 GEMINI - DIA intelligence portal for access to GEOINT database(s)
 GENESIS - Filtering tool for internet communications, related to XKEYSCORE
 GENESIS - Modified GSM handset for covert network surveys, recording of RF spectrum use, and handset geolocation based on software defined radio
 GENIE - Overall close-access program, collection by Sigads US-3136 and US-3137 * *
 GHOSTHUNTER (GH) - System to geolocate targets when they log onto the internet, for example through VSAT or internet cafes (since 2006) *
 GHOSTMACHINE (GM) - NSA's Special Source Operations cloud analytics platform
 GHOSTWOLF - Project to capture or eliminate key nodes in terrorist networks through actionable geolocation intelligence * also related to CT10 *
 GINPENNANT - SSG cloud framework *
 GILGAMESH (GMESH) - Predator-based NSA geolocation system used by JSOC *
 GISTQUEUE (GQ) - NSA tipping and reporting database
 GJALLER - NSA tool or database
 GLAIVE - (Satellite) interception common architecture *
 GLINT - Compartment for Top Secret COMINT information (1947-1949) *
 GLOBALBROKER - NSA tool or database
 GLOBALREACH - Tool for federated querying metadata records shared by NSA and its Five Eyes partners *
 GLOBALTIPPER (GT) - System for internal requests of information *
 GLOBALWATCH - Software suite within the Real Time Regional Gateway (RT-RG)
 GLOMAR - "neither confirm nor deny" a response to a FOIA request
 GM-Halo/DPS - Data cloud *
 GM-PLACE - Database for the BOUNDLESSINFORMANT tool *
 GODLIKELESION - Modernization program for NSA's European Technical Center (ETC) in Wiesbaden in 2011 *
 GODSURGE - Runs on FLUXBABBITT circuit board to provide software persistence by exploiting JTAG debugging interface of server processors, requires interdiction and removal of motherboard of JTAG scan chain reconnection
 GOLD - Joint SIS-CIA operation to wiretap Soviet army landlines through a tunnel under Berlin (1953-1956; British codename: STOPWATCH)
 GOLDBERG - First magnetic drum storage technology (1947)
 GOLDENCARRIAGE - NSA corporate servers, used by the AURORAGOLD application *
 GOLDENRETRIEVER - Storage and/or distribution system *
 GOLLUM - Computer implant created by a partner agency *
 GOPHERRAGE - Pilot project that seeks to develop a hypervisor implant to provide implant capabilities and a back door *
 GOSSAMER - SIGINT/EW collection and exploitation system
 GOTHAM - Processor for external monitor recreating target monitor from red video
 GOURMETTROUGH - Configurable implant for Juniper NetScreen firewalls including SSG type, minimal beaconing
 GOUT - Subcompartment of GAMMA for intercepts of South Vietnamese government communications
 GOVPORT - US government user authentication service
 GRAB - SIGINT satellite program
 GRANDMASTER - Processing system for internet traffic, has been replaced by WEALTHYCLUSTER and TURMOIL *
 GREY FOX - The 2003 covername of the Mission Support Activity (MSA) of JSOC
 GREYSTONE (GST) - CIA's highly secret rendition and interrogation programs *
 GRIZZLY STEPPE - Russian malicious cyber activities related to the 2016 US presidential elections
 GROUPDIVE - Network used by NTOC operational analysts *

GUARDRAIL I / II / IV / V - Series of Army airborne SIGINT collection systems on RC-12 aircraft

GUNMAN - NSA 1984 OPSEC project to remove 11 tons of electronic devices from the US Embassy of Moscow for thorough inspection in the US. GUNMAN eventually found KGB bugs planted into electric typewriters.

GUPY - Subcompartment of GAMMA for intercepts from Soviet leadership car phones (1960's-70's)

[back to top](#)

H

HAIRBALL - Project of NSA's Research Directorate (2008) *

HAMMOCK - Direct SIGINT support process for US Air Force missions over North Vietnam (1965-?)

HAPPYFOOT - Program that intercepts traffic generated by mobile apps that send a smartphone's location to advertising networks

HARD ASSOCIATION - Second party database

HARMONY - DoD national database for DOCEX information, run by the NGIC

HARVEST - A supercomputer, built by IBM for nearly 10 million US dollar and used by NSA from 1962-1976 *

HAVASU - International call detail records collection under FAIRVIEW *

HAVE BLUE - Development program of the F-117A Stealth fighter-bomber

HAVE QUICK (HQ) - Frequency-hopping system protecting military UHF radio traffic

HAWKEYE - AFSS project for an airborne direction-finding system; never operational (1963)

HAYMAKER - Operation against Al Qaida in Afghanistan *

HEADRESS NU - Very high priority project targeting a Pakistan government/military secure network *

HEARTBEAT - Apparently a data handler system, built by Edward Snowden* and/or successor of EPICSHELTER, or an index of surveillance systems *

HEMISPHERE - Program under which AT&T provides telephone records to the DEA

HEMLOCK - The Italian embassy in Washington DC *

HERCULES - CIA terrorism database

HERETIC - NSA tool or database

HERESYITCH - UC collateral tool, collaborative program between NSA units T1222 and SSG *

HERMOS - Joint venture between the German BND and another country with access for NSA (2012)*

HERON - Retired SIGINT product codeword

HIGHCASTLE - Tactical database?

HIGHDECIBEL - Local Area Network (LAN) for the FAIRVIEW and BLARNEY programs *

HIGHLANDS - Technique for close access collection from computer implants *

HIGH PRIDE - ? *

HIGHTIDE - NSA tool or database

HOBGOBLIN - NSA tool or database

HOLLOWPOINT - Software defined radio platform

HOMEbase - Database which allows analysts to coordinate tasking with DNI mission priorities, and/or reporting on targets

HOMEMAKER - Upstream collection site

HOMING PIGEON - Tool for correlating GSM handsets from airplane passengers to subscribers * *

HOTZONE - ?

HYDRA - CIA program to secretly access databases maintained by foreign countries and extract data to add to US watchlists *

HYSON - Retired SIGINT product codeword

[back to top](#)

I

ICEBERG - Major NSA backbone project *

ICE CASTLE - Intelligence exchange agreement between DIA and the Israeli military intelligence directorate (1988) *

ICREACH - Tool for sharing communications metadata among the US Intelligence Community (since 2007)*

IDITAROD (IDIT) - Compartment of the KLONDIKE control system

IGLOO WHITE - Program for detecting movement of vehicles through unattended ground sensors, tested in Laos from 1968-1973

INCENSER - Joint NSA-GCHQ program for tapping an internet cable between Europe and Asia with the help of Cable & Wireless; part of the WINDSTOP program

INDEX - Team at Menwith Hill Station (MHS) *

INDIA - SIGINT Exchange Designator for New Zealand (retired)

INDRA - Satellite intercept station near Khon Khaen, Thailand (1979-ca. 2000)

INTERQUAKE (IQ) - A terrestrial signals knowledge base and interface *

INTOLERANT - Data set stolen by hackers, discovered and exploited by CSEC and Menwith Hill Station since 2010 *

INTREPID SPEAR - The 2009 covername of the Mission Support Activity (MSA) of JSOC

INTRUDER - Series of ELINT and COMINT spy satellites (since 2009)

IRON HORSE - NSA equipment to display intercepted morse grid-positions on a radar scope (1967-?)

IRONSAND (IS) - Second Party satellite intercept station at Waihopai, New Zealand

IRRITANT HORN - Five Eyes pilot project for hacking target's phone connections to app stores in order to implant spyware *

ISHTAR - SIGINT Exchange Designator for Japan (retired)

ISLANDTRANSPORT (IT) - Internal data distribution system, also used for QUANTUM *

IVORY - Retired SIGINT product codeword

IVY BELLS - NSA, CIA and Navy operation to place wire taps on Soviet underwater communication cables

[back to top](#)

J

JACKHAMMER - System used at the Waihopai satellite intercept station *

JACKKNIFE - The NSA satellite intercept station at Yakima (US)

JACKPOT - Internal NSA process improvement program (early 1990s - early 2000s) *

JADE - First codename for what eventually became VENONA *

JAEGER - Former SIGINT Exchange Designator for Austria

JEMA - (see Abbreviations listing)

JOSEKI-1 - Classified Suite A algorithm

JOURNEYMAN - Umbrella program for transforming the way SIGINT analysts can write and disseminate their reports *

JUBILEECORONA - NSA unit *

JUGGERNAUT (JUG) - Ingest system that processes intercepted calls from mobile phone networks * *

JUMPDOLLAR - Tool to support various file systems *

JUMPSEAT - Class of SIGINT reconnaissance satellites (1971-1983)

JUNE - FBI classification marking for information related to unwarranted electronic surveillance and surreptitious entries *

JUNIORMINT - Implant digital core, either mini printed circuit board or ultra-mini Flip Chip Module, contains ARM9 micro-controller, FPGA Flash SDRAM and DDR2 memories

JUPITER GARRET - Operation against Al Qaida in East Africa (EA) in Somalia

contacting whom and when *

LEMONWOOD - NSA satellite intercept station in Thailand

LEXHOUND - CCE Extraction Architecture * and/or Front-end tool that performs Google-like searching across repositories *

LIBERTY - First word of nicknames for collection and analysis programs used by JSOC and other sensitive DOD activities *

LIBERTY BLUE - Modified RC-12 Guardrail surveillance airplane used by JSOC's Mission Support Activity (MSA)

LIGHTNING - Research project into a "1,000 megahertz" computer. Didn't produce a functional computer but pioneered many technology "bricks" (1950s)

LILDIPPER - Billing records data flow within BR FISA collection under FAIRVIEW *

LIONSHARE - Internal NSA process improvement program (2003-2008) *

LITHIUM - Corporate partner for domestic long-distance cable access under the BLARNEY program (presumably AT&T) * *

LITTLE CLOUD - Airborne collection program using RB-57 aircraft based in Pakistan (1963-1965?)

LOCATOR - Some kind of NSA database *

LODESTAR - Cryptanalytic computer subcomplex at NSA headquarters (1978)

LODESTONE - NSA's CRAY-1 supercomputer

LOGGERHEAD - Device to collect contents of analog cell phone calls (made by Harris Corp.) *

LOLLYGAG - SSO mobile telephone interception program, part of the MYSTIC program *

LOMA - SCI control system for Foreign Instrumentation and Signature Intelligence* *

LONGFELLOW - Soviet cipher system of the 1940s

LOPERS - System for processing data collected from Public Switched Telephone Networks (PSTN) * *

LUSTRE - Memorandum of Understanding regarding the exchange of data between the NSA and the French foreign intelligence service DSGE (2011/12) *

[back to top](#)

M

MACHINESHOP - ? *

MADCAPOCELOT - Sub-program of STORMBREW for collection of internet metadata about Russia and European terrorism

MAESTRO-II - Mini digital core implant, standard TAO implant architecture

MAGIC - Codeword for decrypted high-level diplomatic Nazi messages

MAGIC LANTERN - A keystroke logging software developed by the FBI

MAGNES - Remote SATCOM collection facility

MAGNUM - Series of SIGINT spy satellites (since 1985)

MAGNUMOPUS - TAO computer hacking project *

MAGOTHY - The embassy of the European Union in Washington DC *

MAILORDER - NSA's corporate file transfer and distribution system (SFTP-based?)

MAIN CORE - Federal database of personal and financial data of suspicious US citizens

MAINWAY (MW) - NSA system for contact chaining and analysis of metadata from all sources *

MANASSAS - Former NSA counter-encryption program, succeeded by BULLRUN

MARINA - NSA database of bulk internet metadata

MARKHAM - NSA data system?

MARTES - NSA software tool to prepare reports

MASTERLINK - NSA tasking source

MASTERSHAKE - Tool or database with FORNSAT and WiFi data collection *

MATRIX - Some kind of data processing system *

MAXFLI - System related to the Predator drone *

MAYTAG - Upstream collection site

MEDLEY - Classified Suite A algorithm

MENTOR - Class of SIGINT spy satellites? (since 1995?)

MERCED - The Bulgarian embassy in Washington DC *

MERCURY - Soviet cipher machine partially exploited by NSA in the 1960's

MERCURY - Remote SATCOM collection facility

MESA - Cable access under the FAIRVIEW program *

MESSIAH - NSA automated message handling system

METAWAVE - Warehouse of unselected internet metadata *

METRICS - NSA database probably used for call network analysis, or manage and

rationalize SIGINT assets

METROTUBE - Analytic tool for VPN data *

METTLESOME - NSA Collection mission system

MIDAS - Satellite program

MIDFIELD - Processing system related to FAIRVIEW Transit collection under FAA 704 & 705b *

MILKBONE - Question-Focused Dataset used for text message collection *

MINARET - A sister project to Project SHAMROCK (1967-1973)

MIRANDA - System for managing intelligence requirements of GCHQ customers *

MIRROR - Automated survey system that can for example identify the presence of a VPN; interface to the ROADBED system *

MISTRALWIND - Calling card and private network access under the STORMBREW program *

MONKEYROCKET - Sub-program of OAKSTAR for collecting internet metadata and content through a foreign access point (since 2012)

MONSTERMIND - Program that can automatically react to cyber attacks against the US

MOONLIGHTPATH (EGL?) - Cable tapping facility operated in cooperation with a trusted 3rd Party agency, part of the RAMPART-A program * *

MOONPENNY - The NSA satellite intercept station at Harrogate (Great Britain)

MOONSCAPE - System used at the Waihopai satellite intercept station *

MORAY - Compartment for the least sensitive (Category I) COMINT material, retired in 1999 *

MORECOWBELL (MCB) - Covert HTTP/DNS monitoring system for operations support *

MORPHEUS - Program of the Global Access Operations (GAO) *

MOTHMONSTER - NSA tool for exploiting the TOR network

MOUSETRAP - Sandia implant for EFI *

MOVEONYX - Tool related to CASPORT

MULBERRY - The mission of Japan at the United Nations in New York *

> MUSCULAR (JPM?) - Joint NSA-GCHQ operation to tap the cables linking Google and Yahoo data clouds to the internet * Part of WINDSTOP

MUSKET - Retired SIGINT Exchange Designator for ?

MUSKETEER - NSA's Special Signal Collection unit (military/1990s?)

MYSTIC - SSO unilateral wireless/mobile interception program (since 2009)*

MYSTIC STAR - Presidential Global Communications System

[back to top](#)

N

NASHUA - The mission of India at the United Nations in New York *

NAVAJO - The mission of Vietnam at the United Nations in New York *

NAVARRO - The embassy of Georgia in Washington DC *

NEBULA - Base station router similar to CYCLONE Hx9

NEBULA - Airborne SIGINT system carried by MC-12W aircraft

NECTAR - SIGINT Exchange Designator for ? (retired)

NELEUS - Remote SATCOM collection facility

NEMESIS - SIGINT satellite

NEPTUNE SPEAR - Operation to kill or capture Osama bin Laden (2011)

NEPTUNETHUNDER - Connection for afloat computer network operations like aboard

USS Annapolis *

NESTOR - Family of digital secure voice equipment: KY-8, KY-28, and KY-38

NETBOTZ - Remote monitoring tool

NETFLOW - Certain type of cable tapping sensor *

NETWORKPUMP - Distribution system *

NEWSDEALER - NSA's internal intelligence news network

NEXUS 7 - Successor program of the Real Time-Regional Gateway (RT-RG) * *

NIAGARAFILES - Data transfer tool * * (SFTP-based?)

NIGHTGLOW - System related to the Predator drone *

NIGHTWATCH - Portable computer in shielded case for recreating target monitor from progressive-scan non-interlaced VAGRANT signals

NINJANIC - Something related to TURMOIL *

NITESURF - NSA tool or database

NITRO - Remote SATCOM collection facility

NOCON - NSA dissemination marking or COI

NODDY-3 - Coverage of current and forecasted NRTM circuits under the FAIRVIEW program *

NOMAD - Projected Navy-sponsored and Raytheon-made computer for mass data handling (1951-1954)
 NONBOOK (NK) - Compartment of the ENDSEAL control system
 NORMALRUN - NSA tool or database
 NUCLEARWINTER - Signal Intelligence Directorate team that uses anti-tamper solutions *
 NUCLEON - Database for contents of phone calls
 NYMROD - Automated name-matching and recognition system (since 2008)*

[back to top](#)

O

OAKSTAR - Umbrella program to filter and gather information at major telecommunications companies (since 2004)*
 OBELISK - Codename for Al Qaeda's network of websites and servers *
 OBELISK - GSM collection system *
 OCEAN - Optical collection system for raster-based computer screens *
 OCEANARIUM - Database for SIGINT from NSA and intelligence sharing partners around the world *
 OCEANFRONT - Part of the communications network for ECHELON
 OCEAN SHIELD - NATO anti-piracy operation
 OCEANSURF - Engineering hub of the Global Access Operations (GAO) *
 OCELOT - Actual name: MADCAPOCELOT
 OCTAVE - NSA tool for telephony tasking (succeeded by the UTT in 2011)
 OCTSKYWARD - Collection of GSM data from flying aircraft
 OILSTOCK - A system for analyzing air warning and surveillance data
 OILYRAG - SSO mobile telephone interception program, part of the MYSTIC program *
 OLYMPIA - CSEC tool for discovering and identifying telephone and computer connections
 OMNIGAT - Field network component
 ONEROOF - Main tactical SIGINT database, with raw and unfiltered intercepts; or an analytic tool *
 ONYX - Newer units of the LACROSSE reconnaissance satellites
 ORANGEBLOSSOM - Sub-program of OAKSTAR for collection from an international transit switch (sigad: US-3251)*
 ORANGECRUSH - Sub-program of OAKSTAR for collecting metadata, voice, fax, phone and internet content through a foreign access point
 ORION - SIGINT satellite
 ORLANDOCARD - NSA operation that attracted visits from 77,413 foreign computers and planted spyware on more than 1,000 by using a 'honeypot' computer *
 OSAGE - The embassy of India in Washington DC *
 OSCAR - SIGINT Exchange Designator for the USA
 OSWAYO - The embassy annex of India in Washington DC
 OXCART - The Lockheed A-12 program (better known as SR-71)
 OUTPARKS - NSA's unclassified environment for access to the public internet, operational as of 2004, replaced BRAZEN, AIRGAP, OSIS and NIPRNet *
 OZONE - Some kind of application framework *

[back to top](#)

P

PACKAGEDGOODS (PG) - Globally dispersed and clandestine placed traceroute and DNS processors that map internet connections for the TREASUREMAP tool * *
 PACKET RAPTOR - System for processing internet packet data *
 PACKETSCOPE - Internet cable tapping system
 PACKETSWING - NSA tool or database
 PADSTONE - Type 1 Cryptographic algorithm used in several crypto products
 PAINTBALL - Analysis tool (for social network analysis?) *
 PAINTEDEAGLE - SI-ECI compartment related to the BULLRUN program
 PALANTERRA - A family of spatially and analytically enabled Web-based interfaces used by the NSA
 PALMCARTE - System that feeds FISA data to the Network Analysis Center (NAC)? *
 PANGRAM (PM) - Alleged SCI control system *
 PANOPLY - Populates INTERQUAKE with emitter information and reports *
 PANTHER - The embassy of Vietnam in Washington DC *

PARCAE - SIGINT satellite for ocean reconnaissance. Unclassified codename: WHITE
 CLOUD, a.k.a. Naval Ocean Surveillance System (NOSS); part of CLASSIC WIZARD
 PARTNERMALL PROGRAM (PMP) - A single collaboration environment, to be succeeded
 by the Global Collaboration Environment (GCE) *
 PARTSHOP - ?
 PARTSTREAMER - Codeword related to data exchange at NSA's European Cryptologic
 Center (ECC) *
 PATHFINDER - SIGINT analysis tool (developed by SAIC) *
 PATHWAY - NSA's former main computer communications network
 PATTERNTRACER - Call chaining analysis tool (developed by i2)
 PAWLEYS - SI-ECI compartment related to the BULLRUN program
 PEARL - Retired SIGINT product codeword
 PENDLETON - SI-ECI compartment related to the BULLRUN program
 PENNANT RACE - Airborne SIGINT-based geolocation system carried by MC-12W
 aircraft
 PEPPERBOX - Tool or database for targeting Requests (CSEC?)
 PERDIDO - The mission of the European Union at the United Nations in New York *
 PERFECTMOON - An out-sites covering system
 PERFECTSTORM - Limited FISA authorized collection under the STORMBREW program
 (sigad: US-984P) *
 PERMANENTPRESS - SSO mobile telephone interception program, part of the MYSTIC
 program *
 PHANTOMNOVA - Program in cooperation with Turkey *
 PHYLLIS ANN - Air Force airborne radio direction-finding system on EC-47s (1966-?)
 PHOTOANGLO - A continuous wave generator and receiver. The bugs on the other end
 are ANGRYNEIGHBOR class
 PIEDMONT - SI-ECI compartment related to the BULLRUN program
 PICARESQUE (PIQ) - SI-ECI compartment related to the BULLRUN program
 PICASSO - Modified GSM handset that collects user data plus room audio
 PINECONE - Centralized processing facility for data collected under the FAIRVIEW
 program *
 PINUP - Retired SIGINT product codeword
 PINWALE - Database for recorded signals intercepts/internet content
 PISCES - Joint NSA, CIA and State Department program collecting biometric data on
 border crossings from a wide range of countries *
 PITCHFORD - SI-ECI compartment related to the BULLRUN program
 PIVOT - Retired SIGINT product codeword
 PIXIE - Retired SIGINT product codeword
 PLANTATION - Ggeneral processing computer project, later integrated into HARVEST
 (1950s)
 PLATFORM - Computer system linking the ECHELON intercept sites * and/or internal
 NSA e-mail system
 PLUCKHAGEN - An IRATEMONK implantation for ARM-based Fujitsu drives *
 PLUS - NSA SIGINT production feedback program *
 POCOMOKE - The Brazilian Permanent Mission to the UN in New York *
 POGODA - Soviet cipher system of the 1940s
 POISON NUT - CES VPN attack orchestrator *
 POLARBREEZE - NSA technique to tap into nearby computers *
 POPEYSEAR - Database and with an interface (including GraphViz) used at NSA's
 NTOC floor *
 POPPY - SIGINT satellite program
 POPQUIZ - TURMOIL development data(?) *
 POPROCKS - Some tool, probably related to Computer Network Exploitation (CNE)
 POPTOP - Collection system for telephony data
 POUNDSAND - Prototype Incubator *
 POWDER - Program for surveillance of the Turkish embassy in Washington DC
 POWELL - The Greek mission at the United Nations in New York *
 PREFACE - Processing system for Opscomm at NSA HQ, replacement of TIDE (1978-?)
 PREFER - System for identifying and extracting text messages (SMS) from the
 DISHFIRE database *
 PRESSUREPORT - Software interface related to PRESSUREWAVE
 PRESSUREWAVE - NSA cloud database for VPN and VoIP content and metadata * *
 PRIMECANE - American high-tech company cooperating in providing a network access
 point for the ORANGECRUSH program
 PRISM - Program for collecting foreign internet data from US internet companies

PROFORMA - Intelligence derived from computer-based data
 PROPHET - Mobile tactical SIGINT collection system
 PROTEIN - SIGINT Exchange Designator for ?
 PROTON - Storage and analysis system for the CRISSCROSS database of (telephony?)
 metadata of (counterintelligence) targets; operated by CIA and used by DOJ, DOD and
 NSA *
 PROTOSS - Local computer handling radio frequency signals from implants
 PURPLE - Codename for a Japanese diplomatic cryptosystem during WWII
 PURPLE DRAGON - US military OPSEC program (since 1966)
 PUTTY - NSA tool or database
 PUZZLECUBE - TAO division tasking tool
 PYLON - SIGINT Exchange Designator for ?

[back to top](#)

Q

QUADRANT - A crypto implementation code
 QUADRESPECTRE PRIME - ?
 QUANTUM - Secret servers placed by NSA at key places on the internet backbone;
 part of the TURMOIL program *
 QUANTUM LEAP - CIA tool to "find non-obvious linkages, new connections, and new
 information" from within a dataset *
 QUARTERPOUNDER - Upstream collection site
 QUASAR - Relay satellite for reconnaissance satellites
 QUEEN BEE CHARLIE/DELTA - Airborne SIGINT missions using C-130s in South-East
 Asia (1964-1965?)
 QUEENSLAND - Upstream collection site
 QUICKPOINT - Distribution system *

[back to top](#)

R

RADIOSPRING - ?
 RADIANT - First word for two dozen Navy tactical-national data sharing systems,
 including satellites and stealth drones *
 RADIANT GEMSTONE - System from the RADIANT family, installed at the USS
 Annapolis around 2005 *
 RADIUS - Systems that logs ISP dial up customer records, which can create a "natural
 link" between DNR and DNI datasets *
 RADON - Host tap that can inject Ethernet packets *
 RAGTIME (RGT) - ECI compartment for call and e-mail content collected under FISA
 authority *
 RAILHEAD - NCTC database project
 RAINFALL - (NSA unit for decrypting) Russian secure, encrypted voice communications
 (around 1979)*
 RAINFALL - Unclassified codename for RHYOLITE/AQUACADE SIGINT satellites
 RAINFALL - Probably the joint CIA/NSA/DSD satellite ground station in Pine Gap,
 Australia *
 RAISIN - NSA database or tool
 RAMPART-A (RAM-A) - Program for collecting information about Russia, the Middle
 East and North-Africa, in cooperation with at least five 3rd Party partner agencies
 (since 1992)*
 RAMPART-I (RAM-I) - Program for collecting communications from Iraq
 RAMPART-M (RAM-M) - Program for collecting data from undersea fiber-optic cables
 about terrorists, arms traders and Iraq (since 1986)*
 RAMPART-T (RAM-T) - Program providing access to land-based cables, in cooperation
 with the CIA, to collect communications from state leaders and their entourage (since
 1991)*
 RAMPART-X (RAM-X) - Program for collecting information from Afghanistan *
 RAMROD - Unclassified codename for a SIGINT satellite, possibly the 1994-96 ORION
 launches
 RANCIDRINSE - SSO mobile telephone interception program, part of the MYSTIC
 program *
 RANGER - Unclassified codename for a SIGINT satellite (post-2000 launches)
 RATTAN - Codename for overall US effort against Soviet codes (1945-1946, later

BOURBON)*
 RAVEN - SIGINT satellite
 REACTOR - Tool or program related to MARINA? *
 REBA - Major NSA backbone project *
 RECOVERY - ? *
 RED DISK - DIA cloud system to distribute information, images and video to soldiers and other military intelligence users.
 REDHARVEST (RDV) - ECI compartment that protects names, locations and techniques of RAMPART-A cable tapping facilities *
 REDHAWK - NSA tool
 REDRACE - Airborne SIGINT system used for Direction Finding/geolocation and to collect VHF communications
 REDROOF - NSA tool
 REGAL - Compartment for Top Secret COMINT information derivated from the Berlin Tunnel operation (1955-?)
 REMATION - Joint NSA-GCHQ counter-TOR workshop *
 RENOIR - NSA telephone network visualization tool
 REQUETTE - A Taiwanese TECO in New York *
 RESERVE (RSV) - Control system for the National Reconnaissance Office (NRO)
 RESERVEVISION - Remote monitoring tool
 RESOLUTETITAN - Internet cable access program?
 RETRO - see RETROSPECTIVE
 RETROSPECTIVE - 30-day retrospective retrieval tool for SCALAWAG *
 RHINEHART - Tool for both real-time and retrospective keyword-searching of vast amounts of voice content (introduced in 2004, replaced by VoiceRT)*
 RHYOLITE - Class of SIGINT spy satellites (in 1975 changed to AQUACADE)
 RICHTER - SIGINT Exchange Designator for Germany
 RIMROCK - Access to 4ESS circuit switches under the FAIRVIEW program *
 RINGBILL - Some kind of communications traffic, including Internet data *
 RIPCORD - ?
 RIVET GYM - Codename for the four SIGINT positions aboard EC-121 COLLEGE EYE aircraft (Vietnam War)
 RIVET JOINT - Reconnaissance operation
 ROADBED - Probably a military SIGINT database
 ROCKSALT - Corporate partner for domestic long-distance cable access under the BLARNEY program *
 ROCKYKNOB - Optional DSP when using Data Over Voice transmission in CROSSBEAM
 RODEHOUSE - Offsite language processing center for Arabic, Amharic, Pasto/Dari and Tagalog (since 9/11) *
 ROGUE - Cryptanalytic computer from the early 1950s, the first using remote terminals connected to a central processor *
 ROLLERCOASTER - Tool or system that provides access to phone metadata, analyst queries and results of SKYNET Analytics *
 RONIN - NSA tool for detecting TOR-node and/or mobile IP-addresses * *
 RORIPA - SIGINT Exchange Designator for ?
 ROSTER - Unclassified codename for MAGNUM/ORION SIGINT satellites *
 ROUTEMASTER - Server/router for VoIP and audio traffic *
 ROUTEVIEWS - Open source information used for the TREASUREMAP tool *
 ROYALNET - Internet mapping tool to determine access points for target's communications *
 RUFF - Compartment of TALENT KEYHOLE for satellite imagery *
 RUFFER - Unclassified codename for JUMPSEAT/TRUMPET SIGINT satellites
 RUMBUCKET - Analytic tool to access FORNSAT data residing on GINPENNANT *
 RUNWAY - Unclassified codename for CANYON/CHALET/VORTEX SIGINT satellites; or a processing system at Menwith Hill *
 RUSTICBAGGAGE - Data source for the TREASUREMAP tool *
 RUTLEY - Unclassified codename for the MERCURY SIGINT satellites (launched 1995-2003); or a processing system at Menwith Hill *
 RYE - NSA-developed software for Univac 490 computers (introduced 1963) or a system through which 200 remote terminals could access 4 main machines (since 1972)*
 RYE - Computer complex supporting CSOC/NSOC, internetting Opscomm circuits, running several softwares including TIDE (late 1960s-?)

S

SABERTOOTH - SIGINT training program for South Vietnam government (launched in 1961)

SABRE - Retired SIGINT product codeword

SAGUARO (or SAGURA?) - Access to AT&T internet backbone cables under the FAIRVIEW program *

SAGURA (or SAGUARO?) - Access to AT&T internet backbone cables under the FAIRVIEW program *

SALEM - ?

SALTYDOGS - Tool to find frequency and carrier rates and discover signal characteristics of satellite links *

SAMOS - Reconnaissance satellite program

SANDKEY - Joint NSA/DEA program that intercepts and exploits unencrypted VHF voice communications of narco-traffickers at sea *

SAPPY - Retired SIGINT product codeword

SARACEN - Intercept operation using unmanned equipment on a hilltop (Vietnam War, 1972)

SARATOGA - SSO access facility (since 2011) * *

SARDINE - SIGINT Exchange Designator for Sweden

SAVILLE - Narrow band voice encryption for radio and telephone communication

SAVIN - Retired SIGINT product codeword

SCALAWAG - Collection facility under the MYSTIC program *

SCALLION - Upstream collection site

SCAMPI - Secure voice and data network for C4I communications between the commander and the components of the US Special Operations Command, operational sites and other government agencies *

SCAPEL - Second Party satellite intercept station in Nairobi, Kenya

SCATTERED CASTLES - US Intelligence Community database of security clearance holders (since 2008) *

SCHOOLMONTANA - Software implant for Juniper J-series routers used to direct traffic between server, desktop computers, corporate network and internet

SCIMITAR - A tool to create contact graphs? *

SCISSORS - Data scanning, formatting and distribution system *

SCORECARD - NSA tool or database

SCORPIOFORE - SIGINT reporting tool *

SCQAWK - The "SID Mailbag" in the newsletter of NSA's Signals Intelligence Directorate

SEABOOT - SIGINT Exchange Designator for ?

SEADIVER - Collection system for telephony data

SEAGULL - Secure Allied Communications ISO BMD at COMUSSIXTHFLT *

SEARCHLIGHT - NSA's internal corporate directory service for personnel information *

SEARCHLITE - Tactical SIGINT collecting system for like cell phone calls

SEA SENTRY - Program for collecting radar signatures from shipping traffic in the Dardanelles *

SEA SENTRY II - Choke point collection program in cooperation with Turkey *

SEASIDEFERRY - Commercially purchased data source for the TREASUREMAP tool *

SECUREINSIGHT - A software framework to support high-volume analytics

SEED SPHERE - Computer network "intrusion set" already identified in 2007 *

SEENFLARE(?) - Codeword related to data exchange at NSA's European Cryptologic Center (ECC) *

SEMESTER - NSA SIGINT reporting tool

SEMITONE - System that monitors fax and voice messages *

SENIOR SCOUT - Transportable suite of ISR equipment (since 1991)

SENIOR SPAN - Radome on top of the U2 to relay SIGINT data to ground stations

SEAGULL - Servers used for Business Record FISA collection under the FAIRVIEW program *

SENTINEL - NSA database security filter*

SENTRY EAGLE (SEE) - Overarching umbrella program for ECI compartments and SAP programs of the National Initiative to protect US cyberspace

SENTRY HAWK - ECI compartment of SENTRY EAGLE that protects information about Computer Network Exploitation *

SENTRY FALCON - ECI compartment of SENTRY EAGLE that protects information about Computer Network Defense *

SENTRY OSPREY - ECI compartment of SENTRY EAGLE that protects information about

HUMINT enabled SIGINT *

SENTRY RAVEN - ECI compartment of SENTRY EAGLE that protects information about exploitation of encipherment *

SENTRY CONDOR - ECI compartment of SENTRY EAGLE that protects information about general Computer Network Operations *

SENTRY OWL - ECI compartment of SENTRY EAGLE that protects information about relationships with industry *

SERENADE - Corporate partner for domestic long-distance cable access *

SERRATEDEDGE - Conflict number access under the STORMBREW program *

SERUM - Bank of servers within ROC managing approvals and ticket system

SETTEE - Former SIGINT Exchange Designator for South Korea

SHADOWCAT - Some system to be used at the Waihopai satellite station, New Zealand *

SHAMROCK - Operation for intercepting telegraphic data going in or out the US (1945-1975)

SHAREDQUEST (SQ) - Contains the DARKQUEST program *

SHAREDQUEST - 5-Eyes modernization program for the satellite interception architecture (follow-up of SHAREDVISION) *

SHAREDVISION (SV) - 5-Eyes modernization program for the satellite interception architecture (until 2010, followed by SHAREDQUEST) *

SHARKFIN - Sweeps up all-source communications intelligence at high speed and volumes *

SHELLTRUMPET - NSA metadata processing program (since December 2007)*

SHENANIGANS - Aircraft-based NSA geolocation system used by CIA *

SHERMAN - Cryptanalytic computer subcomplex at NSA HQ (1978)

SHIFTINGSHADOW - Sub-program of OAKSTAR for collecting telephone metadata and voice content from Afghanistan through a foreign access point

SHILLELAGH - Classified Suite A algorithm

SHORTHAND - Project initiated in 1966 to employ South Vietnamese as linguists in US LLVI operations

SHOTGIANT - NSA operation for hacking and monitoring the Huawei network (since 2009)

SIDELIGHT - Codeword related to data exchange at NSA's European Cryptologic Center (ECC) *

SIERRAMIST - Tool to support various file systems *

SIGABA - American high-level cipher machine used from World War II until the 1950s, also known as ECM Mark II

SIGCOM - (National) Signals Intelligence Committee *

SIGINT NAVIGATOR - NSA analytic tool used in combination with MAINWAY

SIGSALY - The first secure voice system, used during World War II, also known as Green Hornet

SILKWORTH - A software program used for the ECHELON system

SILLYBUNNY - Some kind of webbrowser tag which can be used as selector *

SILO - Research project in high-speed computer memory, later integrated into HARVEST (1950s)

SILVER - Soviet cipher machine, 1950s-1960s, partially exploited by NSA in the 1960's

SILVER COLLAM (SC) - The only FAIRVIEW collection site outside continental USA, but considered US territory, most likely operated by AT&T *

SILVERCOMET - SIGINT satellites? *

SILVER PEAK - WAN optimization project at Waihopai satellite station, New Zealand *

SILVERZEPHYR (SZ) - Sub-program of OAKSTAR for collecting phone and internet metadata and content from Latin and South America through an international transit switch

SIRE - A software program used for the ECHELON system(?)

SKIDROWE - System for processing low speed internet traffic, replaces WEALTHYCLUSTER2 and interoperates with XKEYSCORE *

SKIPJACK - Type 2 Block cipher algorithms used in various crypto products

SKOPE - SIGINT analytical toolkit

SKYNET - Collaborative cloud research program to identify patterns of suspect activity from bulk telephony data *

SKYSCRAPER - Interface to the ROADBED system

SKYWRITER - NSA tool to prepare (internet) intelligence reports

SLINGSHOT - End Product Reports (CSEC?)

SLIVER - Proof-of-Concept for cross-mission use of passive IP sensors *

SMARTTRACKER - Analytic tool for detecting geolocational patterns in cell phone usage

*
SMOKEYSINK (SMK) - Cable tapping facility operated in cooperation with a 3rd Party agency, part of the RAMPART-A program (closed in June 2011)*
SNICK - GCHQ satellite intercept station in Oman
SNOWHAZE - NSA tool or database *
SOAPOPERA - (former?) database for voice, end product and SRI information *
SOARING EAGLE - Some US military/intelligence network protection program *
SOCIALSTAMP - Commercially purchased data source for the TREASUREMAP tool *
SOCIOPATH - Storage and/or distribution system *
SODAPRESSED - Linux application persistence *
SOLO - NSA-developed general-purpose cryptanalytic computer, the world's first entirely using transistors, later marketed by Philco as Transac S-1000 (mid-1950s) *
SOMALGET - Umbrella program for collecting content from mobile phone networks of two entire countries, part of MYSTIC (sigad: US-3310**)
SORA-2 - IP expansion effort for the FAIRVIEW program *
SORTINGHAT - ?
SORTINGLEAD - NSA tool or database *
SOUNDER - Second Party satellite intercept station at Cyprus
SOUTHWINDS - Collection program for Inmarsat satellite communications, first for its EMEA region, later global coverage *
SPARKLEPONY - Tool or program related to MARINA *
SPEARGUN - Cable access program of New Zealand's GCSB *
SPECTRE - SCI control system for intelligence on terrorist activities *
SPECULATION - Protocol for over-the-air communication between COTTONMOUTH computer implant devices, compatible with HOWLERMONKEY
SPHINX - Counterintelligence database of the Defense Intelligence Agency
SPINALTAP - NSA program for combining data from active hacking operations and passive signals intelligence collection *
SPINNERET (SPN) - Cable tapping facility operated in cooperation with a trusted 3rd Party agency, part of the RAMPART-A program * *
SPIRITFIRE - Robust voice processing system based on speech-to-text keyword search and paired dialogue transcription (succeeded VoiceRT in 2013) *
SPIT - Typewriter designed for copying morse code; project named for SPecial Intercept Typewriter (1957)
SPITEFULANGEL - Hacking tool or method in or for the Python programming language *
SPLITGLASS - NSA analytical database *
SPLUNK - Tool used for SIGINT Development
SPOKE - Compartment for less sensitive (Category II) COMINT material, retired in 1999 * but apparently still in use as unpublished SCI control system
SPOTBEAM - ?
SPORTCOAST - Upstream collection site
SPRIG - Retired SIGINT product codeword
SPRINGRAY - Some kind of internal notification system *
SPYDER - Analytic tool for selected content of text messages from the DISHFIRE database *
STARBURST - The initial code word for the STELLARWIND compartment
STARFIRE - NSA contact chaining algorithm (developed in 1999) *
STARLIGHT - Analyst tool
STARPROC - User lead that can be used as a selector *
STARPROC - Processing system for intercepting foreign Lawful Intercept systems *
STARSEARCH - Target Knowledge tool or database (CSEC?)
STATEROOM - Covert SIGINT collection sites based in US diplomatic facilities *
STEALTHFIGTHER - Codeword found in the source code used by the Equation hacking group *
STEELFLAUTA - SSO Corporate/TAO Shaping program
STEELKNIGHT - (foreign?) partner providing a network access point for the SILVERZEPHYR program *
STEELWINTER - A supercomputer acquired by the Norwegian military intelligence agency *
STEEPLEBUSH - Program to expand satellite interception capabilities at Menwith Hill ca. 1980 *
STELLAR - Second Party satellite intercept station at Geraldton, Australia
STELLARWIND (STLW) - SCI compartment for the President's Surveillance Program information

STEPHANIE - Covert listening post in the Canadian embassy in Moscow (est. 1972)
 STINGRAY - Device for tracking the location of cell phones (made by Harris Corp.) *
 STONEGATE - System used at the Waihopai satellite intercept station * also a processing system related to FAIRVIEW and BLARNEY collection *
 STONEGHOST - DIA network for information exchange with UK, Canada, Australia and New Zealand (TS/SCI)
 STONEHOUSE - Site built in the 1960s at Asmara, Ethiopia, for collection against the Soviet space program. Featured two 150-foot diameter dishes (closed in 1975).
 STONE RUBY - Intelligence exchange agreement between DIA and the Israeli military intelligence directorate (1996) *
 STORMBREW - Domestic cable tapping program in cooperation with Verizon (since 2001) *
 STORMFORCE - Hardware modem for processing satellite signals *
 STRATOS - Tool or database for GPRS Events (CSEC?)
 STRAWHAT - NSA datalinks between field sites and processing centers (1969-?)*
 STREAMLINER - NSA-developed automatic switch for communications centers (early 1970s)
 STRETCH - IBM high-performance computer project, later integrated into HARVEST (1950s)
 S-TRICKLER - Tool or database with IP address fingerprints and potential vulnerabilities from the FORNSAT collection *
 STRONGMITE - Computer at remote operations center used for long range communications
 STRUM - (see abbreviations)
 STYGIAN FLOW - FBI nickname for network intrusions for which assistance of the NSA was asked *
 STYLISHCHAMP - Tool that can create a HPA on a hard drive and then provide raw reads and writes to this area *
 SUBSTRATUM - Upstream collection site
 SUEDE - Compartment for Top Secret COMINT information (1951-1952) *
 SULPHUR - The mission of South Korea at the United Nations in New York *
 SUNSCREEN - Tool or database
 SURFBOARD - System for processing data from (satellite?) telephone networks *
 SURPLUSANGAR (SH) - High to low diode, part of the QUANTUM system *
 SURREY - Main NSA requirements database, where tasking instructions are stored and validated, used by the FORNSAT, SSO and TAO divisions *
 SWEEPFORWARD - Repository for manually processed target data (2009) *
 SYNAPSE - NSA tool for analyzing target connections *

[back to top](#)

T

TABLON - Experiment of mass data storage technology, overtaken by disk storage technology (1960s)
 TACOSUAVE - ?
 TALENT KEYHOLE (TK) - Control system for space-based collection platforms
 TALISMAN - Replaced the Consolidated Authoring Tool (CAT) in 2003 *
 TALK QUICK - An interim secure voice system created to satisfy urgent requirements imposed by conditions to Southeast Asia. Function was absorbed by AUTOSEVOCOM
 TAPERLAY - Covername for the Global Numbering Data Base (GNDB) containing telephony and provider information *
 TARMAC - Program to intercept satellite communications at Menwith Hill Station *
 TAROTCARD - NSA tool or database
 TATTOO - Server used for vPCS shaping operations under the STEELFLAUTA program *
 TAWDRYYARD - Beacon radio frequency radar retro-reflector used to positionally locate deployed RAGEMASTER units
 TEABALL - Direct SIGINT support to fighter escorts of operation Linebacker (1972)
 TELLURIAN - Internet packet processing system, maybe also used to forward data from the collection site to NSA headquarters.
 TEMPEST - Spying on information systems through leaking emanations, including unintentional radio or electrical signals, sounds, and vibrations (codename originally from a COMSEC point of view, not an attacker's one)
 TENNIS - Network to remote-operate intercept facilities through satellite links (1967-?)
 THAWFACTOR - Codeword related to data exchange at NSA's European Cryptologic

Center (ECC) *

THESPIS - SIGINT Exchange Designator for ?

THINTREAD - Prototype program for wiretapping and sophisticated analysis of the resulting data (dismissed in 2002 in favor of TRAILBLAZER)

THIEVING MAGPIE (TM) - Program for collecting metadata of mobile phones from airplane passengers; data source for HOMING PIGEON *

THUMB - Retired SIGINT product codeword

THUNDERCLOUD - Data enrichment tool, collaborative program between NSA units T1222 and SSG *

TIAMAT - Joint venture between the German BND and another country with access for NSA *

TICKETWINDOW - System for sharing Special Source collection among the Five Eyes partners *

TIDALSURGE - Router Configurations tool (CSEC?)

TIDE - Software managing the KLIEGLIGHT database

TIDEWAY - Part of the communications network for ECHELON

TIKICUBE - Unit of NSA's Security and Counterintelligence division (2014)

TIMBERLINE - The NSA satellite intercept station at Sugar Grove (US)

TINMAN - Database related to air warning and surveillance

TINSEL - Processing system related to FAIRVIEW and BLARNEY collection *

TITANPOINTE (TP) - Centralized processing facility for FISA data collected under the BLARNEY and FAIRVIEW programs, most likely located in the AT&T switch at 33 Thomas Street in New York City * *

TITLEHOLDER - NSA tool

TOPAZ - Satellite program

TOPROCK - Facility for access to 4ESS circuit switches under the FAIRVIEW program *

TORUS - Satellite antenna that allows multiple satellites to be viewed simultaneously *

TOWER - SIGINT Emitter Database (SEDB) Query-Focussed Dataset (QFD) fed by telephony metadata from the GMHalo cloud *

TOWERPOWER - NSA tool or database

TOXICARE - NSA tool

TOYGRIPPE - NSA repository of VPN endpoints and metadata * *

TRACFIN - NSA database for financial data like credit card purchases *

TRACTOR - IBM-developed tape drives loading system, used for HARVEST (1960s)

TRAFFICCHIEF - Part of the TURBULENCE umbrella program

TRAILBLAZER - NSA Program to analyze data carried on communications networks (2002-2006, replaced by TURBULENCE)

TRAILMAPPER - NSA tool or database

TRANSIENT - Sub-program of FROSTING directed against Soviet satellites *

TRANSX - Translation, transcription and transliteration system *

TREASUREMAP (TM) - Mapping, exploration and analysing tool that provides a near-real time, interactive map of the global internet *

TREASURETROVE - Analytic tool

TREBLECLEF - System for data received from hacking operations? *

TRIBUTARY - NSA provided voice threat warning network

TRIGGERFISH - Device to collect the content of digital cell phone calls (made by Harris Corp.) *

TRINE - Compartment for Top Secret COMINT information, predecessor of UMBRA (1965-1968) *

TRIEME - System for processing internet packet data *

TRITON - Tool or database for TOR Nodes (CSEC?)

TROJAN SPIRIT - Tactical network for sharing intelligence information with customers in the field

TROPICPUMA - Fax processing capability *

TRUMPET - Series of ELINT reconnaissance satellites (1994-2008)

TUBE - Database for selected internet content? *

TUMULT - Part of the TURBULENCE program

TUNDRA - DSP Research of new statistics for codebook analysis *

TUNDRAFREEZE - NSA's main in-house facial recognition program *

TUNINGFORK - NSA database or tool for protocol exploitation

TURBINE - Active SIGINT: centralized automated command/control system for managing a large network of active computer implants for intelligence gathering (since 2010) *

TURBULENCE (TU) - Integrate NSA architecture with several layers and sub-programs to detect threats in cyberspace (since 2005)

TURMEROL - ? *

TURMOIL (TML) - Passive SIGINT sensors: filtering and collection (with selection at the packet level) of internet traffic on high-speed satellite, microwave and cable links, part of the TURBULENCE program * * Maybe also for selecting common internet encryption technologies to exploit.*

TURNSTILE - SAGUARO VoIP access processing system *

TURNWEALTHY - Component for signal acquisition within the SKIDROW system, replacement for WEALTHYCLUSTER *

TURTLEPOWER - System to process VoIP communications data *

TUSKATTIRE - Ingest system for cleaning/processing/normalizing DNR (telephony) data *

TUTELAGE - Active defense system with detection sensors that monitor network traffic at for example the NIPRNet in order to detect malicious code and network attacks, part of the TURBULENCE program *

TWEED - Retired SIGINT product codeword

TWISTEDPATH - NSA tool or database

TYPHON - Airborne SIGINT system carried by MC-12W aircraft

TYPHON HX - GSM base station router network in box for tactical Sigint geolocating and capturing user

[back to top](#)

U

ULTIMATE - CIA operation sending weather balloons into Eastern Europe in order to map Soviet defense radar activity (1950s) *

ULTRA - Compartment for Top Secret COMINT information, like decrypted high-level military Nazi messages (until 1946)

UMBRA - Compartment for the most sensitive (Category III) COMINT material (1968-1999) * but apparently still in use as unpublished SCI control system

UNIFORM - SIGINT Exchange Designator for Canada

UNITY - System for processing data collected from telephony networks * through a SAGUARO access under the FAIRVIEW program *

USHER - Retired SIGINT product codeword

[back to top](#)

V

VANGUARD - Certain type of cable tapping sensor *

VENATOR - Access to a Philippine mobile network provider, part of the MYSTIC program *

VENONA - Joint US-UK project for decrypting historical intercepts of one-time pad messages from the KGB; previously codenamed JADE, BRIDE and DRUG subsequently

VENUSAFFECT - System used at the Waihopai satellite intercept station *

VERDANT (VER) - Alleged SCI control system *

VESUVIUS - Prototype quantum computer, situated in NSA's Utah Data Center

VICTORYDANCE - Joint NSA-CIA operation to map WiFi fingerprints of nearly every major town in Yemen *

VICTORYUNIFORM - Special Source collection *

VIEWPLATE - Processor for external monitor recreating target monitor from red video

VINEYARD - System used at the Waihopai satellite intercept station *

VINSON - KY-57/58 family of voice encryption systems

VINTAGE - System used at the Waihopai satellite intercept station *

VINTAGE HARVEST - Probably a military SIGINT tool

VISIONQUEST (VQ) - System used at the TITANPOINTE access point under the BLARNEY program

VOICESAIL - Intelligence database?

VORTEX - Class of SIGINT spy satellites (1978-1989)

VOTEDOOR - NSA managed server for the InfoWorkSpace (IWS) collaboration tool (2003) *

VOXGLO - Multiple award contract providing cyber security and enterprise computing, software development, and systems integration support *

[back to top](#)

W

WABASH - The embassy of France in Washington DC *

WAGONBED - Hardware GSM controller board implant on CrossBeam or HP Proliant G5 server that communicates over I2C interface

WALBURN - High-speed link encryption, used in various encryption products

WATERFRONT - Processing system for data collected from vPCS shaping under the STEELFLAUTA program *

WATERWITCH - Hand-held tool for geolocating targeted handsets to last mile

WAVELEGAL - Authorization service that logs data queries

WAYLAND - Processing system related to FAIRVIEW Transit collection under FAA 704 & 705b *

WEALTHYCLUSTER (WC) - Processing system for low data rate internet traffic, that sessionizes all the data on the link before sending it to XKEYSCORE (since 2002, will be replaced by TURMOIL) * *

WEALTHYCLUSTER2 (WC2) - Protocol processing & session reassembly *

WEASEL - Type 1 Cryptographic algorithm used in SafeXcel-3340

WEBCANDID - NSA tool or database

WEE LOOK - ELINT systems on Navy EA-3Bs detecting SAM radars (Vietnam War)

WELLGROUNDED - Proposed, but not implemented internal NSA oversight program (early 1990s)

WELLSPRING - Tool that strips out facial images from e-mails and other communications, and displays those that might contain passport images *

WESTPORT - The mission of Venezuela at the United Nations in New York *

WHARPDRIVE - Joint venture between the German BND and another country with access for NSA (2013)* *

WHIPGENIE (WPG) - ECI compartment for details about the STELLARWIND program *

WHITEBIRCH - ASA project to set up an HF-DF network in South East Asia (initiated 1961)

WHITEBOX - Program for intercepting the public switched telephone network? *

WHITE WOLF - Joint Chiefs of Staff "advisory warning" program for all peripheral airborne reconnaissance missions (1963-?)

WHITE CLOUD - Unclassified codename for the PARCAE SIGINT satellite for ocean reconnaissance

WHITELIST - NSA tool

WHITESQUALL - International gateway switch access under the STORMBREW program *

WHITETAMALE - Operation for collecting e-mails from Mexico's Public Security Secretariat *

WHIZBANG - Training program (?)*

WILLOW - Combination of a JUMPSEAT satellite and Low-Earth Orbit Program-989 ELINT sub-satellites (since 1982)

WILLY - AFSS COMINT support program during the Korea War (1950-?)

WINDCHASER - Tool or program related to MARINA *

WINDSORBLUE - Supercomputer program at IBM *

WINDSTOP - Umbrella program for 2nd Party high-volume cable tapping programs *

WISPYKNIT - Special Source collection *

WIRESHARK - Database with malicious network signatures

WISPYKNIT - Special Source collection *

WISTFULTOLL - Premiere target survey tool for Windows that runs on almost all targets automatically. It brings back informatio about the target system's machine and operating system *

WITCH - Retired SIGINT product codeword

WITCHHUNT - ?

WOLFPOINT - SSO corporate partner under the STORMBREW program *

WORDGOPHER - Platform to enable demodulation of low-rate communication carriers

Wordscape - Vocabulary tool used at NSA

WRANGLER - Database or system which focuses on Electronic Intelligence

[back to top](#)

X

XCONCORD - Program for finding key words in foreign language documents

XKEYSCORE (XKS) - Computer system for indexing and searching internet communications

[back to top](#)

Y

YACHTSHOP - Sub-program of OAKSTAR for collecting internet metadata

YANKEE - Part of the PINWALE database (NOFORN partition?) *

YELLOWSTONE - NSA analytical database *

YIELD - Combination of a JUMPSEAT satellite and low-Earth orbit Program-989 ELINT sub-satellites (since 1982)

YOKE - AFSS tactical voice intercept support program during the Korea War (1951-?)

YUKON - The embassy of Venezuela in Washington DC *

[back to top](#)

Z

ZAP - (former?) database for texts *

ZARF - Compartment of TALENT KEYHOLE for ELINT satellites, retired in 1999 *

(Some contributions were also made by Zone d'Intérêt)

- See also this list of NSA codewords from 2002

Links and Sources

- NSA Observer: Things the NSA doesn't want you to know
- List of NSA Code Names Revealed
- About What the NSA's Massive Org Chart (Probably) Looks Like
- About Code Names for U.S. Military Projects and Operations
- National Reconnaissance Office: Review and Redaction Guide (pdf)
- About How Codes Names Are Assigned
- Wikipedia article about the Secret Service codename
- List of crypto machine designators
- Wikipedia article about the CIA cryptonym
- Article about Security Clearances and Classifications
- Listing in German: Marjorie-Wiki: SIGDEV
- Another list in German: Geheimdienstliche Akronyme und Codenamen
- William M. Arkin, Code Names, Deciphering U.S. Military Plans, Programs, and Operations in the 9/11 World, Steerforth Press, 2005.



+20 Recommendations on Google

18 comments:

Anonymous said...

the latest bombshells from the washington post are particularly rich sources. The reports, not the article.

Also you're missing Silverzephyr and Steelknight from O Globo (ther is an infographic. and a picture on the wikipedia 2013 mass surveillance disclosures article, which now looks halfway decent.

also, go the the nsa's website, and look at the United States v Thomas drake. you will see a document mentioning Turbulance, turmoil tutelege and traffichief, and note that that traffichief does interact with xkeyscore.

Lithium, blarney, oakstar, fairfiw are mentinoed on a press release. that release describes them as aliases for corporations. Which means that they are all part of SSO. So is Silverzephyr. But check the washinton post's