

NSA Code Names Revealed

Posted on [March 13, 2012](#) | [13 Comments](#)

The list below current NSA (and NSA-contractor) programs (as of March 13, 2012) involved in all aspects of signals intelligence (SIGINT) collection, processing, analysis, dissemination, and storage. Some are purely administrative programs, some are tools and databases associated with social network analysis, metadata analysis, and target research. The current focus of NSA's work seems to be the telecommunications infrastructure to include wireless, optical, electrical, and converged networks.

Current intelligence lingo associated with these programs include:

- Dial Number Recognition (DNR)
- Digital Network Intelligence (DNI)
- Geospatial Metadata Analysis (GMA)
- SIGINT Geospatial Analysis (SGA)
- SIGINT Terminal Guidance (STG)

THE PROGRAMS

AGILEVIEW: DNI tool

AGILITY: DNI tool

AIRGAP/COZEN

AIGHANDLER: Geolocation analysis

ANCHORY/MAUI: DNI

ARCANAPUP

ARTEMIS: Geospatial analysis

ASSOCIATION

AUTOSOURCE

BEAMER

BELLVIEW

BLACKPEARL

CADENCE/GAMUT: Collection mission system for tasking

CHALKFUN

CINEPLEX

CLOUD

COASTLINE

COMMONVIEW

CONTRAOCTAVE

CONVERGENCE

COURIERSKILL: Collection mission system

CREEK

CREST

CROSSBONES

CPE (Content Preparation Environment): Reporting tool

CULTWEAVE: SIGINT database

CYBERTRANS

DISHFIRE: DNI

DOUBLEARROW

DRAGONFLY: Geolocation analysis

Enhanced WEALTHYCLUSTER (EWC)

ETHEREAL: DNI

FASCIA

FASTSCOPE

FOREMAN

GAMUT/UTT

GISTQUEUE

GJALLER: Geospatial analysis

GLAVE

GLOBALREACH

GOLDMINER

GOLDPOINT

GOSSAMER: Geospatial analysis

GROWLER: Geospatial analysis

HERCULES: CIA terrorism database

HIGHTIDE/SKYWRITER: Desktop dashboard

HOMEBASE

INFOSHARE

JOLLYROGER

KINGFISH: Geospatial analysis

LIQUIDFIRE

MAINWAY: DNI signals navigation database

MARINA: Database

MASTERLINK: Tasking source

MASTERSHAKE

MAUI/ANCHORY

MESSIAH

METTLESOME: Collection mission system

NEWHORIZONS

NIGHTSURF

NORMALRUN/CHEWSTICK/FALLENORACLE

NUCLEON

OCTAVE: DNI/DNR tool for tasking

PATHMASTER/MAILORDER

PINWALE: DNI database

PANOPTICON

PRESENTER

PROTON: SIGINT database

RAVENWING

RENOIR: Visualization tool

ROADBED

SCORPIOFORE/CPE

SHARKFINN

SKOPE: SIGINT analytical toolkit

SKYWRITER: DNI reporting tool

SNAPE

SPOTBEAM

STINGRAY: Geospatial analysis

SURREY

TAPERLAY

TAROTCARD

TEMPTRESS: Geolocation analysis

TRACFIN

TRAILMAPPER

TREASUREMAP: DNI visualization tool

TRICKLER

TUNINGFORK/SEEKER: DNI

TURMOIL: Collection mission system

TUSKATTIRE

TWISTEDPATH

UIS/PINWALE: DNI

UTT: DNR tool for tasking

WEALTHYCLUSTER: Collection mission system

WIRESHARK

WITCHHUNT: Geolocation analysis

XKEYSCORE: DNI collection mission system


YELLOWSTONE/SPLITGLASS

[About these ads](#)

SHARE THIS:

- [Twitter101](#)
- [Facebook49](#)
- [LinkedIn4](#)
-

LIKE THIS:

 This entry was posted in [Arkin's Lists](#), [Spying](#) and tagged [code names](#), [NSA](#). Bookmark the [permalink](#).
← [Deterrence and Iran. Secrecy Gets in the Way](#)
[Getting to the Bottom of the Intelligence Community: Is There a Way?](#) →

13 RESPONSES TO NSA CODE NAMES REVEALED

1. *unnamed* | [June 16, 2013 at 2:31 pm](#) | [Reply](#)

Interesting that ETHEREAL and WIRESHARK are, respectively, the previous and current names for a network protocol analysis tool <https://www.wireshark.org/about.html>

2. *Cruella* | [June 17, 2013 at 3:37 am](#) | [Reply](#)

The goal of terrorism is get get a gov't to react and clamp down on it's own constituents. It seems that goal is being met...

3. *Thebes* | [July 1, 2013 at 9:58 am](#) | [Reply](#)

So now they are using Tarot Cards and Hunting Witches???

They have so many spy programs that one is left to wonder in how many different ways the NSA

backs up all Americans' data. Perhaps they could be nice enough to provide us copies when our computers crash?

I'm very troubled by this....

4. *Quatsch* | [July 1, 2013 at 10:00 am](#) | [Reply](#)

Is one of those programs to watch all the other programs?



5. *mogamboguru* | [July 1, 2013 at 12:19 pm](#) | [Reply](#)

@ Quatsch:

Skynet...

6. Pingback: [NSA Code Names Revealed « Document The Truth](#)
7. Pingback: [Edward Snowden | Anthony Mesojednik!](#)
8. Pingback: [Hiding the 215 Index from Defendants, Too | emptywheel](#)
9. Pingback: [Internetüberwachung: US-Spionagefirmen suchen XKeyscore-Fachleute | Kiss Canaries](#)
10. Pingback: [The Cocoon Blog XKeyscore, PRISM - What's Next? - The Cocoon Blog](#)
11. Pingback: [NSA's X-Keyscore One of Many Surveillance Programs Used On Americans](#)
12. Pingback: [NSA's X-Keyscore One of Many Surveillance Programs Used On Americans Dark Politricks](#)
13. Pingback: [XKEYSCORE: NSA TOOL COLLECTS 'NEARLY EVERYTHING A USER DOES ON THE INTERNET' | sreaves32](#)

<http://williamaarkin.wordpress.com/2012/03/13/nsa-code-names-revealed/>

Code Names II

Posted on [March 10, 2012](#) | [Leave a comment](#)

[Originally posted March 10, 2012, this is a list of Code Names that do not appear in the first edition of Code Names (2005). This is a work in progress and more are being added over time.]

Accordian: 1. NSA produced cryptographic device related to nuclear weapons command and control.
2. Nuclear weapons subcritical experiment conducted at the Nevada Test Site. Accordian will be followed up by Accordian Prime.

Added Force: Joint rehearsal exercise (JRX) 4-06, September 2006.

Advance Trec: Joint rehearsal exercise (JRX) 2-06, March 2006.

Barnstorm: Navy submarine emergency procedure.

Blue Action: Spanish led Proliferation Security Initiative (PSI) air/ground interdiction event in Spain, May 2005..

Blue Dart: Anti-terrorism threat-warning program designed to rapidly disseminate threat information in a simple, easy to understand format. All services, combatant commands, components, defense agencies and DOD activities are responsible for establishing procedures to disseminate Blue Dart warnings. A Blue Dart warning must contain all of the following elements:

- Specific TIMING of a threat: specific near-time frame within the next 72 hours.
- Specific TARGET of a threat: exact unit, activity or location
- Specific TYPE or MEANS of threat: explosive/VBIED, bombing, small arms/drive-by, sniper, assassination, etc.

Originates with Navy Anti-terrorism Alert Center (NAVATAC) reporting established in 1997.

Bow Warrior: Joint rehearsal exercise (JRX) 1-06, November 2005.

Brave Hero: Joint rehearsal exercise (JRX) 3-06, June 2006.

Bridge Troll: Joint rehearsal exercise (JRX) 4-05, September 2005, with NSA involvement.

Bright Star (additional information): Bright Star 03 was cancelled due to ongoing operations in Iraq. It is the most expensive exercise in the Middle East, using almost 20 percent of the total Air Force JCS exercise program funding, and many in the military believe that the cost greatly exceeds the training value. It has also been a “cash cow” for host Egypt. CENTCOM is now attempting to realign Bright Star to a global war on terrorism scenario or focus and is envisioning the next Bright Star to be centered around a lighter, more lethal exercise force package.

Brown Dog: Air Force Information Warfare Center project, 2004-2005.

Buggy Ride (additional information): STRATCOM plan related to emergency evacuation of bomber and tanker aircraft in a nuclear alert under OPLAN 8044. See also Dakota.

Cheetah: Air Force Information Warfare Center project, 2004-2005.

Cirrus Blue: Air Force Information Warfare Center TENCAP related project, 2004-2005.

Cirrus Orange: Air Force Information Warfare Center TENCAP related project, 2004-2005.

Code Silver: Air Force Surgeon General initiated tabletop exercise program centering on biological warfare defense medical consequence planning, preparation, and capabilities at the installation level, initiated in 2003.

Comet: Air Force Information Warfare Center project, 2004-2005.

Coronet Dance: Air Force deployment, 2004.

Creek Bridge: USAFE nuclear weapons related project, 2004.

Dakota (Dakota Force): Non-alert survival launch force consisting of bombers and tankers, generated during during a nuclear alert under OPLAN 8044. Dakota aircraft are sent airborne or moved to dispersal bases for protection. See also Buggy Ride.

Deep Sabre 05: Singapore led Proliferation Security Initiative (PSI) maritime/ground interdiction event in South China Sea, 15-18 August 2005.

Diablo Canyon: FEMA full-scale radiological response exercise, San Clemente, CA, 15 January 2005.

Diligent Endeavor: Defense Threat Reduction Agency (DTRA) sponsored interagency nuclear weapons accident FTX in preparation for Diligent Warrior 04, 17-18 February 2004, Washington, DC. See also Diligent Warrior.

Diligent Thunder: Army and Air Force related testing project, 2005.

Diligent Warrior 04: Office of Secretary of Defense directed, Defense Threat Reduction Agency (DTRA) sponsored and Air Force Space Command (AFSPC) supported national-level, nuclear weapons accident full-scale exercise (FSX), Malmstrom AFB, MT, 13-16 September 2002.

Dingo King: National level domestic US nuclear weapons and special operations exercise, 22-26 August 2005.

Distant Thunder: Defense Threat Reduction Agency (DTRA) internal WMD command post exercise (CPX) to examine agency response capabilities under CONPLAN 0100, 18 February 2004, Washington, DC.

Dynamic Quarantine: Air Force Information Warfare Center project, 2004-2005.

Eagle Scout: Air Force commercial satellite imagery program. The FY 2005 Appropriation report 108-622, dated 20 July 2004, included a Congressional add of \$1,500,000 to this program. No FY 2006 funding was requested.

Elder Prince: National level inter-service military working group related to operations security (OPSEC) and counter-terrorism.

Electric Eel: Air Force research and development project, 2004-2005.

Emerald (additional information): Counter-narcotics related intelligence program.

Exmoor: Air Force Information Warfare Center project, 2004-2005.

Falcon Nest: Air Force research and development project, 2004-2005.

Falcon Talon: Air Force research and development project, 2004-2005.

Firefly: NSA produced cryptographic device related to nuclear weapons command and control.

Fishwrap: Air Force research and development project, 2004-2005.

Gallant Journey 05: Classified intelligence or special operations exercise, March 2005, with DIA, NAS and CIA/OMA involvement.

Gauged Strength: DOD sponsored WMD-related interagency domestic response exercise, June 1998. The FBI participated in the “Gauged Strength” exercise in Norfolk, Va. and established interagency organizations, such as a Joint Operations Center and a Joint Information and Intelligence Support Element. State and local participation was limited by DOD classification requirements. Likely a JSOC exercise.

Global Lightning: STRATCOM nuclear weapons exercise that rehearses operations during a tran-/post-attack nuclear environment, including reconstitution, redirection and targeting of STRATCOM forces, 19-28 October 2005.

Global Storm: STRATCOM nuclear weapons exercise, 8-12 August 2005.

Global Thunder 06: STRATCOM nuclear weapons exercise, 11-15 April 2005.

Grace (Project Grace): Foreign acquired MiG-29 live fire training and testing project.

Gridlock: National Geospatial Intelligence Agency (NGA)-led Advanced Concept Technology Demonstration (ACTD) designed to provide an enhanced capability for kill-chain compression in time sensitive targeting by reducing the timeline needed to produce highly accurate target coordinates using imagery from sensors.

Gypsy Charlie: B-1 test series associated with satellite guided weapon employment in a degraded GPS environment.

Ibis Dawn II: Foreign material exploitation project, 2004-2005.

Ibis Munin: Foreign material exploitation project, 2004-2005.

Keesee: Cryptographic key generation (KOK-13) device or system, anticipated for funding in the FY 2007 budget.

Last Mile: STRATCOM command and control network upgrades.

Layman Teacher 05: Classified intelligence or special operations exercise, March 2005, with DIA and NRO involvement.

Limit Mustang: Navy Concept of Operations for OPLAN 5077 Weapons System. (added April 9, 2012)

Loyal Guardian: OPLAN published in July 2001 dealing with Army force protection. (added April 9, 2012).

Medley: NSA produced cryptographic device related to nuclear weapons command and control.

Minerva: Joint Information Operations Center (JIOC) information operations search engine that provides an indexed format of available intelligence related to information warfare (foreign adversary influence networks, decision making processes, information infrastructure and cultural considerations for information operations planning). Minerva provides hotlinks to IO-related information available on both the JWICS and the SIPRNET.

Neptune Shield: Coast Guard Operations Order (ORDER).

NINFA 2005: Portuguese led Proliferation Security Initiative (PSI) maritime/ground interdiction event in Eastern Mediterranean, 8-15 Apr 2005.

Noble Eagle (Operation Noble Eagle): Overall name for domestic military operations in response to 9/11, including surveillance and interceptor flights by NORAD and coastal patrols by the Coast Guard. Noble Eagle is the domestic counterpart to Operation Enduring Freedom, which is officially the overall name for the (overseas) war on terrorism.

North Star (Project North Star): Organization that respond to the needs of, and requests from, the Joint Coordination Group (JCG), a border (U.S. and Canada) law enforcement coalition. The primary emphasis is on counterdrug activities along the U.S. and Canadian border.

Olsina: U.S.-German-Czech Republic NATO PfP peacekeeping training exercise, Boletice training area in the Czech Republic, 12-20 September 1995.

Omaha (Task Force Omaha): Informal name for Task Force 626 (formerly TF 121) special operations activity in Iraq, 2004.

Outlaw Bandit: Navy ship board passive countermeasure system.

PatentHammer: National tactical integration SIGINT project (Project 168, JMIP, FY 2006 budget)

Pegasus: Army intelligence Trojan Classic SIGINT system.

Phantom Point: Ft. Hood, Texas deployment procedures.

Phoenix (additional information): AMC transport assistance to Middle East operations in 2003-2004.

- **Phoenix Alkali** (additional information): FY 2004 exercise
- **Phoenix Birch**
- **Phoenix Calvin**
- **Phoenix Court**
- **Phoenix Maple**
- **Phoenix Master**
- **Phoenix Nitrate**
- **Phoenix Poplar**
- **Phoenix Rack**
- **Phoenix Shell**
- **Phoenix Sphinx**

Phoenix Cedar: Contingency deployments, presumably to Jordan, beginning in December 1998 in support of Desert Fox.

Pontiff: Foreign materiel exploitation project, 2004-2005.

Power Geyser: Presidential-related contingency plan for continuity of government operations during an emergency, specifically a weapons of mass destruction incident, and thought to be involving the Joint Special Operations Command (JSOC) under JCS CONPLAN 0300.

Pluto New Horizons: Nuclear weapons accident or incident response related mission slated to be implemented in January 2006.

Project 9GH (additional information): As of 7 January 2005, this Project Code was revised and is no longer in support of OEF.

Project 9GL: EUCOM counter-terrorism operations in a classified country. See also Project 9GI/9GK

Quick Saber: OPLAN 5027 (Korean peninsula) response option (RO).

Saltpit: Informal name (aka “The Pit”) for a military interrogation facility for terrorism high value targets, presumably in Afghanistan.

Scorpion: Joint US-Jordanian CIA/DOD detention facility, located in Jordan.

Sensor Chief: Air Force intelligence foreign material exploitation support, 2004-2005.

Sensor Ego: Former Air Force intelligence foreign material exploitation support, 2004-2005.

Sensor Shelby: Air Force intelligence foreign material exploitation support, 2004-2005.

Sensor Robin: Air Force intelligence foreign material exploitation support, 2004-2005.

Ship Rider: Procedure relating to the one-time or short duration installation of a communications security (COMSEC) cryptographic device during an operation or training exercise with a foreign government entity that does not have secure communications with the U.S.

Silent Watch: Navy submarine periscope mounted ESM upgrade, part of the Integrated Submarine Imaging System (ISIS), installed aboard attack submarines (SSNs) and new cruise missile submarines (SSGNs).

Silver Fox: Small (22 lbs.) tactical UAV, originally deployed with four hour endurance, an off-the-shelf design able to carry infrared, black and white and color cameras and be controlled from a “pocket PC” like device. Used for surveillance relating to convoy escort and Navy special operations. Through 2004, 18 Silver Foxes had been deployed to CENTCOM.

Site 6250: CJTF-180/CTF-82 base in Afghanistan or an adjoining country.

Site 6251: Joint Special Operations Task Force (JSOTF) base in the CENTCOM region.

Steadfast Response: FEMA sponsored Region V interagency continuity of operations (COOP) exercise, 5 February 2004, Chicago, IL.

Stocktake: U.S.-U.K. nuclear weapons related technical exchange program administered under the authority of the Joint Atomic Information Exchange Group (JAIEG).

Swift Deflector: Ft. Carson, CO related OPLAN. (added April 9, 2012)

Talon (Threat and Local Observation Notice): Formated suspicious activity reporting done in accordance with Deputy SECDEF directive issued 2 May 2003 via the Joint Protection Enterprise Network (JPEN).

Tasmanian Devil?: NSA-related global war on terrorism related special access program

Venom x?: Office of the Secretary of Defense global war on terrorism related special access program?

Vigilant Warrior: OPLAN 5027 (Korean peninsula) response option.

Vital Archer 05: Chairman of the Joint Chiefs of Staff directed NORTHCOM and presumably Joint Special Operations Command (JSOC) classified command post exercise (CPX) focused on sensitive special operations and homeland defense in the US. The exercise employs the NORTHCOM battle staff and Compartmented Planning and Operations Cell (CPOC) focused on implementation of sensitive CONPLANS.

Wasatch Rings: Multi-agency WMD field training domestic exercise cosponsored by the FBI and the Utah Olympic Public Safety Command in preparation for the 2002 Olympic Winter Games in Salt Lake City, Utah.

Watchkeeper: Air Force ultra-wideband (UWB) unattended ground sensor perimeter defense demonstration.

White Angel II: B-2 bomber testing and evaluation program, complete 2003-2004.

<http://williamaarkin.wordpress.com/2012/03/10/code-names-ii/>

NSA Codenamed Programs 4 August 2013

Thanks to [@spyblog](#)

Via DailyDot:

<http://www.dailydot.com/news/nsa-fairview-slides-brazil-spying/>

http://www.youtube.com/watch?feature=player_embedded&v=kOAv7zbJkCk



Seen on FAIRVIEW
(2/15/2012 - 3/11/2012)

Top 20 Pakistani domains (-pk)

	Avg (Kbps)
express.com.pk	917
pemra.gov.pk	812
cyber.net.pk	710
brain.net.pk	425
edenhousing.com.pk	424
ass.edu.pk	289
pec.org.pk	193
super.net.pk	166
ntu.edu.pk	160
icel.com.pk	149
teekrete.com.pk	141
ra.edu.pk	136
il.net.pk	123
comsats.net.pk	121
ifa.edu.pk	
comsats.net.pk	
organt.com.pk	
s.com.pk	
il.com.pk	
sts.net	

NSA Hawaii in USB Made in China Flickr Photos in Link Under This Video

La CIA y la NSA espionaron mediante satélites desde Brasil & Slides



on Managers
W Craig Hicks
BREW Stu Bathurst
Y "DL BLARNEY_CM"
"DL OAKSTAR_OPS"
CELOT Stu Bathurst

nagement
p_mm"

te Portfolio" Wiki

NSA Hawaii in USB Made in China Flickr Photos in Link Under This Video



4:07 / 8:14



YouTube



La CIA y la NSA espionaron mediante satélites desde Brasil & Slides



NSA Codenames:

DL BLARNEY_CM and DL OAKSTAR_OPS. STORMBREW and FAIRVIEW.

Possibly HOMEBREW and OCELOT.

Previously: PRISM, XKEYSTORE.

More NSA codenames invited: cryptome[ar]earthlink.net

<http://cryptome.org/2013/08/nsa-codenames.htm>

NSA X-Keyscore Member of Cyberespionage Family 3 August 2013

Related: X-Keyscore Server Sites:

<http://cryptome.org/2013/08/nsa-x-keyscore-servers.htm>

It would be logical for NSA to use US embassies abroad as a family of outposts for X-Keyscore harvesting local communications. Embassies have always been used for full-spectrum espionage in all its guises and disguises, military, political, economic, social, so adding cyber was inevitable. The embassies have multiple networks for communications from minimal to highest levels of security. To conduct cyber-espionage would be a seamless extension of existing technology.

Further revelations of Snowden's documents could describe how this is done with personnel, networks and data-server architecture, not only by PRISM and X-Keyscore. Staff of these spy systems may be seen as HUMINT androids safely bunkered for intimately wielding their remote-spying apparatus in concert with remote-commanding officials and killing-machine operators with whom they work to surveil, analyze, target and execute.

LinkedIn and other social media, job recruiters, conference sponsors, have since 9/11 rushed to fill burgeoning "intel analyst" positions, many military and official spy-trained, now seeking greater pay and perks on the cyberespionage market. These "intel analyst" job seekers and holders (happily "endorsing" each other) parade the codenames of espionage tools and programs they have mastered, XKeyscore only one among these compiled by A's quick overnight search of LinkedIn¹:

AGILEVIEW, AGILITY, AIRGAP/COZEN, AIGHANDLER, ANCHORY/MAUI, ARCANAPUP, ARTEMIS, ASSOCIATION, AUTOSOURCE, BEAMER, BELLVIEW, BLACKPEARL, CADENCE/GAMUT, CHALKFUN, CINEPLEX, CLOUD, COASTLINE, COMMONVIEW, CONTRAOCTAVE, CONVERGENCE, COURIERSKILL, CREEK, CREST, CROSSBONES, CPE, CULTWEAVE, CYBERTRANS, DISHFIRE, DOUBLEARROW, DRAGONFLY, Enhanced WEALTHYCLUSTER (EWC), ETHEREAL (maybe opensource network analysis?), FASCIA, FASTSCOPE, FOREMAN, GAMUT/UTT, GISTQUEUE, GJALLER, GLAVE, GLOBALREACH, GOLDMINER, GOLDPOINT, GOSSAMER, GROWLER, HERCULES (CIA terror database) HIGHTIDE/SKYWRITER, HOMEBASE, INFOSHARE, JOLLYROGER, KINGFISH, LIQUIDFIRE, MAINWAY, MARINA, MASTERLINK, MASTERSHAKE, MAUI/ANCHORY, MESSIAH, METTLESOME, NEWHORIZONS, NIGHTSURF, NORMALRUN/CHEWSTICK/FALLENORACLE, NUCLEON, OCTAVE,

PATHMASTER/MAILORDER, PINWALE, PANOPTICON, PRESENTER, PROTON, RAVENWING, RENOIR, ROADBED, SCORPIOFORE/CPE, SHARKFINN, SKOPE, SKYWRITER, SNAPE, SPOTBEAM, STINGRAY; SURREY, TAPERLAY, TAROTCARD, TEMPTRESS, TRACFIN, TRAILMAPPER, TREASUREMAP, TRICKLER, TUNINGFORK/SEEKER, TURMOIL, TUSKATTIRE, TWISTEDPATH, UIS/PINWALE, UTT, WEALTHYCLUSTER, WIRESHARK (opensource network analysis?) WITCHHUNT, XKEYSCORE, YELLOWSTONE/SPLITGLASS

These manifold programs imply that US embassies operating X-Keystone networks and data-servers to tap into global nations' telecommunications hubs for cyber spying would require no more than doing what US spy agencies do inside the USA: overtly and covertly arranging access through domestic official and commercial spying and law enforcement agencies, corporations, telecommunications networks, financial institutions, consultants, cyber mercenaries, organized criminal organizations, opportunistic patriots, informants, educational institutions, all the ancient cooperators, and now variable-hatted hackers, cryptographers, anonymizers, freedom of information fighters, civil liberties fronts, political organizations, lobbyists, press officers, governmental office-holders, donors and funding organizations.

Note: 3 August 2013

A clarifies source of codenames:

The list of codenames aren't siphoned off LinkedIn but compiled over time to help look for interesting intelligence professionals and connections — a lot from William Arkin's excellent work:

<http://williamaarkin.wordpress.com/2012/03/13/nsa-code-names-revealed/>

After the X-Keyscore article in Guardian I began looking for CV's on LinkedIn referring X-Keyscore and the other systems from the list. As you must have found out by now there are lots of references to these systems. [Cryptome: Search also for "intel analyst."]

Notably, as you can see, ECHELON, ECHELON II, MAGISTRAND etc are missing. I believe these are the "Windows 3.1" of SIGINT software. Obsolete. Evolved.

<http://cryptome.org/2013/08/nsa-x-keystone-family.htm>