



# Exclusive: UK's secret Mid-East internet surveillance base is revealed in Edward Snowden leaks

Data-gathering operation is part of a £1bn web project still being assembled by GCHQ

Duncan Campbell, Oliver Wright, James Cusick, Kim Sengupta

Friday, 23 August 2013

Britain runs a secret internet-monitoring station in the Middle East to intercept and process vast quantities of emails, telephone calls and web traffic on behalf of Western intelligence agencies, *The Independent* has learnt.

The station is able to tap into and extract data from the underwater fibre-optic cables passing through the region.

The information is then processed for intelligence and passed to GCHQ in Cheltenham and shared with the National Security Agency (NSA) in the United States. The Government claims the station is a key element in the West's "war on terror" and provides a vital "early warning" system for potential attacks around the world.

*The Independent* is not revealing the precise location of the station but information on its activities was contained in the leaked documents obtained from the NSA by Edward Snowden. *The Guardian* newspaper's reporting on these documents in recent months has sparked a dispute with the Government, with GCHQ security experts overseeing the destruction of hard drives containing the data.

The Middle East installation is regarded as particularly valuable by the British and Americans because it can access submarine cables passing through the region. All of the messages and data passed back and forth on the cables is copied into giant computer storage "buffers" and then sifted for data of special interest.

Information about the project was contained in 50,000 GCHQ documents that Mr Snowden downloaded during 2012. Many of them came from an internal Wikipedia-style information site called GC-Wiki. Unlike the public Wikipedia, GCHQ's wiki was generally classified Top Secret or above.

The disclosure comes as the Metropolitan Police announced it was launching a terrorism investigation into material found on the computer of David Miranda, the Brazilian partner of *The Guardian* journalist Glenn Greenwald – who is at the centre of the Snowden controversy.



Scotland Yard said material examined so far from the computer of Mr Miranda was "highly sensitive", the disclosure of which "could put lives at risk".

*The Independent* understands that *The Guardian* agreed to the Government's request not to publish any material contained in the Snowden documents that could damage national security.

As well as destroying a computer containing one copy of the Snowden files, the paper's editor, Alan Rusbridger, agreed to restrict the newspaper's reporting of the documents.

The Government also demanded that the paper not publish details of how UK telecoms firms, including BT and Vodafone, were secretly collaborating with GCHQ to intercept the vast majority of all internet traffic entering the country. The paper had details of the highly controversial and secret programme for over a month. But it only published information on the scheme – which involved paying the companies to tap into fibre-optic cables entering Britain – after the allegations appeared in the German newspaper *Süddeutsche Zeitung*. A Guardian spokeswoman refused to comment on any deal with the Government.

A senior Whitehall source said: "We agreed with *The Guardian* that our discussions with them would remain confidential".

But there are fears in Government that Mr Greenwald – who still has access to the files – could attempt to release damaging information.

He said after the arrest of Mr Miranda: "I will be far more aggressive in my reporting from now. I am going to publish many more documents. I have many more documents on England's spy system. I think they will be sorry for what they did."



One of the areas of concern in Whitehall is that details of the Middle East spying base which could identify its location could enter the public domain.

The data-gathering operation is part of a £1bn internet project still being assembled by GCHQ. It is part of the surveillance and monitoring system, code-named "Tempora", whose wider aim is the global interception of digital communications, such as emails and text messages.

Across three sites, communications – including telephone calls – are tracked both by satellite dishes and by tapping into underwater fibre-optic cables.

Access to Middle East traffic has become critical to both US and UK intelligence agencies post-9/11. The Maryland headquarters of the NSA and the Defence Department in Washington have pushed for greater co-operation and technology sharing between US and UK intelligence agencies.

The Middle East station was set up under a warrant signed by the then Foreign Secretary David Miliband, authorising GCHQ to monitor and store for analysis data passing through the network of fibre-optic cables that link up the internet around the world

The certificate authorised GCHQ to collect information about the "political intentions of foreign powers", terrorism, proliferation, mercenaries and private military companies, and serious financial fraud.

However, the certificates are reissued every six months and can be changed by ministers at will. GCHQ officials are then free to target anyone who is overseas or communicating from overseas without further checks or controls if they think they fall within the terms of a current certificate.

The precise budget for this expensive covert technology is regarded as sensitive by the Ministry of Defence and the Foreign Office.

However, the scale of Middle East operation, and GCHQ's increasing use of sub-sea technology to intercept communications along high-capacity cables, suggest a substantial investment.

Intelligence sources have denied the aim is a blanket gathering of all communications, insisting the operation is targeted at security, terror and organised crime.