

# Why we need Independence from America

Dave Webb  
Chair, C.N.D.  
Convenor, Global Network Against Weapons  
and Nuclear Power in Space





The US uses MHS for: Monitoring, Surveillance, Drome Operations, and as part of its Missile 'Defence' System.

Menwith Hill is a major component of the US electronic surveillance and hacking network. Its role is to collect information which it does through COMINT and SIGINT activities.

**COMINT** - information gathered from the **communications** of individuals, including telephone conversations, text messages and various types of online interactions.

**SIGINT** – intelligence gathered by the interception of signals.



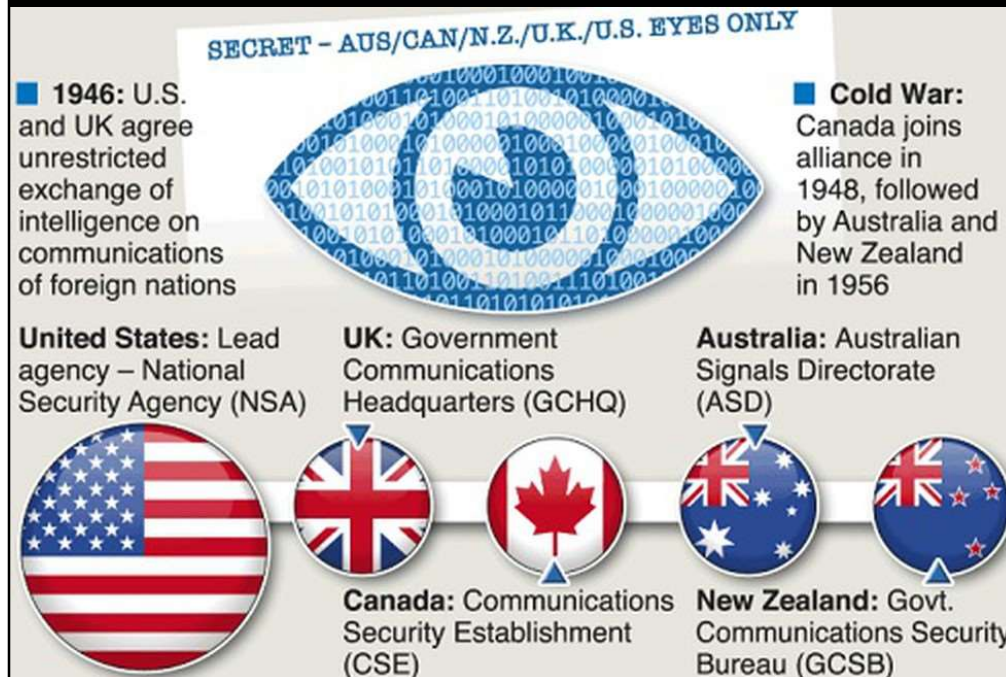
Two US organisations are involved –  
the NRO (National Reconnaissance Office) designs, builds, launches, and operates the reconnaissance satellites.

the NSA (National Security Agency) which is responsible for global monitoring, collection, and processing of information and data for foreign and domestic intelligence and counterintelligence purposes.

Both are members of the United States Intelligence Community and along with the Central Intelligence Agency (CIA), the Defense Intelligence Agency (DIA), and the National Geospatial-Intelligence Agency (NGA) form the "big five" U.S. intelligence agencies.

The UK's GCHQ works quite closely with the NSA and there are a few hundred operatives from there also present at Menwith.

# Five Eyes intelligence sharing

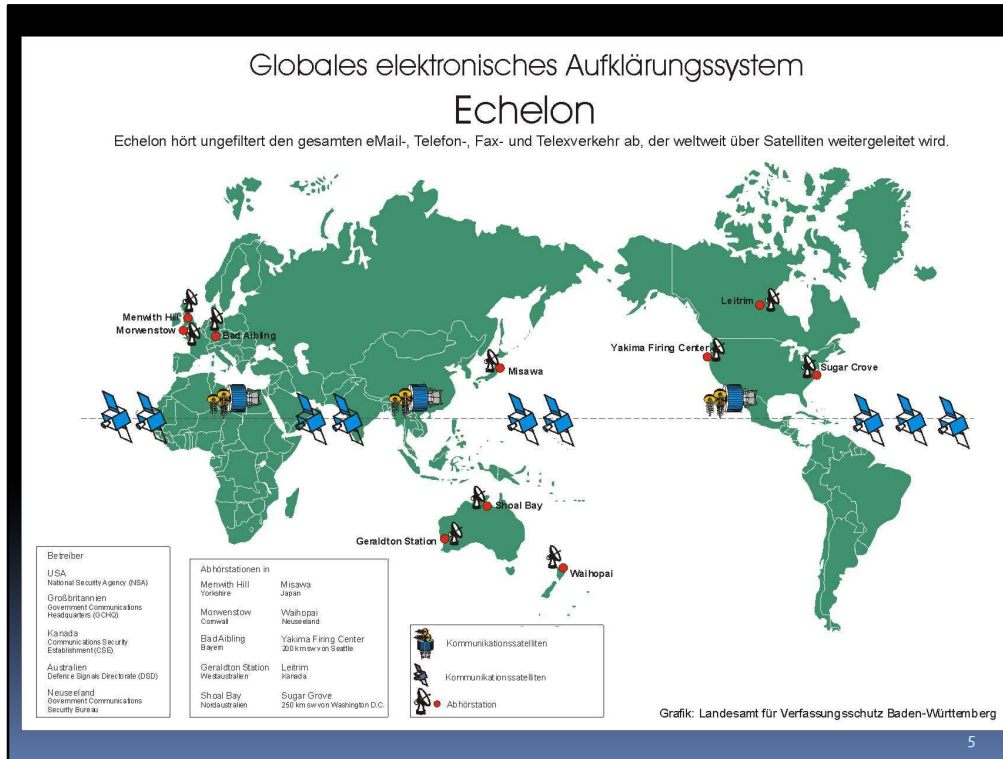


The UK is a member of the Five Eyes intelligence sharing community.

The US-UK intelligence sharing during and after WW2 is well known. The UK had also been involved in the US high altitude U2 spy plan operations. As things developed and the US moved to space reconnaissance, the UK realised it was in a privileged position with regard to US space systems and it became important politically to maintain this position. It therefore adjusted its political stance on some major issues accordingly.

E.g. in June 1984 a joint-MoD/FCO study highlighted the fact that the West was more dependent on communications and reconnaissance satellites than the Soviet Union. It advocated that a ban on ASATs would be in our national interest because SDI and ASATs involved many of the same fundamental technologies and a ban on ASATs would have likely prevented SDI from moving into a testing and deployment phase. However, Thatcher disagreed and saying that the U.S. had a great deal more technical knowledge than the UK and we would risk annoying them on ASATs and SDI, possibly harming Anglo-American intelligence sharing.

The UK has followed this path ever since. In an effort to boost Britain's relevance (and because of the importance of the SIGINT information made available by the US during the Falklands War) Thatcher approved the development of Zircon, a SIGINT satellite that was intended to be launched in 1988. This too was exposed by Duncan Campbell and although most of the program's details remain classified, the program was cancelled in 1987 due to cost.



Perhaps Menwith Hill is best known for echelon – an information gathering and sorting system that enabled powerful computers at Menwith Hill to search for specific types of information. The system was disclosed by Duncan Campbell in the 1970s from information provided by a whistle-blower working at the station - Margaret Newsham.

Information gathered by the US intelligence satellites was partly analysed at Menwith Hill relevant information sent on to NSA HQ at Fort Mead in Maryland, U.S.A.



**ECHELON**, originally a secret government code name, is a surveillance program (signals intelligence/SIGINT collection and analysis network) operated by the United States with the aid of four other signatory states to the UKUSA Security Agreement: Australia, Canada, New Zealand, and the United Kingdom, also known as the Five Eyes.

Created in the late 1960s to monitor the military and diplomatic communications of the Soviet Union and its Eastern Bloc allies during the Cold War, the ECHELON project became formally established in 1971.

By the end of the 20th century, the system referred to as "ECHELON" had evolved beyond its military and diplomatic origins into "a global system for the interception of private and commercial communications" (mass surveillance and industrial espionage).

6

Created in the late 1960s to monitor the military and diplomatic communications of the Soviet Union and its Eastern Bloc allies during the Cold War, the ECHELON project became formally established in 1971.

By the end of the 20th century, the system referred to as "ECHELON" had evolved beyond its military and diplomatic origins into "a global system for the interception of private and commercial communications" (mass surveillance and industrial espionage).

used for political purposes – e.g. Thatcher in 2000

## Thatcher ordered Echelon surveillance when PM

Ex-spy discloses surveillance orders made during Thatcher's reign



By ZDNet UK February 25, 2000 1:07 GMT (11:07 GMT) | Topic: Innovation

It is reported a Canadian agent spied on at least two cabinet ministers using the Echelon surveillance network during Margaret Thatcher's premiership, according to revelations on US TV this week.

Ex-spy Mike Frost told the CBS *60 Minutes* programme that Thatcher had ordered surveillance on two cabinet colleagues according to excerpts released on Thursday. The allegation comes in the same week that a European Parliament report said Echelon, a surveillance system run by the United States, Canada, Britain, Australia and New Zealand, was used for industrial espionage.

Echelon was originally designed as a crime-fighting network: to eavesdrop on suspected terrorists, drug lords and governments hostile to the five members. It is capable of intercepting phone conversations, faxes and email messages around the world.

In excerpts released by *60 Minutes*, Frost talks of the spying ordered by Thatcher. "[Thatcher] had two ministers that she said 'they weren't onside'... so my boss went to London and did intercept traffic from those two ministers." He does not identify the ministers.

Political spying ... by-passing legal issues.





## Menwith Hill has two main spying capabilities:



1. **FORNSAT** uses powerful antennae contained within the golf balls to eavesdrop on communications as they are being beamed between foreign satellites.
2. **OVERHEAD** uses U.S. government satellites orbiting above targeted countries to locate and monitor wireless communications on the ground below — such as cellphone calls and even WiFi traffic.

9

Menwith has 2 main spying capabilities:

**FORNSAT** uses powerful antennae contained within the golf balls to eavesdrop on communications as they are being beamed between foreign satellites.

**OVERHEAD** uses U.S. government satellites orbiting above targeted countries to locate and monitor wireless communications on the ground below — such as cellphone calls and even WiFi traffic.

## Spy satellite generations:

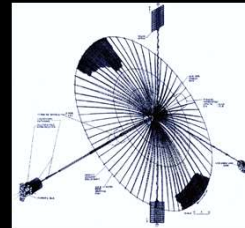
**Jumpseat series:** 1970s & 1980s – SIGINT collection from highly elliptical orbits which meant they would move very slowly over the northern hemisphere for most of their orbital period, allowing interception of microwave line-of-sight communications beams.

**Canyon-Chalet-Vortex-Mercury series:** 1980s & 1990s, geostationary orbit; focussed on COMINT, but had the capability to also intercept missile telemetry (1982- assisted the UK during the Falkland's War).

**Trumpet series:** 1990s SIGINT, replaced 'Jumpseat', highly elliptic orbits; constellation required to monitor Soviet communications throughout the day; probably also intercepted up- or down-links from Soviet strategic communications satellites.

**TRUMPET follow-on series:** first launched 2006, NROL-42 also carries additional payload for SBIRS-HEO for the USAF.

**Nemesis series:** 2009 - other high orbit SIGINT.



Chalet/Vortex (1980s, 1990s)



ORION/Mentor SIGINT satellite



NROL-42: Trumpet follow-on satellite

10

Menwith Hill has been using a series of satellites dating back to the 1970s for these activities.

**Jumpseat series:** 1970s & 1980s – SIGINT collection from highly elliptical orbits which meant they would move very slowly over the northern hemisphere for most of their orbital period, allowing interception of microwave line-of-sight communications beams.

**Canyon-Chalet-Vortex-Mercury series:** 1980s & 1990s, geostationary orbit; focussed on COMINT, but had the capability to also intercept missile telemetry (1982- assisted the UK during the Falkland's War and led to plans for Zircon).

**Trumpet series:** 1990s SIGINT, replaced 'Jumpseat', highly elliptic orbits; constellation required to monitor Soviet communications throughout the day; probably also intercepted up- or down-links from Soviet strategic communications satellites.

**TRUMPET follow-on series:** first launched 2006, NROL-42 also carries additional payload for SBIRS-HEO for the USAF.



PAN, the first NEMESIS-class satellite was launched in 2009, its "mission will be Foreign Satellite (FORNSAT) collection from space – targeting commercial satellite uplinks not normally accessible via conventional means." It is probably the first US high-altitude SIGINT satellite not derived from a cold war-era design.

11

**Nemesis series:** 2009 - other high orbit SIGINT – first named PAN has a mission for FORNSAT collection from space – targeting commercial satellite uplinks not normally accessible via conventional means." Probably first US high-altitude SIGINT satellite not derived from a cold war era design.



# Primary Fornsat Collection Operations



This map, from 2002, shows the following satellite intercept stations:

### US Sites:

- TIMBERLINE, Sugar Grove (US)
- CORALINE, Sabena Seca (Puerto Rico)
- SCS, Brasilia (Brazil)
- MOONPENNY, Harrogate (Great Britain)
- GARLICK, Bad Aibling (Germany)
- LADYLOVE, Misawa (Japan)
- LEMONWOOD, Thailand
- SCS, New Delhi (India)

### 2nd Party Sites:

- CARBOY, Bude (Great Britain)
- SOUNDER, Ayios Nikolaos (Cyprus)
- SNICK, near Seeb (Oman)
- SCAPEL, Nairobi (Kenya)
- STELLAR, Geraldton (Australia)
- SHOAL BAY, Darwin (Australia)
- IRONSAND, New Zealand

12

**PRIMARY FORNSAT COLLECTION OPERATIONS:** This map, from 2002, shows the following satellite intercept stations:

### US Operated Sites:

- TIMBERLINE, Sugar Grove (US)
- CORALINE, Sabena Seca (Puerto Rico)
- SCS, Brasilia (Brazil)
- MOONPENNY, Harrogate (Great Britain)
- GARLICK, Bad Aibling (Germany)
- LADYLOVE, Misawa (Japan)
- LEMONWOOD, Thailand
- SCS, New Delhi (India)

### 2nd Party Sites:

- CARBOY, Bude (Great Britain)
- SOUNDER, Ayios Nikolaos (Cyprus)
- SNICK, near Seeb (Oman)
- SCAPEL, Nairobi (Kenya)
- STELLAR, Geraldton (Australia)
- SHOAL BAY, Darwin (Australia)
- IRONSAND, New Zealand

TOP SECRET// COMINT //REL USA, AUS, CAN, GBR, NZL

## *Approved SIGINT Partners*

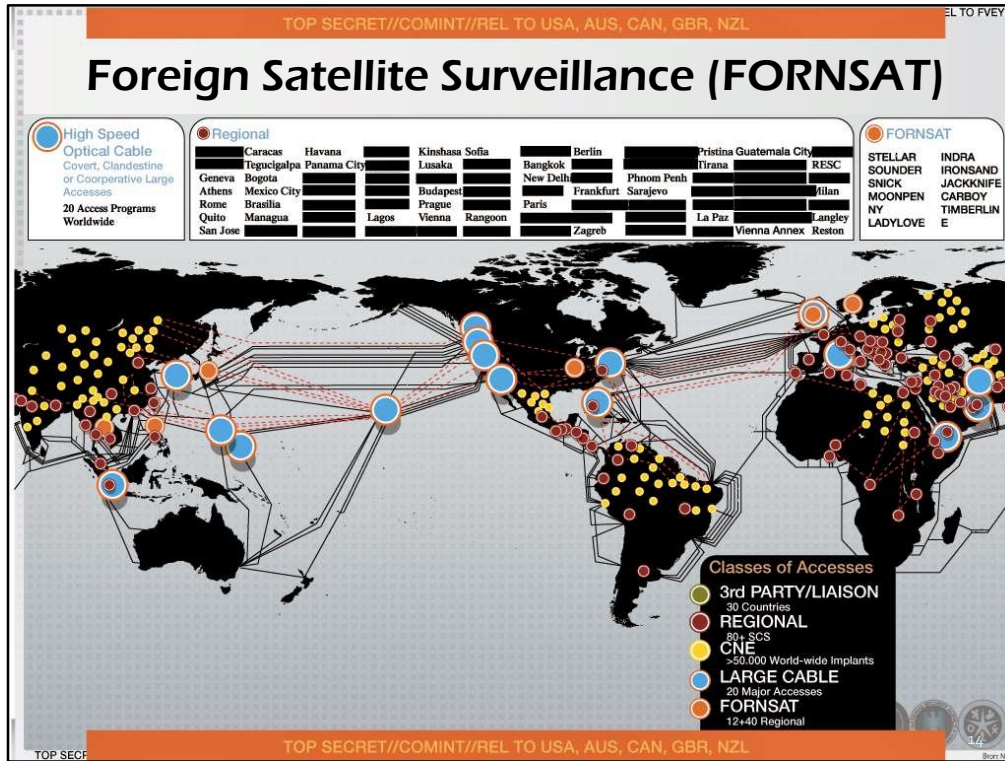


<u>Second Parties</u>	<u>Third Parties</u>	
Australia Canada New Zealand United Kingdom	Algeria Austria Belgium Croatia Czech Republic Denmark Ethiopia Finland France Germany Greece Hungary India	Israel Italy Japan Jordan Korea Macedonia Netherlands Norway Pakistan Poland Romania Saudi Arabia Singapore
<u>Coalitions/Multi-lats</u>		
AFSC NATO SSEUR SSPAC	Spain Sweden Taiwan Thailand Tunisia Turkey UAE	

TOP SECRET// COMINT //REL USA, AUS, CAN, GBR, NZL

13

5 EYES Approved SIGINT Third Party Partners



### The Global reach of Foreign Satellite Surveillance (FORNSAT)

- Different classes of access –
- 3<sup>rd</sup> Party;
  - Regional;
  - CNE (Computer Network Exploitation);
  - Large Cable;
  - FORNSAT

DYNAMIC PAGE -- HIGHEST POSSIBLE CLASSIFICATION IS  
TOP SECRET // SI / TK // REL TO USA AUS CAN GBR NZL

**(S//SI//REL) APPARITION Becomes a Reality: New Corporate VSAT-Geolocation Capability Sees Its First Deployment**

FROM: [REDACTED] and [REDACTED]  
Office of Overhead (S333)  
Run Date: 12/11/2008

(S//SI//REL) The first operational version of APPARITION achieved Initial Operating Capability (IOC) at Misawa, Japan, in late September. APPARITION is a precision geolocation capability for targeting foreign very small aperture satellite terminals (VSAT) -- an important target, because VSATs are often used by Internet cafes and foreign governments in the Middle East. APPARITION builds on the success of the GHOSTHUNTER prototype developed at Menwith Hill Station, a tool that enabled a significant number of capture-kill operations against terrorists.

**(U) Going Global**

(S//SI//REL) The GHOSTHUNTER prototype (see [background](#)) capitalized on the co-location of Overhead SIGINT and FORNSAT\* at Menwith Hill Station to combine collection from both apertures to perform precise geolocations of VSATs. With APPARITION, this capability will not be limited to collocated sites; it will now be possible for collection from sites *worldwide* to be combined with Overhead collection. Plans call for APPARITION to be deployed to a number of FORNSAT and Special Collection Service (SCS) sites in the coming years.

(S//SI//REL) This first APPARITION system builds on lessons learned from the initial GHOSTHUNTER implementation, and represents a more generic concept of operations (CONOP) for use worldwide. Rather than "chasing" the targets when they come on-line in a reactive approach, APPARITION uses an "industrial survey" concept that proactively targets and geolocates VSATs and populates the MASTERSHAKE (see [background](#)) database with the results. This approach reduces response time: by interrogating the database, a geolocation of the VSAT can be provided within seconds of the target appearing on-line.

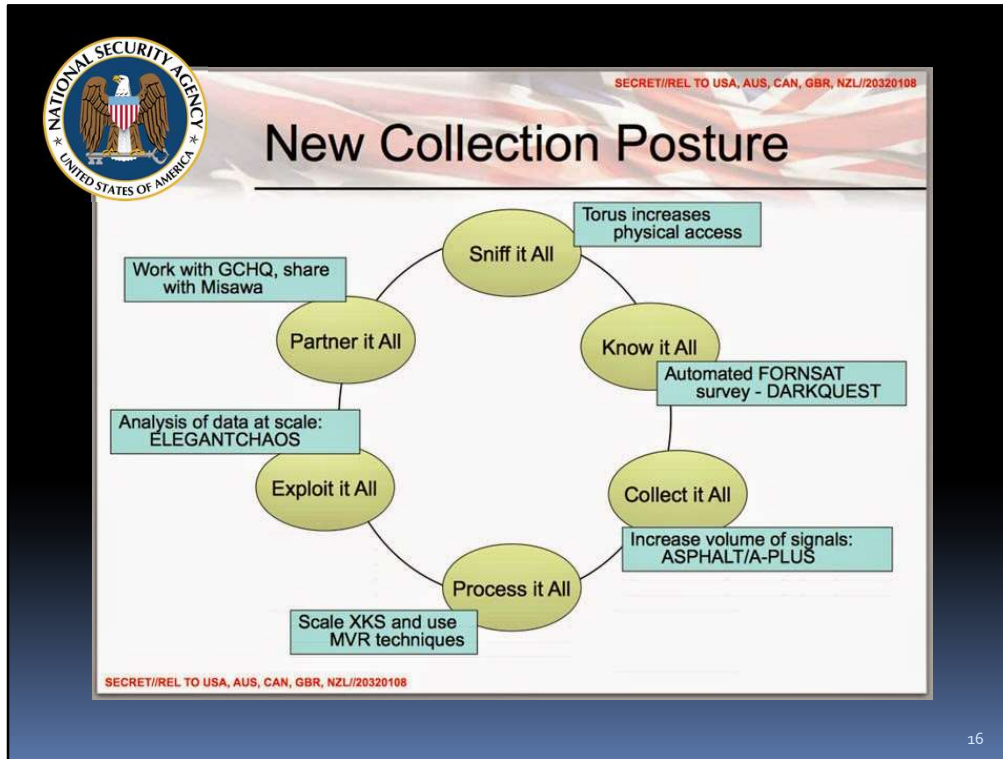
Surveillance tools such as the **GHOSTHUNTER** system were developed to directly aid military operations, pinpointing the locations of targeted people or groups so that they could then be captured or killed.

NSA describes **GHOSTHUNTER** as a means "to locate targets when they log onto the internet" -- it has enabled "a significant number of capture-kill operations" against alleged terrorists.

15

Surveillance tools such as the **GHOSTHUNTER** system have been developed to directly aid military operations, pinpointing the locations of targeted people or groups so that they could then be captured or killed.


The NSA describes **GHOSTHUNTER** as a means "to locate targets when they log onto the internet" -- it has enabled "a significant number of capture-kill operations" against alleged terrorists.

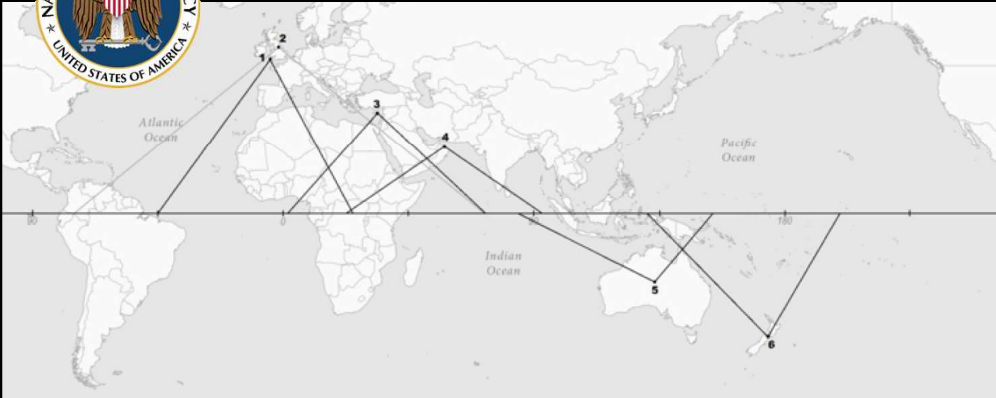


**New Collection Posture:**

Sniff it all – access it all, the new Torus system increases the physical access ability;  
 Know it all – FORNSAT; Collect it all; Process it all; Exploit it All;  
 Partner it all (with GCHQ and others)



 **The Torus System**



Multiple advanced quasi-parabolic multi-beam antenna sites (can simultaneously intercept up to 35 satellite communications) - the geostationary satellite coverage.

1. Morwenstow 2. Menwith Hill 3. GCHQ Ayios Nikolaos, Cyprus 4. Seeb, Oman 5. Pine Gap, Australia 6. Waihopai, New Zealand

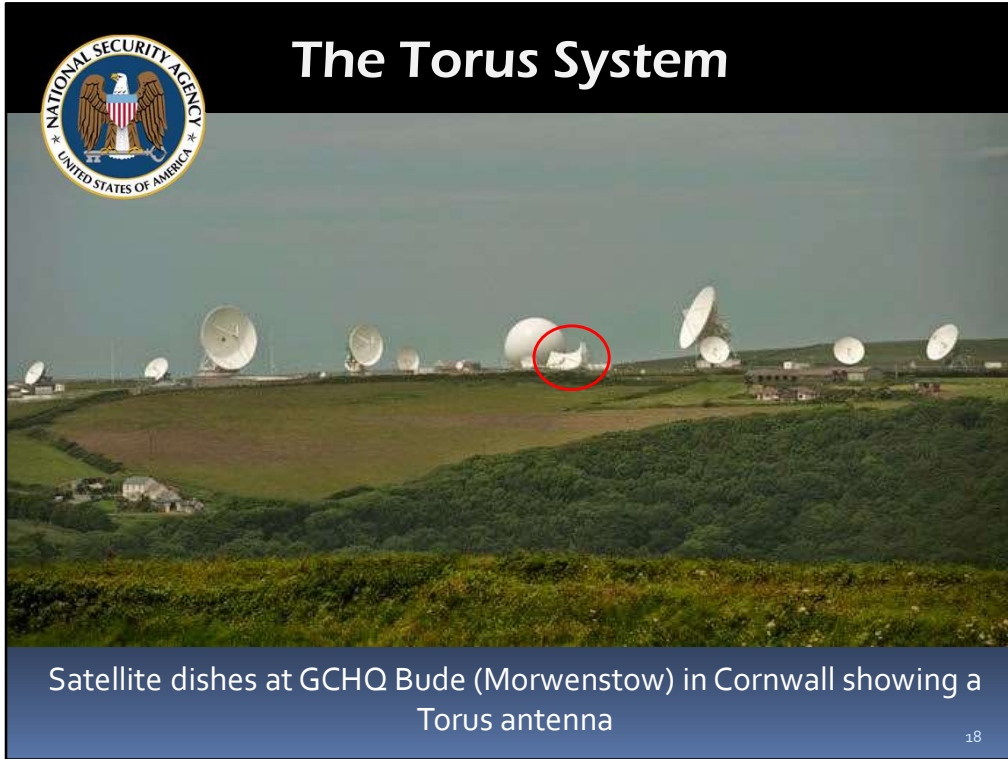
17

## The Torus System

A Multiple advanced quasi-parabolic multi-beam antenna sites (can simultaneously intercept up to 35 satellite communications) and the geostationary satellite coverage.

Relay stations at:

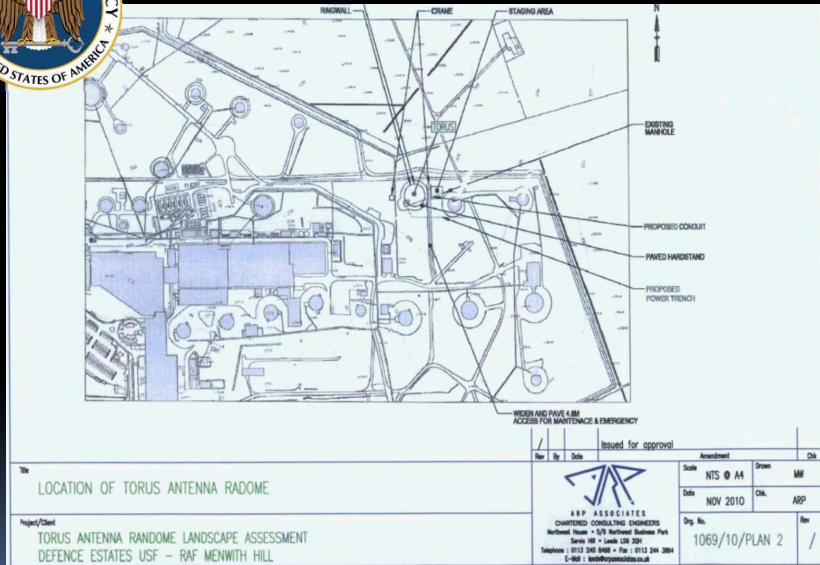
1. Morwenstow (Bude, Cornwall)
2. Menwith Hill
3. GCHQ Ayios Nikolaos, Cyprus
4. Seeb, Oman
5. Pine Gap, Australia
6. Waihopai, New Zealand



Satellite dishes at GCHQ Bude (Morwenstow) in Cornwall showing a Torus antenna



# Torus at Menwith

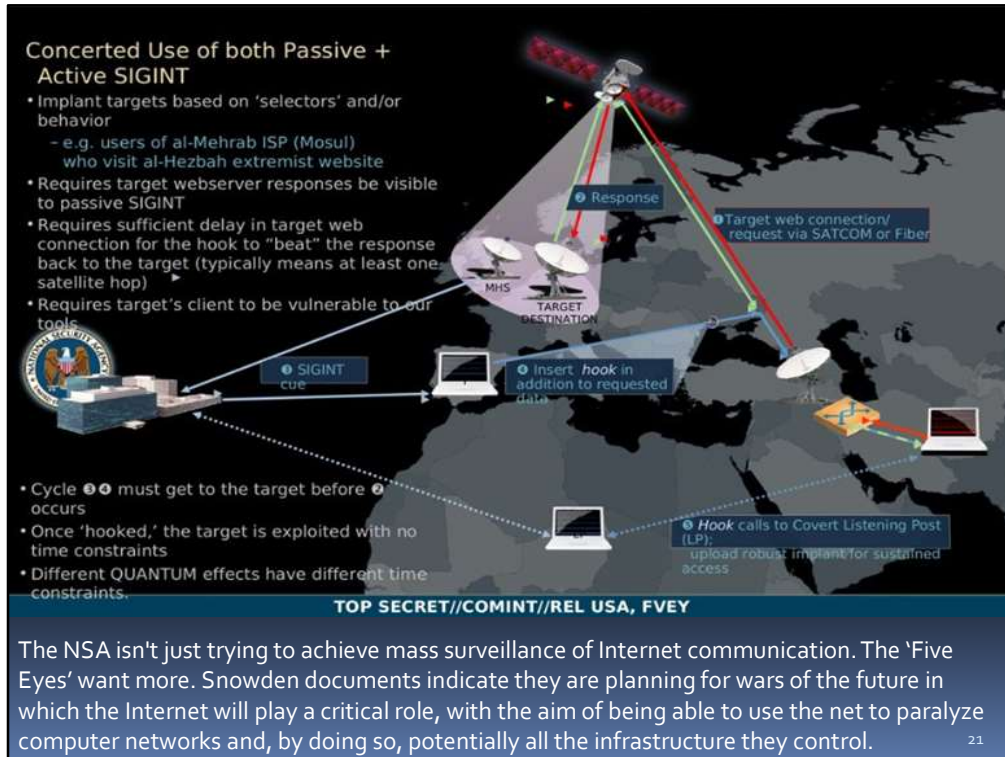


A Torus was apparently installed at Menwith Hill in late 2011 - underneath a slightly 'squashed' radome.

Here are the plans for the Menwith installation.



And this is it - installed at Menwith Hill in late 2011 - underneath a slightly 'squashed' radome.



On March 7, 2017, Wikileaks published 8761 documents and files on computer malware and viruses used to penetrate smartphones, smart televisions, computer systems, web browsers (including Google Chrome, Microsoft Edge, Mozilla Firefox, and Opera Software ASA), and the operating systems of most smartphones (including Apple's iOS and Google's Android) and computers (such as Microsoft Windows, macOS, and Linux).

“Active SIGINT” – involves infecting computers with malware. The NSA intercepts computer servers during shipment through its Tailored Access Operations (TAO) unit and implants devices that transmit data to the NSA.

These might allow the NSA to take over the microphone and record conversations, take photographs via the webcam or even gain complete control of an infected computer.

## 'Hybrid Warfare'

Military strategists talk of '*hybrid warfare*' – which brings together conventional warfare and cyberwarfare with such things as fake news, diplomacy, lawfare and foreign electoral intervention into a form of political warfare. Cyber-attacks and hacking play an important role in the execution of both covert and overt warfare.

The hacking of communications systems and eavesdropping on for example, embassies, is now common place and cyber-attacks threaten to disrupt important infrastructure networks such as communications, the power grid, the financial sector, etc. or worse - they may attempt to neutralise security systems or even take them over with possible catastrophic results.

22

Targets include embassies and UN missions. A form of hybrid warfare.

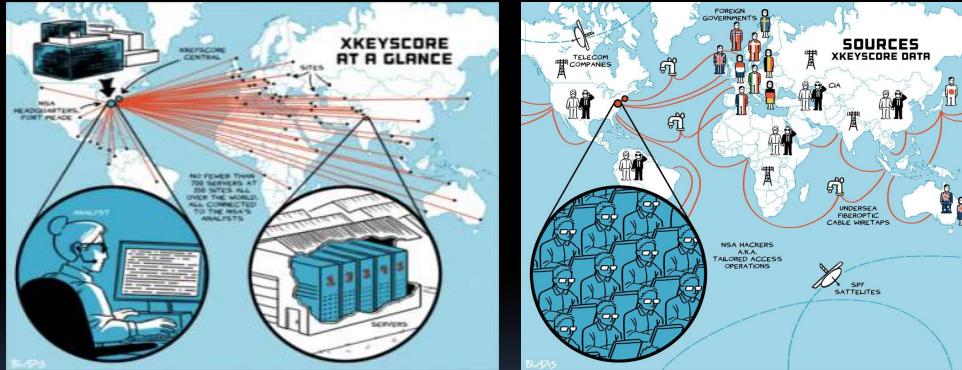
'*Hybrid warfare*' – brings together conventional warfare and cyberwarfare with such things as fake news, diplomacy, lawfare and foreign electoral intervention into a form of political warfare. Cyber-attacks and hacking play an important role in the execution of both covert and overt warfare.

The hacking of communications systems and eavesdropping on embassies and politicians, is now common place and cyber-attacks threaten to disrupt important infrastructure networks such as communications, the power grid, the financial sector, etc. or worse - they may attempt to neutralise security systems or even take them over with possible catastrophic results.



# XKeyscore

Used by the NSA to search and analyse global Internet data, which it collects continually.



The NSA has shared *XKeyscore* with other intelligence agencies including the UK, Australia, NZ, Japan and Germany.

23

**XKeyscore** - One of the tools used by the NSA to search and analyse global Internet data, which it collects continually.

The NSA has shared *XKeyscore* with other intelligence agencies including the UK, Australia, NZ, Japan and Germany.



XKeyscore servers of the NSA collect data from "US and allied military and other facilities as well as US embassies and consulates". The data come from three main collection systems:



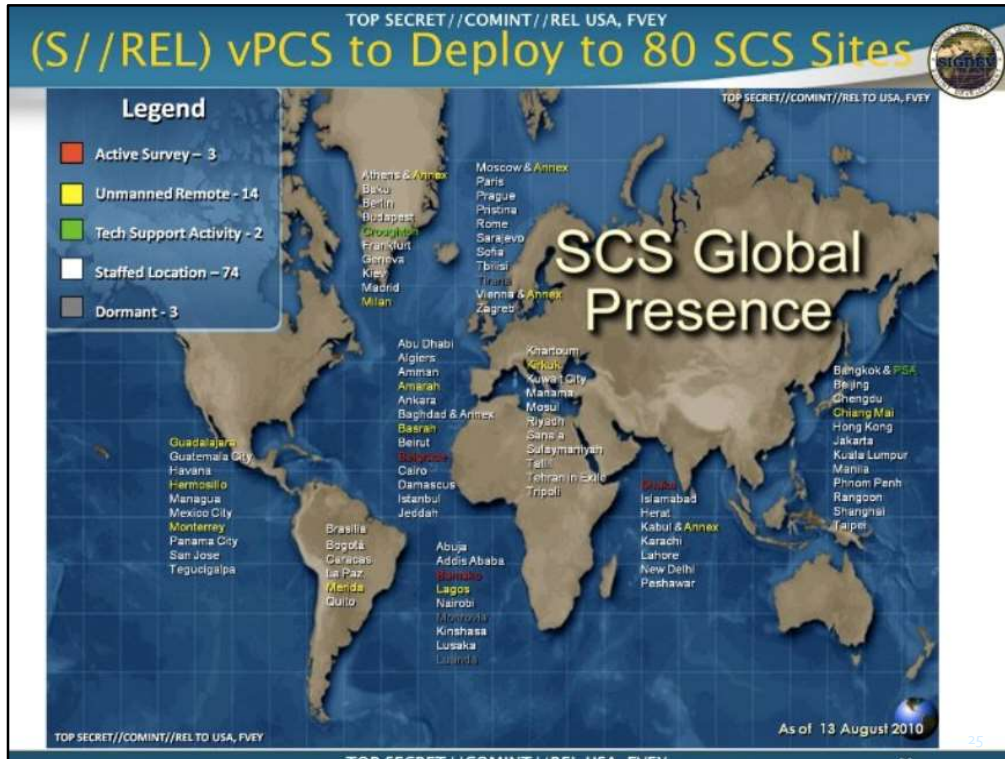
1. **F6 (Special Collection Service)** – joint CIA and NSA clandestine operations including espionage on foreign diplomats and leaders;
2. **FORNSAT** – "foreign satellite collection", intercepts from satellites;
3. **SSO (Special Source Operations)** – a division that cooperates with telecommunication providers.

24

The NSA collects data from its sites such as "US and allied military and other facilities as well as US embassies and consulates". These XKeyscore servers are fed with data from the following collection systems:

- F6 (Special Collection Service) – joint CIA and NSA clandestine operations including espionage on foreign diplomats and leaders;
- FORNSAT – "foreign satellite collection", intercepts from satellites;
- SSO (Special Source Operations) – a division that cooperates with telecommunication providers.





### Special Collection Sites

The Special Collection Service (SCS) 'Global Presence' map released by *Der Spiegel* as part of the Snowden revelations details 96 covert surveillance sites around the world.

This information was available to USA and other 'Five Eyes' countries: Australia, Canada, Great Britain and New Zealand. It is unclear whether this map is a complete list of operational SCS locations because it does not include Britain, Canada, Australia or New Zealand.

Search jobs Sign in Search UK edition

**The Guardian**

News Opinion Sport Culture Lifestyle More

World Europe US Americas Asia Australia Middle East Africa Inequality Global development

**World news**

## Revealed: US dirty tricks to win vote on Iraq war

Secret document details American plan to bug phones and emails of key Security Council members

**Martin Bright, Ed Vulliamy in New York and Peter Beaumont**  
Sun 2 Mar 2003 04:18 GMT

f t e 47



Katharine Gun exposed the US plot to spy on the UN.

The United States is conducting a secret 'dirty tricks' campaign against UN Security Council delegations in New York as part of its battle to win votes in favour of war against Iraq. Details of the aggressive surveillance operation, which involves interception of the home and office telephones and the emails of UN delegates in New York, are revealed in a document leaked to The Observer.

The disclosures were made in a memorandum written by a top official at the National Security Agency - the US body which intercepts communications around the world - and circulated to both senior agents in his organisation and to a friendly foreign intelligence agency asking for its input.

The memo describes orders to staff at the agency, whose work is clouded in secrecy, to step up its surveillance operations 'particularly directed at... UN Security Council Members (minus US and GBR, of course)' to provide up-to-the-minute intelligence for Bush officials on the voting intentions of UN members regarding the issue of **Iraq**.

Example of the kinds of surveillance undertaken by the NSA – the bugging of UN Security Council delegates in 2003 during the US battle to win votes in favour of a war against Iraq.

Katharine Gun was working at GCHQ at the time and blew the whistle on these activities – as depicted in the film “Official Secrets”.

Search jobs My account Search UK edition

**The Guardian**

News Opinion Sport Culture Lifestyle More

World Europe US Americas Asia Australia Middle East Africa Inequality Global development

**The NSA files**

**Ewen MacAskill in Rio de Janeiro and Julian Borger**  
Sun 30 Jun 2013 21:28 BST



## New NSA leaks show how US is bugging its European allies

**Exclusive: Edward Snowden papers reveal 38 targets including EU, France and Italy**

**Berlin accuses Washington of cold war tactics**

US intelligence services are spying on the European Union mission in New York and its embassy in Washington, according to the latest top secret US National Security Agency documents leaked by the whistleblower **Edward Snowden**.

One document lists 38 embassies and missions, describing them as "targets". It details an extraordinary range of spying methods used against each target, from bugs implanted in electronic communications gear to taps into cables to the collection of transmissions with specialised antennae.

Along with traditional ideological adversaries and sensitive Middle Eastern countries, the list of targets includes the EU missions and the French, Italian and Greek embassies, as well as a number of other American allies, including Japan, Mexico, South Korea, India and Turkey. The list in the September 2010 document does not mention the UK, Germany or other western European states.

27

2013 – Snowden files reveal that the US is bugging its European allies.

“One of the bugging methods mentioned is codenamed Dropwire, which, according to a 2007 document, is "implanted on the Cryptofax at the EU embassy, DC" – an apparent reference to a bug placed in a commercially available encrypted fax machine used at the mission.

The NSA documents note the machine is used to send cables back to foreign affairs ministries in European capitals.

The documents suggest the aim of the bugging exercise against the EU embassy in central Washington is to gather inside knowledge of policy disagreements on global issues and other rifts between member states.”

Search jobs My account Search UK edition

**The Guardian**

News Opinion Sport Culture Lifestyle More

World Europe US Americas Asia Australia Middle East Africa Inequality Global development

**NSA** This article is more than 4 years old

**NSA tapped German Chancellery for decades, WikiLeaks claims**

**New documents released suggest communications between top officials including Angela Merkel were intercepted by the US spy agency**

*Reuters in Berlin*  
Wed 8 Jul 2015 23:39 BST

878 254



The US **National Security Agency** tapped phone calls involving German chancellor Angela Merkel and her closest advisers for years and spied on the staff of her predecessors, according to WikiLeaks.

A report released by the group on Wednesday suggested NSA spying on Merkel and her staff had gone on far longer and more widely than previously realised. **WikiLeaks** said the NSA targeted 125 phone numbers of top German officials for long-term surveillance.

The release risks renewing tensions between Germany and the US a month after they sought to put a row over spying behind them, with Barack Obama declaring in Bavaria that the two nations were “inseparable allies”.

WikiLeaks published what it said were three NSA intercepts of Merkel’s conversations, and data it said listed telephone numbers for the chancellor, her aides, her office and even her fax machine.

“The names associated with some of the targets indicate that spying on the Chancellery predates **Angela Merkel** as it includes staff of former Chancellor Gerhard Schroeder (in office 1998-2002), and his predecessor Helmut Kohl,” WikiLeaks added in a statement.

▲ Cables released by WikiLeaks allege communications from German chancellor Angela Merkel were intercepted. Photograph: Arben Celaj/Reuters

Also – the 2015 revelation of the tapping of Angela Merkel’s phone (and probably other European leaders too).



The program continues, with the intelligence agencies and governments convincing the public that it is necessary to prevent terrorism.  
But terrorism and attacks continue anyway.  
What is clear is that the intelligence agencies continue to operate autonomously, without accountability, eavesdropping on the public and politicians alike - and even the UN.  
If we cannot do anything to put a stop to this situation then we could eventually find ourselves in a police state, in which privacy no longer exists.

29

And so the program continues, with the intelligence agencies and governments convincing the public that it is necessary to prevent terrorism.

But terrorism and attacks occur in any case.

What is clear is that the intelligence agencies continue to operate autonomously, without accountability, eavesdropping on the public and politicians alike - and even the UN.

If we cannot do anything to put a stop to this situation then we could eventually find ourselves in a police state, in which privacy no longer exists.

It is so important to keep up the protest, keep up the pressure. Thanks to MHAC and to CAAB previously for keeping this issue in the news and for the continued opposition to the activities of Menwith Hill.

There are other similar groups in other countries – the U.S., Canada, Australia and New Zealand for example, who are also leading the protests there, but we really need a mass protest and/or strong political opposition to make any real headway on these issues.

**Thanks for  
Listening!**

30

Excuse the pun!