cybersecurity centre

GCHQ Academic Centre of Excellence EPSRC

UNIVERSITY OF Southampton
Electronics and Computer Science

The dark side of the moon

Denis A Nicole

2013-06-17

CEPBA: Service

Manuf.	Model	Processor	Memory Disc	Peak Performance	Service
IBM	SP3+p360	128 Power3 + 36 Power4	64+18 GB 1,8 TB	336 Gflop/s	10/01 12/02
Compaq	Alpha Server GS-160	16 Alpha 21264	8 GB 108 GB	23,3 Gflop/s	9/00
Parsytec	CCi-8D	16 Pentium II	1 GB 30 GB	3,2 Gflop/s	4/98
Silicon Graphics	Origin 2000	64 MIPS R10000	8 GB 360 GB	25 Gflop/s	1/97
Digital	Alpha Server 8400	12 Alpha 21164	2 GB 32 GB	10,5 Gflop/s	12/96
Silicon Graphics	Power Challenge	12+12 R8000/R10000	4 GB 50 GB		7/96 - 7/97
Thinking Machine	CM-2	2048 1 bit	256 MB	640 Mflops	4/92 - 2/98
Convex	C3480	8	1 GB 16 GB	0,4 Gflop/s	10/91 - 1/98
Parsys	SN 1000	32 T800	128 MB 2 GB	64 Mflops	5/90 - 5/95

cybersecurity centre

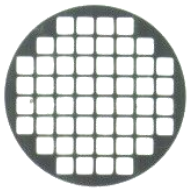
GCHQ Academic Centre of Excellence EPSRC

UNIVERSITY OF Southampton
Electronics and Computer Science

ESPRIT
P1085

Royal Signals and
Radar Establishment
Malvern

The University
of Southampton

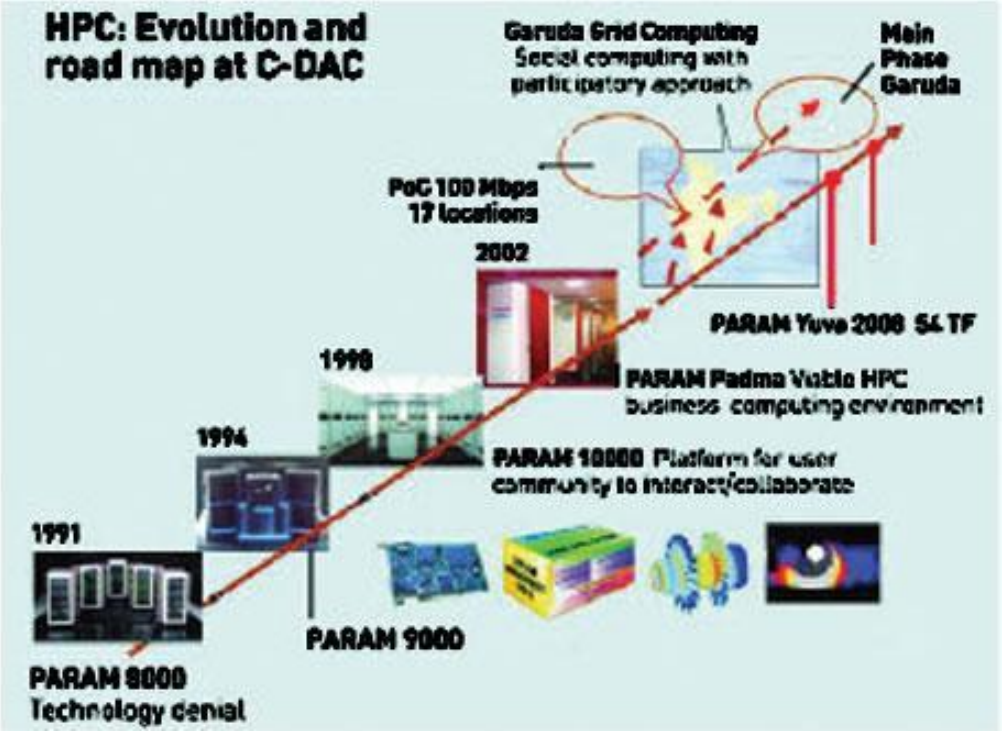


inmos

INMOS is a member of the SGS-THOMSON Microelectronics Group

CDAC

After being denied Cray supercomputers, Indian scientists developed their own, which proved the world that we could beat them at their own game, and at a fraction of the cost. The final result of the effort was the PARAM 8000 which was installed in 1991.



http://www.pcquest.com/pcquest/news/177688/products-made-india

The architect of PARAM 8000, India's first supercomputer…

Vijay Pandurang Bhatkar, one of India's most acclaimed scientists, is best known as the architect of India's first supercomputer—PARAM 8000.

http://www.livemint.com/Industry/jmNVLeBoYXUbJzFJBTdNLK/Yesterdays-supercomputers-are-todays-laptops-Bhatkar.html?utm_medium=referral&utm_source=t.co

C-DAC furthering ties with ICAD, Moscow: From PARAM 8000 to PARAM 10000

The C-DAC and ICAD association:

C-DAC's decade old association with the Institute of Computer Aided Design (ICAD), Moscow of the Russian Academy of Sciences began in 1991-92 when the Department of Science &. Technology, Government of India, brought it under the ambit of an Indo-Russian Scientific Programme, popularly called Integrated long Team Programme (ILTP) of collaboration in science and technology between India and Russia.

C-DAC, has over the years established a close association with ICAD owing to the Indo-Russian collaboration in Science and Technology. ICAD, an important constituent of the Russian Academy of Sciences, has expertise in the fields of Computational Fluid Dynamics, Finite Element Method, Mathematical Modeling and Scientific Visualization. C-DAC's experience in designing and installing High Performance Computers and in diverse scientific and business computing applications has ensured a good synergy between the two organizations for an effective and mutually beneficial collaboration.

The PARAM series for ICAD

With the areas identified for research collaborations, a parallel computing system, PARAM 8000 was first installed at ICAD, Moscow in 1991-92 based on the then very powerful Transputer Processor Chip. The Software dealing with Fluid Mechanics and Structural Analysis were operated and parallelized on the system. The efforts were further complemented by C-DAC by optimizing the system software tools and graphics on the installation of PARAM 8000 system at ICAD containing 128 nodes in all.

http://www.cdac.in/html/about/success/moscow.aspx

Shakti-1: 1998-05-11

- Claimed Indian underground thermonuclear test.
- Rumoured not to have worked too well

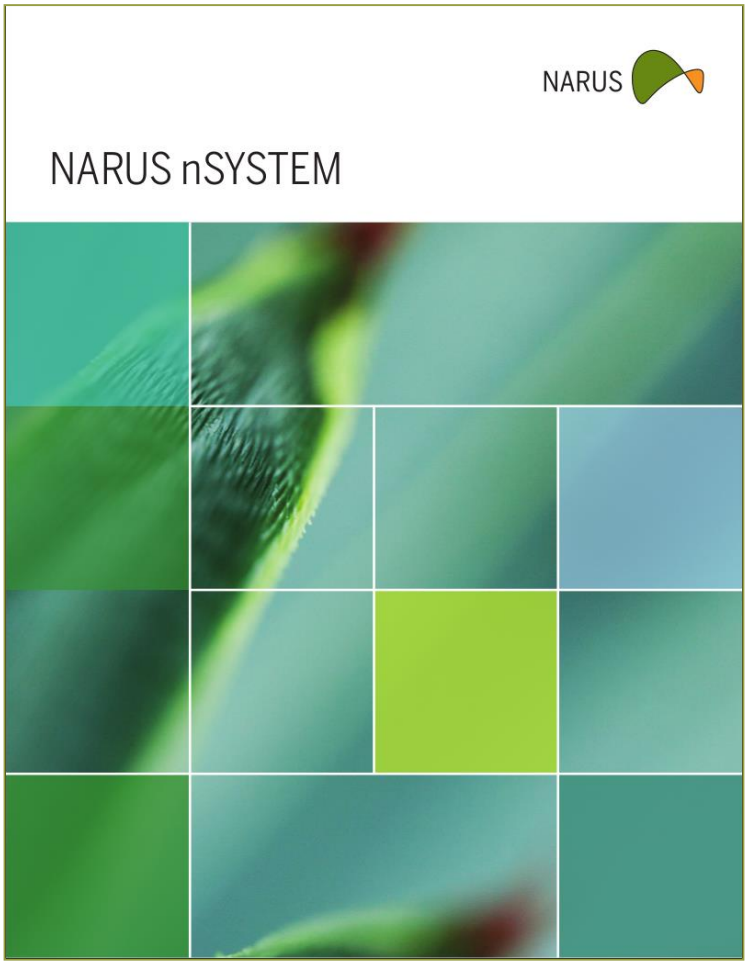
http://www.fas.org/nuke/guide/india/nuke/shakti-pix1.htm & CNN

Not Pink Floyd after all

But a "Local Hero"

http://www.adam-hart-davis.org
http://gallery.hd.org/_exhibits/natural-science/prism-and-refraction-of-light-into-rainbow-2-AJHD.jpg

Or maybe this



NARUS nSYSTEM

CONSTANTLY DEEPENING INSIGHT FOR A NEW LEVEL OF CONTROL

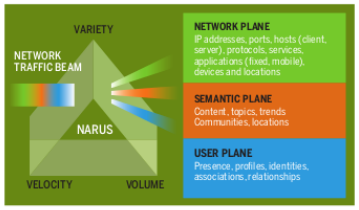
As the Internet grows more complex and dynamic, information security organizations are inundated with enormous volumes of data, users connected at tremendous speeds, and ever-changing dynamics with new devices and applications entering the network all the time.

The only way for organizations to stay ahead is to identify and analyze every piece of data that flows across the network and to understand it in context of everything else that is happening — a job that is impossible for any human or team of humans to undertake. The future of cybersecurity requires a new approach: drawing from the richly layered semantic web to enable machine-to-machine analysis and automated machine learning to bring deep new meaning to network activity and user behavior.

BRINGING CYBER 3.0 TO CYBERSECURITY

Narus nSystem is a portfolio of analytics that apply automated machine-based algorithms to process 100% of network packets to discover, analyze, and understand every interaction on a network. nSystem develops rich profiles of every interaction to provide deeper context for faster, more accurate awareness. Analysts can hone in immediately on critical issues instead of wasting their time on unimportant conditions or manually trying to piece together data to get the big picture.

This context is possible because of the way nSystem separates the data it processes into three different "planes," which offer distinct sets of dimensions critical to developing a complete understanding of network activity and user behavior. The network plane consists of information about devices (brand, type and operating system) and hosts (client, server, applications, protocols and services).



The semantic plane consists of content, topics, trends, communities and locations. The user plane consists of presence, profiles, identities, associations and relationships about users. The nSystem analytics automate the understanding of each of these planes, identify the context of the interactions, and aggregate data across the planes to deliver incisive intelligence.

NETWORK PLANE ANALYTICS

These analytics provide solutions for some of the most common challenges network operators and security analysts face:

- **Visibility:** Situational awareness and visability across every dimension, with volumetric analysis of traffic patterns and targeted packet capture for in-depth analysis
- **Control:** Alignment of every aspect of network usage with enterprise goals
- **Context:** Identification of hidden relationships and connectivity patterns between network elements and end users

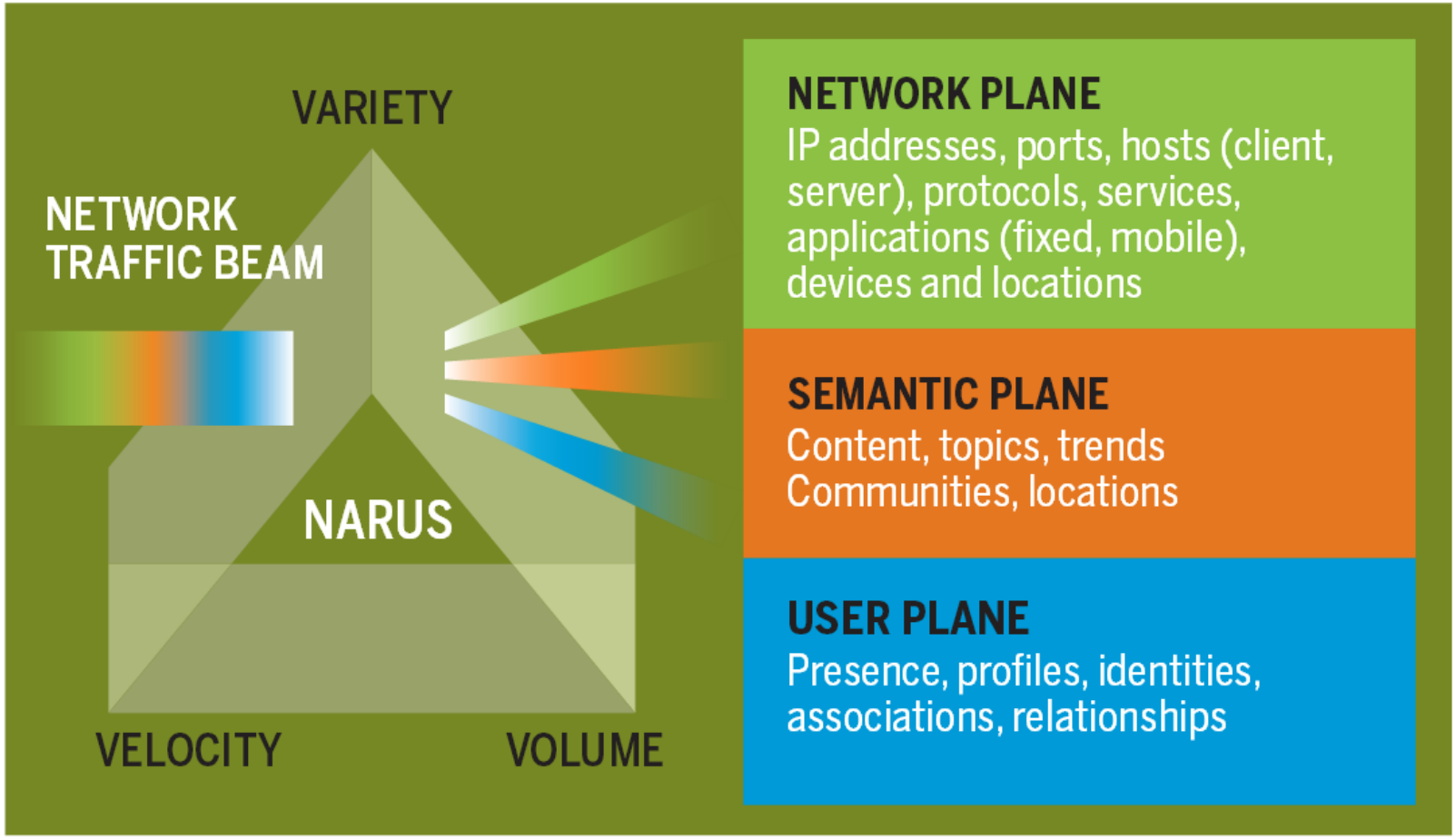
SEMANTIC PLANE ANALYTICS

Semantic analytics allow users to perform sentiment analysis, identify relationships between users through the content they share or network elements they share. These analytics provide:

- **Visibility:** Situational awareness about content, communities, locations, and demographics
- **Context:** Insight into explicit and implicit relationships, association of content with users, their locations and their roles

http://narus.com/images/pdf/Narus_nSYSTEM_brochure.pdf

Now part of Boeing



Presumably NARUS processes this bit

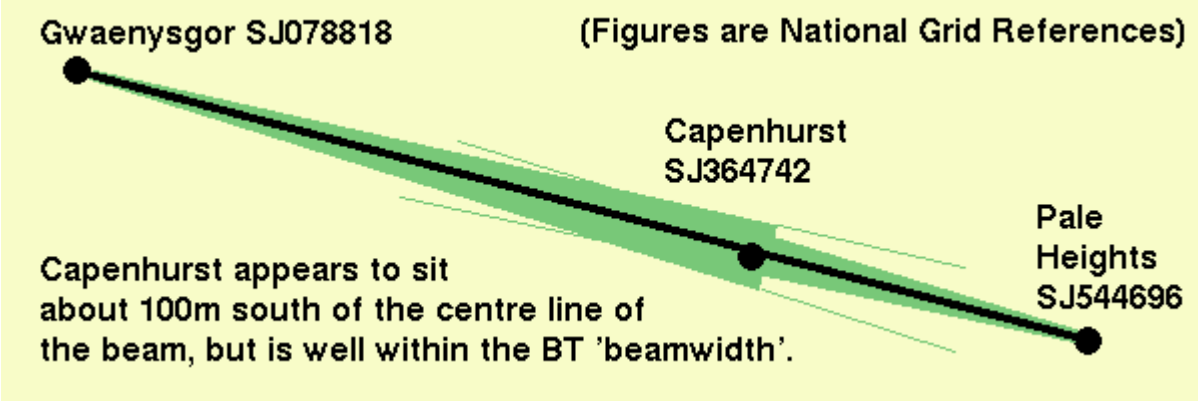
And the RSA keys?

SIGINT people really *hate* to ask

This is the secret radio tower which the government used to intercept thousands of trunk phone lines running through Britain to the Republic of Ireland.

The structure was located on the boundary of the URENCO uranium enrichment plant at Capenhurst in Cheshire

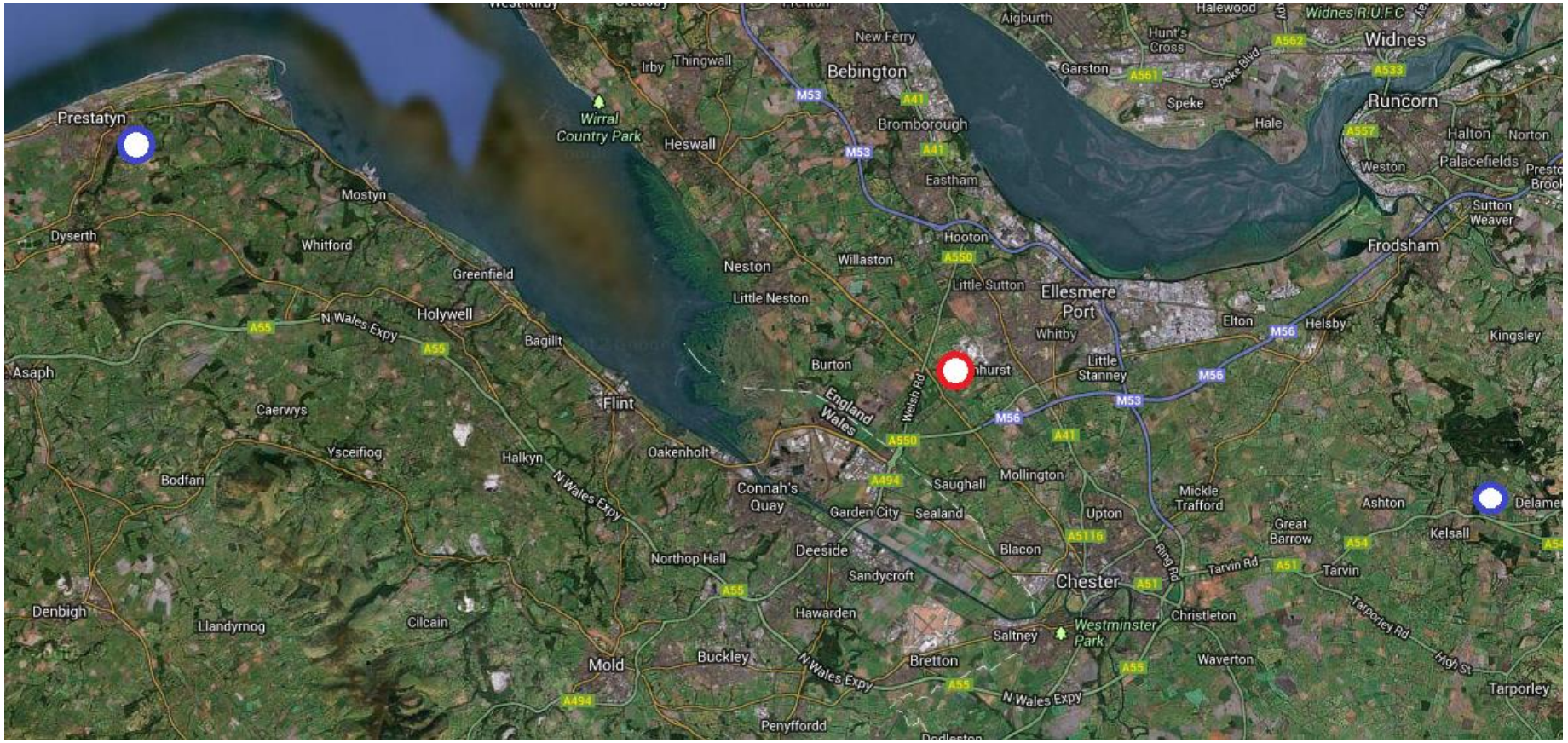
http://www.lamont.me.uk/capenhurst/



It is also located right on the microwave line-of-sight between two British Telecom radio towers at Gwaenysgor in North Wales and Pale Heights in Cheshire.

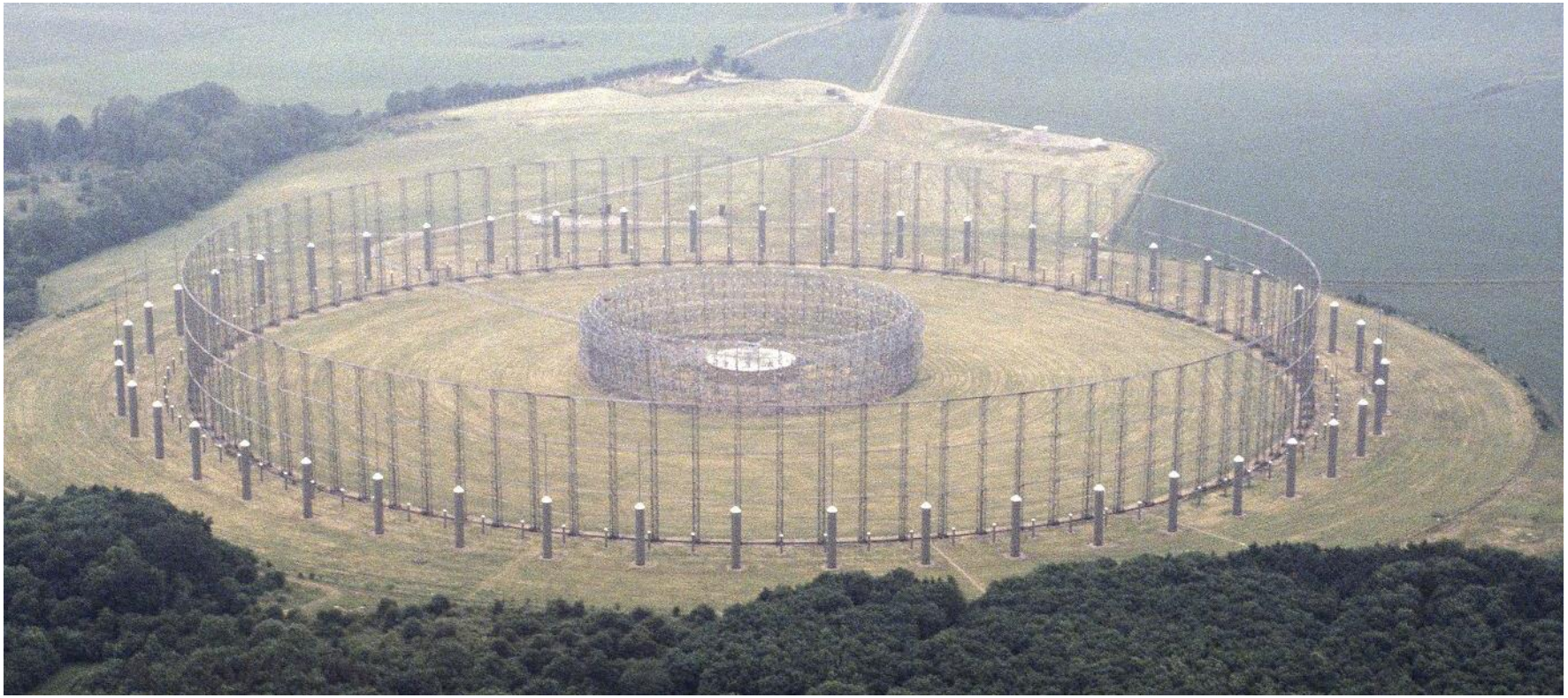
The BT towers form part of a chain carrying thousands of phone lines from England, along the north Wales coast to Anglesey, then across the Irish Sea to Dublin. Four microwave channels ran in each direction, each capable of carrying one TV channel or roughly 1,000 phone calls, using frequencies around 6.5 GHz.

They could have just asked BT



Radomes don't just keep the pigeons out

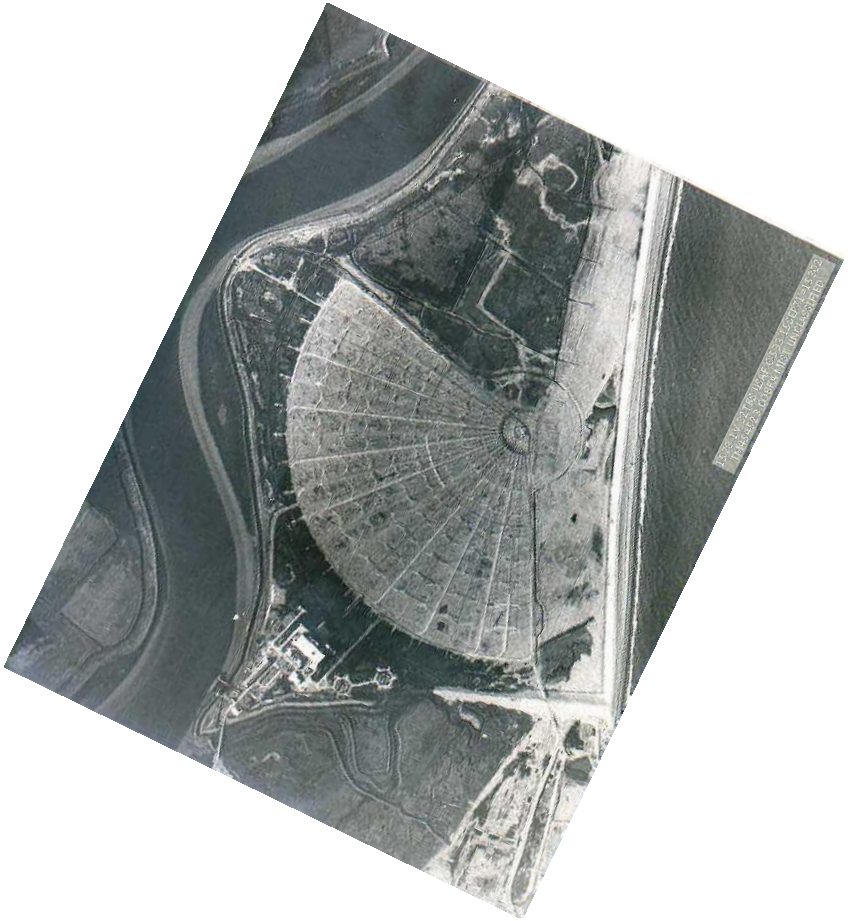
And where was the AN/FLR-9 looking?



To be fair, there are also technical reasons that a Wullenweber is *circularly disposed*.

http://www.ftva.org/heritage/anflr9/RAFChicksands.jpg
http://www.premium-rx.org/ref/wullenweber.pdf

It's obvious where this was pointing...



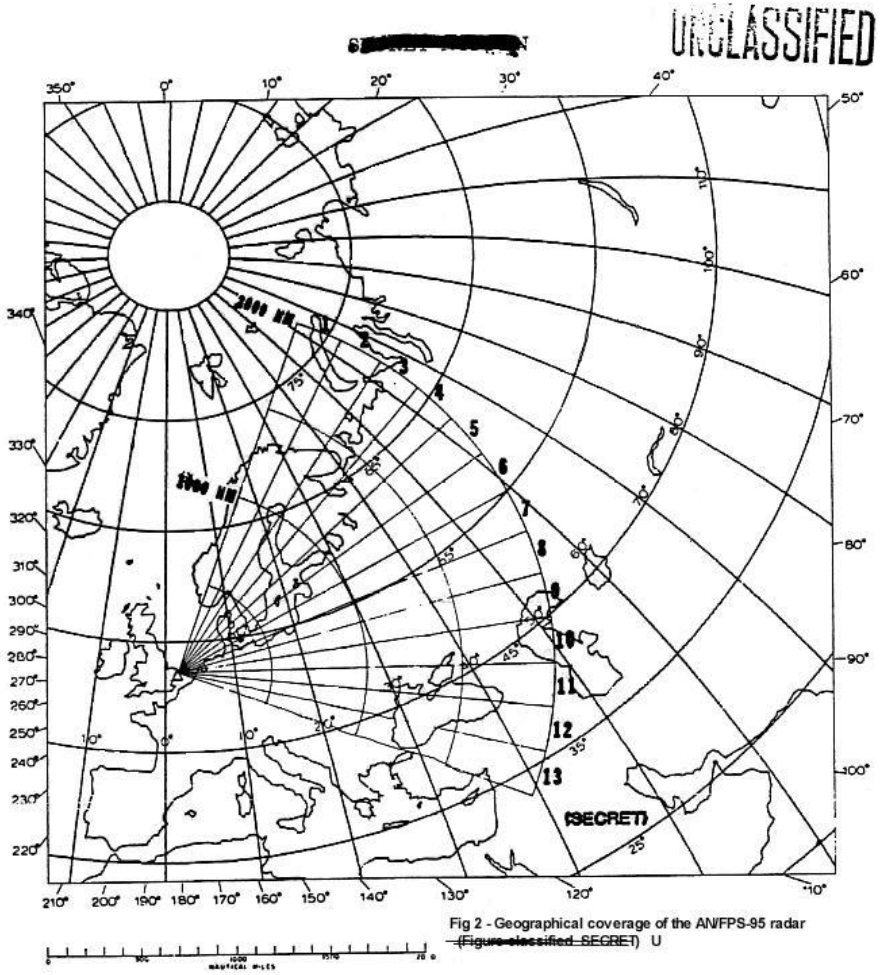


Fig 2 - Geographical coverage of the AN/FPS-95 radar (Figure classified SECRET) U

...and it didn't work

The Enigma of the AN/FPS–95 OTH Radar (U)

E. N. Fowle, E. L. Key, R. I. Millar, and R. H. Sear

The MITRE Corporation, Bedford, Mass.

(Received May 22, 1979)

(U)

(S) Cobra Mist, the AN/FPS–95 over-the-horizon (OTH) radar built on the English North Sea Coast in the late 1960's to overlook air and missile activity in Eastern Europe and the western areas of the USSR, was the most powerful and sophisticated radar of its kind up to that time. The design, which emulated Naval Research Laboratory's Madre over-the-horizon radar, incorporated rather coarse spatial resolution and relied upon ultralinear, wide dynamic range components and complex signal processing in attempting to achieve the extreme subclutter visibility (scv) of 80 to 90 dB needed to separate target returns from the strong ground clutter—a goal well beyond the 60-odd decibel subclutter visibility previously achieved. The detection performance of the radar was spoiled, however, because the actual subclutter visibility achieved was only 60 to 70 dB, the limitation being due to a noise with approximately flat amplitude-versus-Doppler frequency, which appeared in all range bins containing ground clutter and aircraft returns. Experiments performed at the site failed to uncover the source of the noise, either in the equipment or in the propagation medium. Other experimental results imply that the noise was associated with returns from land areas and not from sea surfaces; the possibility of electronic countermeasures was not ruled out. Because the source of the noise was not located and corrected, the radar program was terminated in June 1973 and the equipment removed from the site. The cause of the noise is unknown to this day.

http://www.dod.mil/pubs/foi/Science_and_Technology/Other/480.pdf

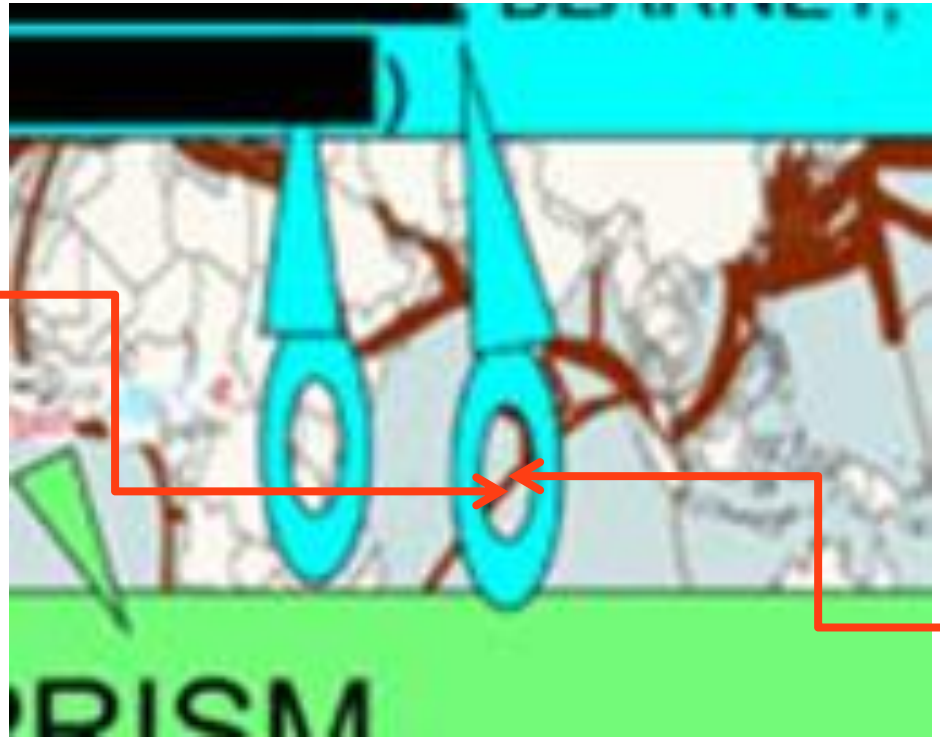
Back to the topic. I'm no lawyer, but...

- I don't think *international* communications are protected from inspection.
- So NSA are probably within their rights to *deep packet inspect* at the terminations of international cables/sat-links.
- But, it seems, that is not what they did:

> AT&T provided National Security Agency eavesdroppers with full access to its customers' phone calls, and shunted its customers' internet traffic to data-mining equipment installed in a secret room in its San Francisco switching centre, according to a former AT&T worker cooperating in the Electronic Frontier Foundation's lawsuit against the company.
>
> The split circuits included traffic from peering links connecting to other internet backbone providers, meaning that AT&T was also diverting traffic routed from its network to or from other domestic and international providers, according to Klein's statement.
>
> The secret room also included data-mining equipment called a Narus STA 6400, "known to be used particularly by government intelligence agencies because of its ability to sift through large amounts of data looking for pre-programmed targets," according to Klein's statement.
>
> http://www.wired.com/science/discoveries/news/2006/04/70619

What's this here?

Diego Garcia



France Telecom,
BT, AT&T etc.
SAFE fibre
http://www.safe-sat3.co.za/

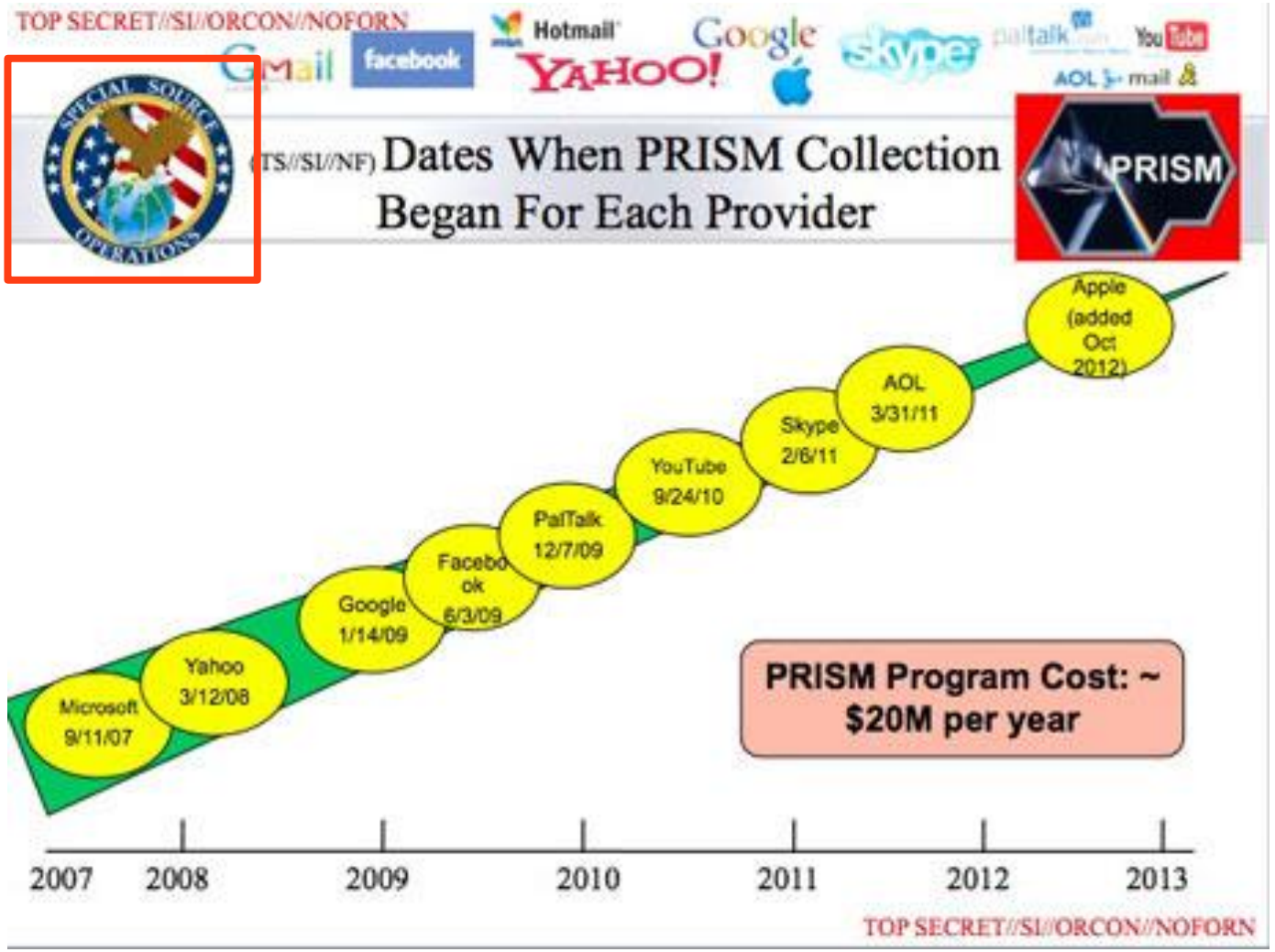
USS Jimmy Carter

This boat is different from its sister boats, the USS Seawolf, and the USS Connecticut, in that it has an additional section inserted into the hull for special operations.

Commissioned 2005-02-19.

http://www.fxmodels.com/SSN23.shtml

Leaking is dangerous



People will say anything on the Web

[redacted]

DEPUTY DIRECTOR
INFORMATION ASSURANCE DIRECTORATE, NATIONAL SECURITY AGENCY/CENTRAL SECURITY SERVICE, FORT MEADE, MD USA

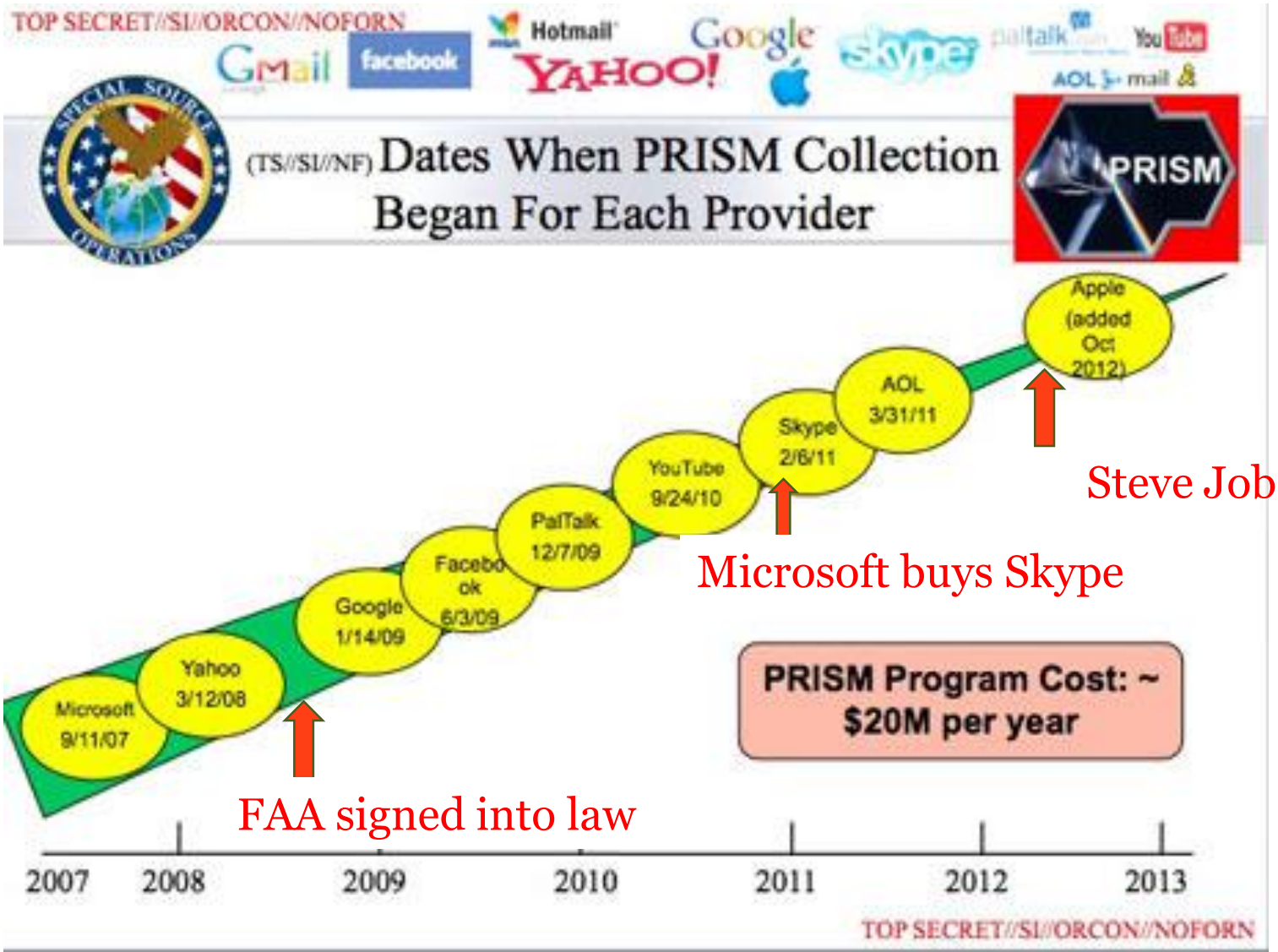
[redacted] is the Deputy Director of the Information Assurance Directorate (IAD) at the National Security Agency. On behalf of the Director, NSA, the IAD is the focal point for cryptography, telecommunications system security and information systems security for all national security systems. Specific responsibilities include research and development activities to generate IA techniques and solutions, ensuring the availability of IA products and solutions and understanding the threat to and vulnerability of national security systems.

Before coming to IAD, [redacted] served as the SID Associate Deputy Director for Counterterrorism (ADD/CT). In this position, he led NSA's counterterrorism efforts. His charge was to optimize the SIGINT system, ensuring maximum effectiveness against the CT mission, utilizing all NSA capabilities, integrating with the other US Government entities and global SIGINT partners.

Early in his career, [redacted] completed the Engineering and Physical Science intern program rotating through SIGINT and INFOSEC offices. He spent significant time developing collection equipment and supporting field efforts. For five years, he was the chief of the Selection Systems Branch where he led in-house and contractor development of collection technology. Subsequently, he held a leadership role as the Technical Director in NSA's Special Source Operations activities involving some of NSA's most important accesses. Starting in 2003, [redacted] served as an Iraq Issue Manager establishing priorities and providing guidance for all elements engaged in SIGINT planning, preparation, and execution for the operational campaign. Most recently, in 2005, [redacted] was the Technical Director for the NSA Commercial Solution Center's Commercial Partnerships Office, working strategic relationships with industry for technical solutions in support of support NSA missions. He served as the technical director to the Associate Deputy Director for Counterterrorism before taking on the role himself in August 2006.

[redacted] graduated from [redacted] in 1989 with a Bachelors Degree in Electrical and Computer Engineering and received a Masters Degree in Electrical Engineering from [redacted] in 1993. [redacted] resides in [redacted], Maryland with his wife, [redacted], son [redacted] and [redacted]. He enjoys sports including basketball and volleyball and is interested in coin collecting, computers and genealogy.

Dates


TOP SECRET//SI//ORCON//NOFORN
Gmail facebook Hotmail YAHOO! Google skype paltalk YouTube AOL mail
(TS//SI//NF) Dates When PRISM Collection Began For Each Provider
PRISM
Microsoft 9/11/07
Yahoo 3/12/08
Google 1/14/09
Facebook 6/3/09
PalTalk 12/7/09
YouTube 9/24/10
Skype 2/6/11
AOL 3/31/11
Apple (added Oct 2012)
FAA signed into law
Microsoft buys Skype
Steve Jobs dies
PRISM Program Cost: ~ $20M per year
2007 2008 2009 2010 2011 2012 2013
TOP SECRET//SI//ORCON//NOFORN

Microsoft has "form": NT4 SP5 `_NSAKEY` 1999

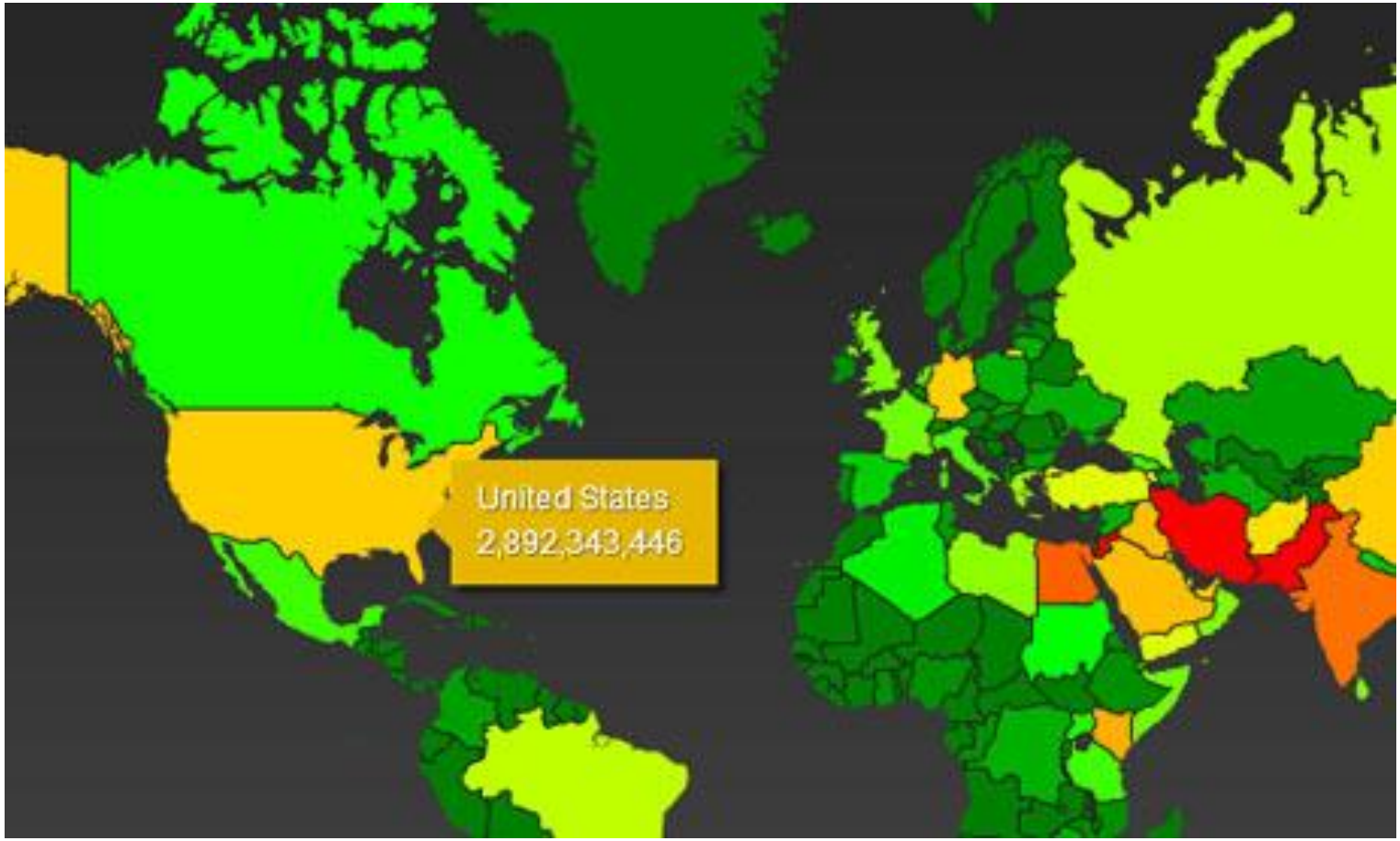
Andrew Fernandes discovered a back door for the NSA in every copy of Win95/98/NT4 and Windows2000.

In this service release of software from Microsoft, the company crucially forgot to remove the symbolic information identifying the security components. It turns out that there are really two keys used by Windows; the first belongs to Microsoft, and it allows them to securely load CryptoAPI services; the second belongs to the NSA. That means that the NSA can also securely load CryptoAPI services on your machine, and without your authorization. The result is that it is tremendously easier for the NSA to load unauthorized security services on all copies of Microsoft Windows, and once these security services are loaded, they can effectively compromise your entire operating system.

It turns out that there is a flaw in the way the function is implemented. Because of this, users can easily eliminate or replace the NSA key from the operating system without modifying any of Microsoft's original components. Since the NSA key is easily replaced, it means that non-US companies are free to install "strong" crypto services into Windows, without Microsoft's or the NSA's approval.

http://cryptome.org/

Why do this?



Boundless Informant

- Reads like a Web Technology MSc Project

8) What is the technical architecture for the tool?

- Click here for a graphical view of the tool's architecture
- (U//FOUO) DNI metadata (ASDF), DNR metadata (FASCIA) delivered to Hadoop Distributed File System (HDFS) on GM-PLACE
- (U//FOUO) Use Java MapReduce job to transform/filter and enrich FASCIA/ASDF data with business logic to assign organization rules to data
- (U//FOUO) Bulk import of DNI/DNR data (serialized Google Protobuf objects) into Cloudbase (enabled by custom aggregators)
- (U//FOUO) Use Java web app (hosted via Tomcat) on MachineShop (formerly TurkeyTower) to query Cloudbase
- (U//FOUO) GUI triggers queries to CloudBase – GXT (ExtGWT)

Boundless Informant is nothing to do with Prism

5) **(U) Do you have all the data? What data is missing?**

- (U//FOUO) The tool resides on GM-PLACE which is only accredited up to TS//SI//NOFORN. Therefore, the tool does not contain ECI or FISA data.
- (U//FOUO) The Map View only shows counts for records with a valid normalized number (DNR) or administrative region atom (DNI).
- (U//FOUO) Only metadata records that are sent back to NSA-W through FASCIA or FALLOUT are counted. Therefore, programs with a distributed data distribution system (e.g. MUSCULAR and Terrestrial RF) are not currently counted.
- (U//FOUO) Only SIGINT records are currently counted. There are no ELINT or other "INT" records included.

So why Prism?

- Here's a guess
  - Direct connection to trusted set-up at hosting site.
  - Lower latency, cheaper, but most important,
    - control over who sees the requests.
- Another guess
  - NSA cannot routinely crack SSL/TLS at high volume in their NARUS (or whatever) boxes. A few trusted (trusting) individuals have shared their keys with NSA.

Some claims rings true

theguardian

Edward Snowden Q&A:

Encryption works. Properly implemented strong crypto systems are one of the few things that you can rely on. Unfortunately, endpoint security is so terrifically weak that NSA can frequently find ways around it.

Leaving the US was an incredible risk, as NSA employees must declare their foreign travel 30 days in advance and are monitored. There was a distinct possibility I would be interdicted en route, so I had to travel with no advance booking to a to allow me tc

Really? You got to China.

Second, let's be clear: I did not reveal any US operations against legitimate military targets. I pointed out where the NSA has hacked civilian infrastructure such as universities, hospitals, and private businesses because it is dangerous. These nakedly aggressively criminal acts are wrong no matter the target. Not only that, when NSA makes a technical mistake during an exploitation operation, critical systems crash. Congress hasn't declared war on the countries - the majority of them are our allies - but without asking for public permission, operations against them that people. And for what? So we can have secret access to a computer in a country we're not even fighting? So we can potentially reveal a potential terrorist with the potential to kill fewer Americans than our own Police? No, the public needs to know the kinds of things a government does in its name, or the "consent of the governed" is meaningless.

Upcoming story?