INCENSER, or how NSA and GCHQ are tapping internet cables

Archived: 2026-04-05 23:15:32 UTC

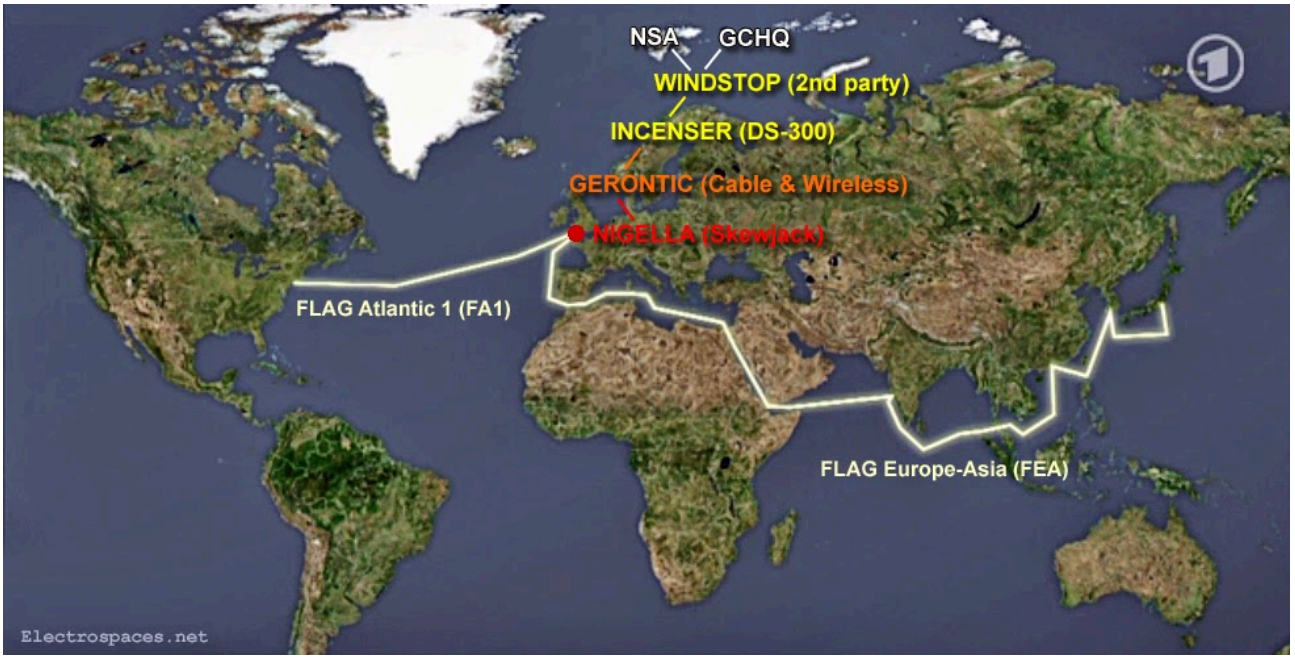
(Last edited: January 9, 2018)

Recently disclosed documents show that the NSA's fourth-largest cable tapping program, codenamed INCENSER, pulls its data from just one single source: a submarine fiber optic cable linking Asia with Europe.

Until now, it was only known that INCENSER was a sub-program of WINDSTOP and that it collected some 14 billion pieces of internet data a month. The latest revelations now say that these data were collected with the help of the British company Cable & Wireless (codenamed GERONTIC, now part of Vodafone) at a location in Cornwall in the UK, codenamed NIGELLA.

For the first time, this gives us a view on the whole interception chain, from the parent program all the way down to the physical interception facility. Here we will piece together what is known about these different stages and programs from recent and earlier publications.

- **NIGELLA** - **GERONTIC** - **INCENSER** - **WINDSTOP** -



The cables tapped at NIGELLA by GERONTIC under the INCENSER and WINDSTOP programs
(Map: ARD.de - Text: Electrospaces.net - Click to enlarge)

NIGELLA

Last week's joint reporting by the British broadcaster Channel 4, the German regional broadcasters WDR and NDR and the German newspaper Süddeutsche Zeitung, identified NIGELLA as an interception facility at the intersection of Cable & Wireless and Reliance cables at Skewjack Farm.

There, just north-west of Polgigga Cottage in Cornwall, is a large building that was constructed in 2001 for FLAG Telecom UK Ltd for 5.3 million pounds. It serves as a terminus for the two ends of a submarine optical cable: one from across the Atlantic which lands at the beach of nearby Sennen, and one that crosses the Channel to Brittany in France:

- **FLAG Atlantic 1 (FA1)**
Connecting the east coast of North America to the United Kingdom and France (6.000 kilometers)

The FLAG Atlantic 1 cable to America consists of 6 fibre pairs, each capable of carrying 40 (eventually up to 52) separate light wavelengths, and each wavelength can carry 10 Gigabit/s of traffic. This gives a potential capacity of 2.4 terabit/s per cable. However, in 2009, only 640 gigabit/s were actually used, which went apparently up to 921 gigabit/s in 2011.

The FLAG terminus station in Skewjack Farm, Cornwall
(still from 'The Secrets of Cornwall' - click to enlarge)

The cable was initially owned by FLAG Telecom, where FLAG stands for Fiber-optic Link Around the Globe. This company was renamed into Reliance Globalcom when it became a fully owned subsidiary of the Indian company Reliance Communications (RCOM). In March 2014, Reliance Globalcom was again renamed, now into Global Cloud Xchange (GCX).

More important is another, much longer submarine cable, which was also owned by this company, and which has its landing point on the shore of Porthcurno, a few miles south-west of Skewjack Farm:

- **FLAG Europe-Asia (FEA)**
Connecting the United Kingdom to Japan through the Mediterranean, with landing points in Egypt, the Saudi Peninsula, India, Malaysia, Thailand, Hong Kong, China, Taiwan, South Korea and Japan (28.000 kilometers)

This cable has 2 fibre pairs, each capable of carrying up to 40 separate light wavelengths, and each wavelength can again carry 10 gigabit/s of traffic. This gives a potential capacity of 800 gigabit/s, but in 2009 only 70 gigabit/s were used, which went up to 130 gigabit/s in 2011 - still an unimaginable 130.000.000.000 bits per second.

The

backhaul connection between the FLAG Atlantic 1 (FA1) and the FLAG Europe-Asia (FEA) is provided by a local area network of Cable & Wireless, which also connects both submarine cables to its terrestrial internet backbone network.

According to the newly disclosed GHCQ Cable Master List from 2009, the interception of the FA1 and the FEA cables takes place at the intersection with this backhaul connection:

Collateral	CNE PFENNING ALPHA
Access_Direct Interconnections	NIGELLA* (Backhaul between FEA and FA1 cables)

This list also shows that the interception of these two cables is accompanied by a Computer Network Exploitation (CNE) or hacking operation codenamed PFENNING ALPHA.

Because the owner of the cables (Reliance Globalcom, now Global Cloud Xchange) is not a cooperating partner of GCHQ, they hacked into their network for getting additional "router monitoring webpages" and "performance statistics for GTE [Global Telecoms Exploitation]".

Interception equipment

How the actual interception takes place, can be learned from an article in The Guardian from June 2013, which provides some details about the highly sophisticated computer equipment at cable tapping points.

First, the data stream is filtered through what is known as MVR (Massive Volume Reduction), which immediately rejects high-volume, low-value traffic, such as peer-to-peer downloads. This reduces the volume by about 30%.

Selectors

The next step is to pull out packets of information that contain selectors like phone numbers and e-mail, IP and MAC addresses of interest. In 2011, some 40,000 of these were chosen by GCHQ and 31,000 by the NSA, according to The Guardian. This filtering is most likely done by devices from Boeing-subsidiary Narus, which can analyse high-volume internet traffic in real-time.

A single NarusInsight machine can monitor traffic up to 10 Gigabit/second, which means there have to be up to a dozen of them to filter the relevant traffic from the FA1 and FEA submarine cables. Most of the information extracted in this way is internet content, such as the substance of e-mail messages.

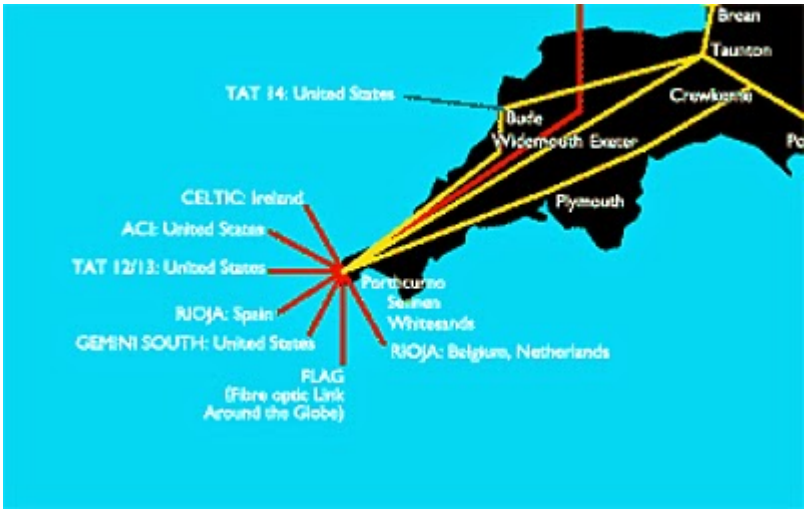
Full sessions

Besides the filtering by using specific selectors, the data are also sessionized, which means all types of IP traffic, like VoIP, e-mail, web mail and instant messages are reconstructed. This is something the Narus devices are also

capable of.

These "full take" sessions are stored as a rolling buffer on XKEYSCORE servers: content data for only three to five days, and metadata for up to 30 days. But "at some sites, the amount of data we receive per day (20+ terabytes) can only be stored for as little as 24 hours" according to an NSA document from 2008.

The aim is to extract the best 7,5% of the traffic that flows past the access, which is then "backhauled" from the tapping point to GCHQ Bude through two 10 gigabit/s channels (the "egress" capacity). This might be a dedicated cable, or a secure VPN path over the regular Cable & Wireless backbone that connects Bude with the south-west of Cornwall:



The Cable & Wireless internet backbone (yellow) in Cornwall
and the connections to submarine fiber-optic cables (red)
(Map from before 2006 - Click for the full verion)

GERONTIC (Cable & Wireless)

The secret GCHQ documents about these cable tapping operations only refer to the cooperating telecommunications provider with the cover name GERONTIC. The real name is protected by STRAP 2 dissemination restrictions. But nonetheless, German media already revealed that GERONTIC is Cable & Wireless last year.

In july 2012, Cable & Wireless Worldwide was taken over by Vodafone for 1.04 billion pounds, but according to the GCHQ documents, the covername GERONTIC was continued, and was seen active until at least April 2013.

According to the press reports, GCHQ had access to 63 undersea internet cables, 29 of which with the help of GERONTIC. This accounted for about 70% of the total amount of internet data that GCHQ had access to in 2009.

Cable & Wireless was involved in these 29 cables, either because it had Direct Cable Ownership (DCO), an Indefeasible Right of Use (IRU) or Leased Capacity (LC). Besides that, the GCHQ Cable Master List from 2009 lists GERONTIC also as a landing partner for the following nine cables:

- FLAG Atlantic 1 (FA1)
- FLAG Europe-Asia (FEA)

- Apollo North
- Apollo South
- Solas
- UK-Netherlands 14
- UK-France 3
- Europe India Gateway (EIG)
- GLO-1

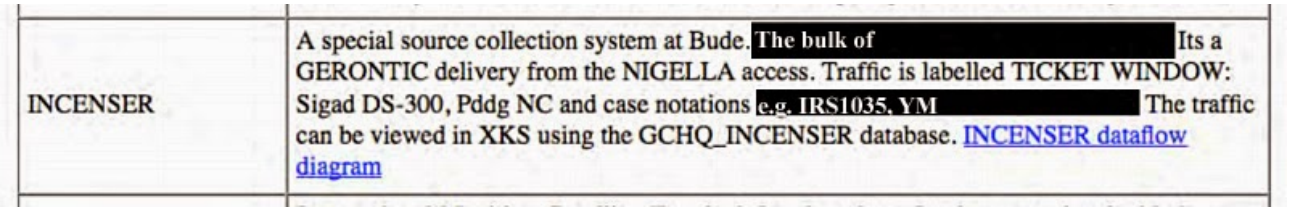
Disclosed excerpts from internal GCHQ wiki pages show that Cable & Wireless held regular meetings with GCHQ from 2008 until at least 2010, in order to improve the access possibilites, like selecting which cables and wavelenghts would provide the best opportunities for catching the communications GCHQ wanted.

GCHQ also paid Cable & Wireless tens of millions of pounds for the expenses. For example, in February 2009 6 million pound was paid and a 2010 budget references a 20.3 million pound payment to the company. By comparison, NSA paid all its cooperating telecommunications companies a total of 278 million dollars in 2013.

The intensive cooperation between Cable & Wireless and GCHQ may not come as a surprise for those knowing a bit more of British intelligence history. The company already worked with predecessors of GHCQ during World War I: all international telegrams were handed over so they could be copied before being sent on their way, a practice that continued for over 50 years.*

INCENSER (DS-300)

Among the documents about the GCHQ cable tapping is also a small part of an internal glossary. It contains an entry about INCENSER, which says that this is a special source collection system at Bude. This is further specified as the GERONTIC delivery from the NIGELLA access, which can be viewed in XKEYSCORE (XKS):



INCENSER	A special source collection system at Bude. **The bulk of** [redacted] Its a GERONTIC delivery from the NIGELLA access. Traffic is labelled TICKET WINDOW: Sigad DS-300, Pddg NC and case notations **e.g. IRS1035, YM** [redacted] The traffic can be viewed in XKS using the GCHQ_INCENSER database. INCENSER dataflow diagram

This entry was also shown in the German television magazine Monitor, although not fully, but without the redactions, so from this source we know the few extra words that were redacted for some reason.

The entry also says that INCENSER traffic is labeled TICKETWINDOW with the SIGINT Activity Designator (Sigad) DS-300. From another source we know that TICKETWINDOW is a system that makes cable tapping collection available to 2nd Party partners. The exact meaning of Sigads starting with DS is still not clear, but probably also denotes 2nd Party collection.

TEMPORA

In Bude, GCHQ has its Regional Processing Center (RPC), which in 2012 had a so-called "Deep Dive" processing capability for 23 channels of 10 gigabit/second each under the TEMPORA program.

TEMPORA comprises different components, like the actual access points to fiber-optic cables, a Massive Volume Reduction (MVR) capability, a sanitisation program codenamed POKERFACE, and the XKEYSCORE system. As we have seen, most of the hardware components are located at the interception point, in this case the facility in Skewjack (NIGELLA).

Analysing

These collection systems can be remotely instructed ("tasked") from Bude, or maybe even also from NSA headquarters. For one part that involves entering the "strong selectors" like phone numbers and internet addresses. For another part, that is by using the additional capabilities of XKEYSCORE.

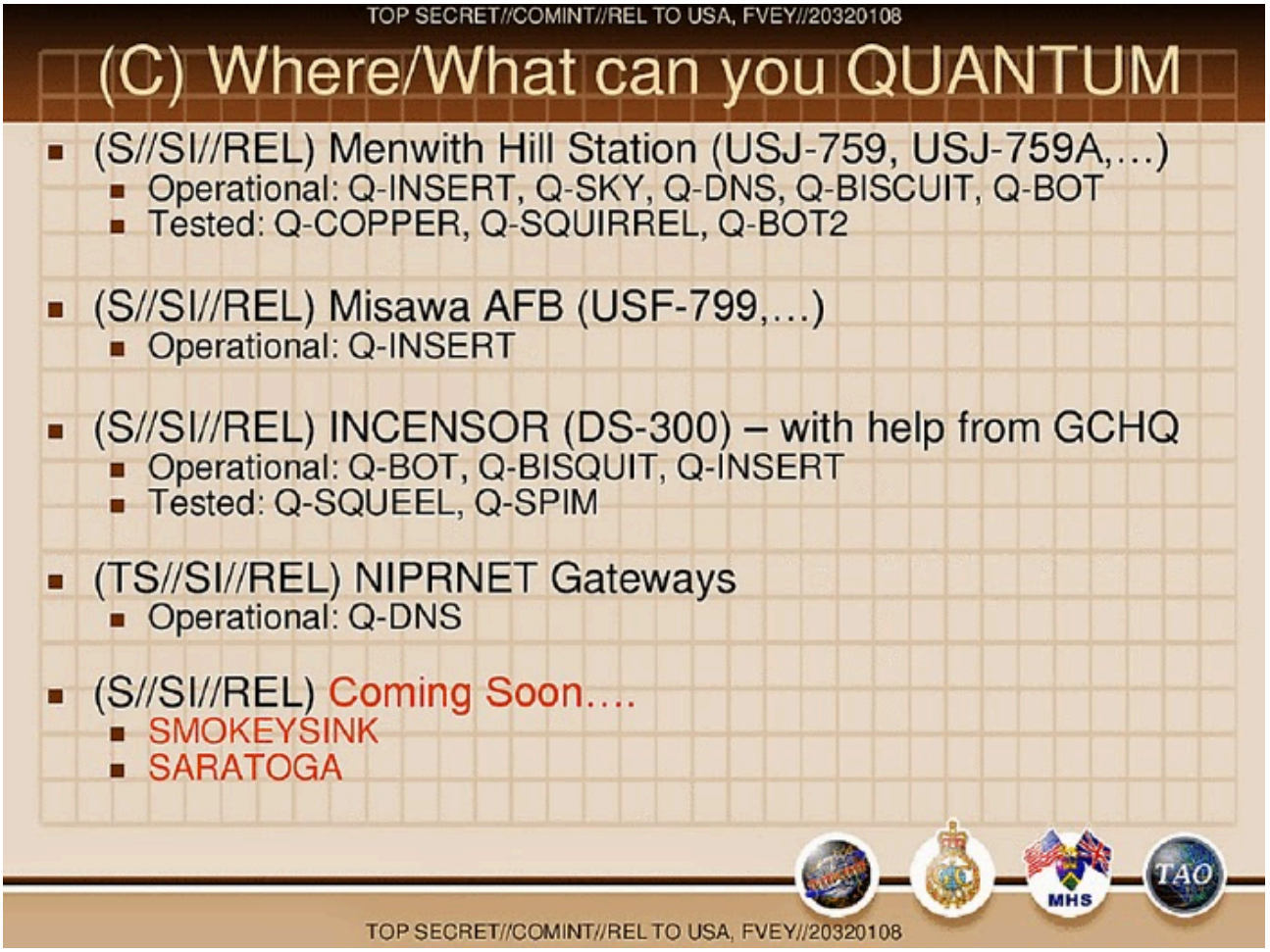
Because the latter system buffers full take sessions, analysts can also perform queries using "soft selectors", like keywords, against the body texts of e-mail and chat messages, digital documents and spreadsheets in English, Arabic and Chinese. XKEYSCORE also allows analysts to look for the usage of encryption, the use of a VPN or the TOR network, and a number of other things that could lead to a target.

This is particularly useful to trace target's internet activities that are performed anonymous, and therefore cannot be found by just looking for the known e-mail addresses of a target. When such content has been found, the analyst might be able to find new intelligence or new strong selectors, which can then be used for starting a traditional search.

Hacking operations

According to a 2010 NSA presentation that was published by The Intercept in December 2014, the INCENSER access is also capable of supporting the QUANTUMBOT (IRC botnet hijacking), QUANTUMBISQUIT (for targets who are behind large proxies), and QUANTUMINSERT (HTML web page redirection) hacking techniques.

Two other components of the QUANTUMTHEORY computer network exploitation framework, QUANTUMSQUEEL (for injection of MySQL databases) and QUANTUMSPIM (for instant messaging), had been tested, but weren't yet operational:



This means that at the INCENSER collection site NIGELLA, there are also TURMOIL sensors which detect when targeted user's packets are among the traffic that flows past. TURMOIL tips off the central automated command & control system codenamed TURBINE, which then launches one or more QUANTUM attacks, as directed by NSA's hacking division Tailored Access Operations (TAO). An explanation of this method is on the weblog of Robert Sesek and the website of Wired.

Possible targets

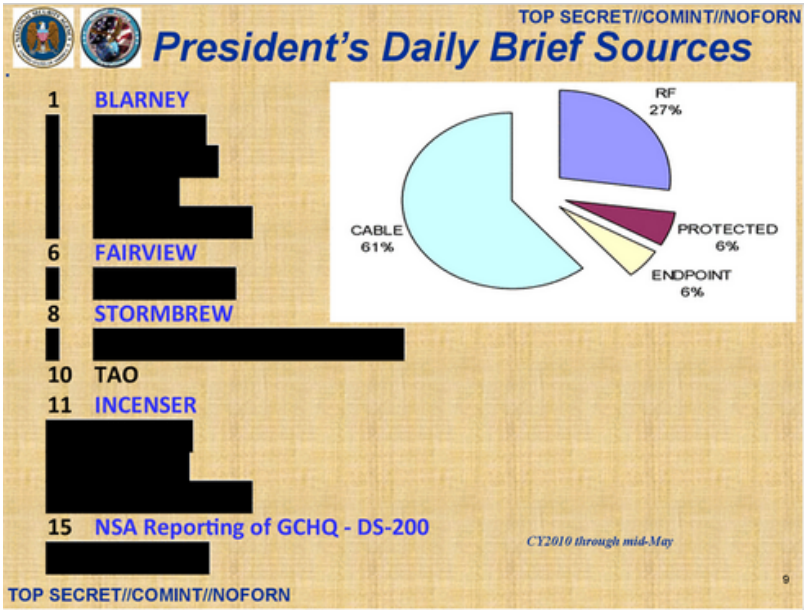
The disclosed GCHQ documents contain no specific targets or goals for the INCENSER program, which provided Channel 4 the opportunity to claim that this Cable & Wireless/Vodafone access allows "Britain's spies to gather the private communications of millions of internet users worldwide". Vodafone, which also has a large share of the telecommuncations market in Germany, was even linked to the eavesdropping on chancellor Merkel.

Both claims are rather sensationalistic. Merkel's phone was probably tapped by other means, and both GCHQ and NSA aren't interested in the private communications of ordinary internet users. On the contrary, by tapping into a submarine cable that connects to Asia and the Middle East, INCENSER looks rather focussed at high-priority targets in the latter region.

> **Update:** The redacted source trigraphs of the case notations in the internal GCHQ glossary, which start with IR and YM, seem to point to Iran (Iraq is IQ) and Yemen as target countries of the INCENSER program.

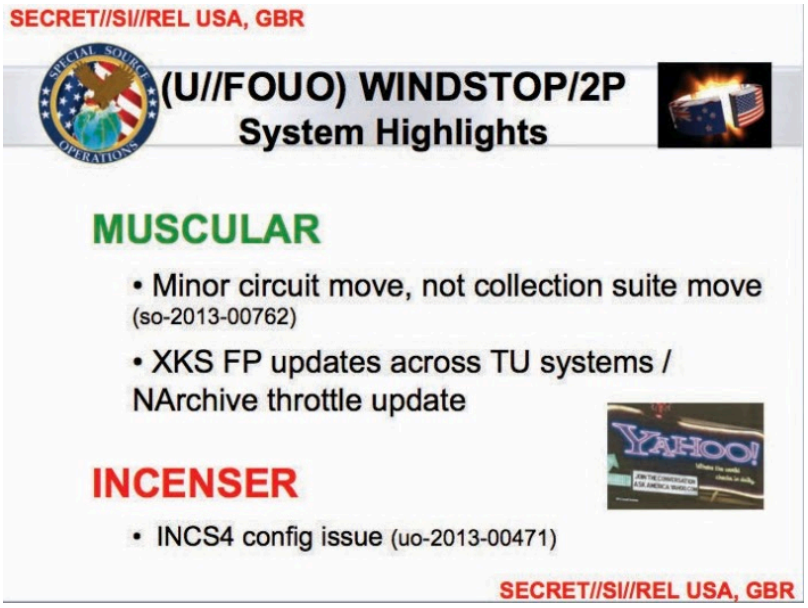
Reporting

Despite INCENSER being NSA's fourth-largest cable tapping program regarding to the volume which is collected, the intelligence reports analysts are able to write based upon this only made it to the 11th position of contributors to the President's Daily Brief - according to a slide from a 2010 presentation about Special Source Collection, published by The Washington Post in October last year:



WINDSTOP (2nd Party)

Data collected under the INCENSER program are not only used by GHCQ, but also by NSA, which groups such 2nd Party sources under the codename WINDSTOP. As such, INCENSER was first mentioned in a slide that was published by the Washington Post on in October 2013 for a story about the MUSCULAR program:

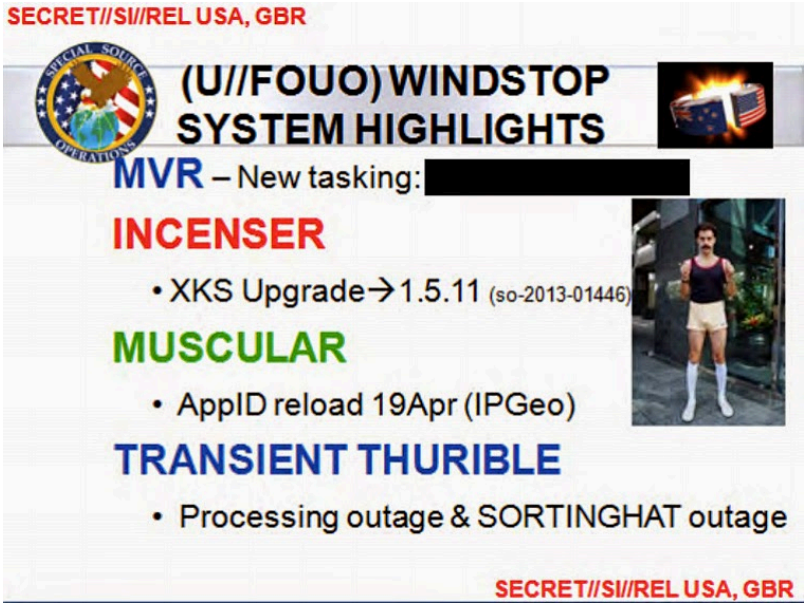


According to NSA's Foreign Partner Access budget for 2013, which was published by Information and The Intercept last June, WINDSTOP involves all 2nd Party countries (primarily Britain, but also Canada, Australia and

New Zealand) and focusses on access to (mainly internet) "communications into and out of Europe and the Middle East" through an integrated and overarching collection system.

MUSCULAR is a program under which cables linking big data centers of Google and Yahoo are tapped. The intercept facility is also located somewhere in the United Kingdom and the data are processed by GCHQ and NSA in a Joint Processing Centre (JPC) using the Stage 2 version of XKEYSCORE.

A new slide from this presentation about WINDSTOP was published by Süddeutsche Zeitung on November 25, which reveals that a third program is codenamed TRANSIENT THURIBLE. About this program The Guardian reported once in June 2013, saying that it is an XKeyscore Deep Dive capability managed by GHCQ, with metadata flowing into NSA repositories since August 2012.



In November 2013, the Washington Post published a screenshot from BOUNDLESSINFORMANT with numbers about data collection under the WINDSTOP program. Between December 10, 2012 and January 8, 2013, more than 14 billion metadata records were collected:

The bar chart in the top part shows the numbers by date, with DNR (telephony) in green and DNI (internet) in blue. The section in the center of the lower part shows these data were collected by the following programs:

- DS-300 (INCENSER): 14100 million records
- DS-200B (MUSCULAR): 181 million records

XKEYSCORE, which is used to index and search the data collected under the INCENSER program, can be seen in the bottom right section of the chart.

With just over 14 billion pieces of internet data a month, INCENSER is the NSA's fourth-largest cable tapping program, accounting for 9 % of the total amount collected by Special Source Operations (SSO), the division responsible for collecting data from internet cables. According to another BOUNDLESSINFORMANT chart, the NSA's Top 5 of cable tapping programs is:

SSO worldwide total:	160.168.000.000 (100%)
DANCINGOASIS:	57.788.148.908 (36%)
SPINNERET (part of RAMPART-A):	23.003.996.216 (14%)
MOONLIGHTPATH (part of RAMPART-A):	15.237.950.124 (9%)
INCENSER (part of WINDSTOP):	**14.100.359.119 (9%)**
AZUREPHOENIX (part of RAMPART-A):	13.255.960.192 (8%)
...	...
Other programs:	38.000.000.000 (24%)

It's remarkable that just one single cable access (NIGELLA in Cornwall) provides almost one tenth of everything NSA collects from internet cables. This also means that besides a large number of small cables accesses, NSA seems to rely on just a few important cables for about 2/3 of it's collection from this type of source.

Links and Sources

- Documentary about the cable landing stations: The Secrets of Cornwall
- Golem.de: Die Abhörkette der Geheimdienste
- The recently disclosed documents about GCHQ cable tapping:
  - NetzPolitik.org: Cable Master List: Wir spiegeln die Snowden-Dokumente über angezapfte Glasfasern, auch von Vodafone
  - Sueddeutsche.de: Snowden-Leaks: How Vodafone-Subsidiary Cable & Wireless Aided GCHQ's Spying Efforts
- ArsTechnica.com: New Snowden docs: GCHQ's ties to telco gave spies global surveillance reach
- Sueddeutsche.de: Vodafone-Firma soll GCHQ und NSA beim Spähen geholfen haben
- WDR.de: Neue Snowden-Dokumente enthüllen Ausmaß der Zusammenarbeit von Geheimdiensten und Telekommunikationsunternehmen
- TheRegister.co.uk: REVEALED: GCHQ's BEYOND TOP SECRET Middle Eastern INTERNET SPY BASE
- Weblog about Uk Submarine Cable Landings & Cable Stations
- Article about Explaining submarine system terminology – Part 1

Thanks also to Henrik Moltke, who did most of the research for the German press reports

More reactions on Hacker News and Schneier's Blog
