

افغانستان آزاد – آزاد افغانستان

AA-AA

چو کشور نیاشد تن من مباد بدین بوم ویر زنده یک تن مباد
همه سر به سر تن به کشتن دهیم از آن به که کشور به دشمن دهیم

www.afgazad.com

afgazad@gmail.com

European Languages

زبان های اروپائی

<http://www.guardian.co.uk/world/2013/jun/22/nsa-leaks-britain-us-surveillance>

US and Britain team up on mass surveillance

Latest revelations from Edward Snowden show that the state risks crossing ever more ethical and legal boundaries

6/22/2013

The so-called UKUSA agreement goes back over 60 years.

Twelve years ago, in an almost forgotten report, the European parliament completed its investigations into a long-suspected western intelligence partnership dedicated to global signals interception on a vast scale.

Evidence had been taken from spies and politicians, telecommunications experts and journalists. In stark terms the report detailed a decades-old arrangement which had seen the US and the UK at first – later joined by Canada, New Zealand and Australia to make up the the so-called "Five Eyes" – collaborating to access satellites, transatlantic fibre-optic cables and radio signals on a vast scale.

This secretive (and consistently denied) co-operation was itself the product of a mutual agreement stretching back to the first world war, expanded in the second, and finally ratified in 1948 in the so-called UKUSA agreement.

The problem for the authors of the Brussels report was that it had based its analysis on scattered clues and inferences. "It is only natural," its authors asserted ruefully, "that secret services do not disclose details of their work ... The existence of such a system thus needs to be proved by gathering as many clues as possible, thereby building up a convincing body of evidence."

Despite the limitations of such detective work, the parliamentarians came to a deeply troubling conclusion: the "Five Eyes" were accessing the fibre-optic cables running under the Atlantic.

Not only that, the report concluded tentatively, but it was the UK specifically among the five partners – and GCHQ in particular – which it suspected had been given primary responsibility for intercepting that traffic.

"The practical implication," the report surmised, "is that communications can be intercepted at acceptable cost only at the terminals of the underwater cables which land on their territory.

"Essentially they can only tap incoming or outgoing cable communications. In other words, their access to cable communications in Europe is restricted to the territory of the United Kingdom."

That GCHQ was at the very heart of secret efforts to tap into the internet and cable-carried telephony was finally confirmed in the most dramatic terms on Friday by the latest batch of documents to be leaked by former US National Security Agency contractor Edward Snowden, who is now being sought by the US government for alleged theft and breaches of the Espionage Act.

Those documents, published by the *Guardian*, not only describe the UK's lead role in tapping the cables carrying global internet traffic – enjoying the "biggest internet access" of the Five Eyes – but its efforts to suck up ever-larger amounts of global data to share with its partners, and principally with the US.

From a handful of cables at the beginning, the UK is now able, according to the documents, to access some 200 on a daily basis and store the information contained within for up to 30 days for analysis, including up to 600m "telephone events" each day.

GCHQ's own excitement at the scope of its reach is evident in the documents, in which there is an excited reference to an ability to collect "massive amount of data!" and to "producing larger amounts of metadata (the basic information on who has been contacting whom, without detailing the content) than NSA".

Up to the late 1980s, in excess of 90% of all international voice-and-data traffic, including diplomatic cables, was being carried by satellite and microwave networks. That began to change rapidly in 1988 when AT&T finished laying the first undersea fibre-optic fibre cable from New Jersey to the UK.

Even before that project was completed, the NSA was already experimenting how to gain access to the cables, efforts that would lead to the US making its first attempts to bug one in the mid-1990s with an underwater vehicle.

Now, the documents seem to suggest, access is achieved through some degree of co-operation – voluntary or otherwise – from the companies operating the cables or the stations at which they come into the country. And in addition to confirming details of how the partnership functions,

the latest disclosures from Snowden also describe in detail what appears to be one of its latest iterations – Project Tempora, initiated some four years ago.

The direct descendent of earlier UKUSA treaty programmes, Project Tempora's purpose remains the hoovering up of the largest amount of signals intelligence, principally in the form of metadata. Then, as now, it appears the priorities are not only related to national security but also economic advantage – interventions which can be justified under UK law by reference to the ill-defined notion of "economic wellbeing".

In one sense, GCHQ is simply trying to keep up with the dizzying pace of technological development over recent decades. As the most recent batch of leaked documents has made clear – interception – like drugs-testing in sport – has tended to lag one step behind technology.

"It is becoming increasingly difficult for GCHQ," the authors of one memo write, "to acquire the rich sources of traffic needed to enable our support to partners within HMG [Her Majesty's government], the armed forces, and overseas.

"The rapid development of different technologies, types of traffic, service providers and networks, and the growth in sheer volumes that accompany particularly the expansion and use of the internet, present an unprecedented challenge to the success of GCHQ's mission. Critically we are not currently able to prioritise and task the increasing range and scale of our accesses at the pace, or with the coherence demanded of the internet age: potentially available data is not accessed, potential benefit for HMG is not delivered."

But the dangers lie in the various legal and ethical thresholds being crossed in the race to catch up with the proliferating forms of communication. If that report from almost a decade and a half ago was prescient in one area, it was over the human rights, privacy and legal concerns that were raised by the ambitions of western intelligence. Those issues have only been brought into sharper focus as signals intelligence gathering has moved ever more forcefully into capturing the worldwide web.

According to the leaked Snowden documents, the latest attempts to improve interception of internet communications began in earnest in 2007. The first experimental project was run at GCHQ's outpost at Bude in Cornwall.

Within two years it would be judged enough of a success to allow analysts from the NSA to have access to the new project, which by 2011 would be capturing and producing more intelligence data in the UK than the NSA did in the US.

Other documents underline how the decades-old intelligence arrangement has worked, not least how within the UKUSA treaty different roles have been subcontracted to partners – for both practical and regulatory reasons.

In one document, the NSA's chief Lt Gen. Keith Alexander asks pointedly: "Why can't we collect all the signals all the time? ... Sounds like a good summer project for Menwith" — a reference to GCHQ's Menwith Hill eavesdropping site in northern England.

On the legal front – as GCHQ's own lawyers boasted in advice to its US partners – Cheltenham had an advantage to its US partners: "We have a light oversight regime compared with the US".

Such potential subcontracting has long been at the heart of international legal concerns over how surveillance material is shared between the Five Eyes. The suspicion is that individual states within the agreement can produce material for partners that might be illegal to gather in the other collaborating states, including the US.

Shami Chakrabarti, the director of Liberty, said: "The big point we should recognise is that states tend to have a broader licence to snoop abroad and a tighter one at home. What we are seeing in arrangements like this is states' ability to subcontract their dirty work to others."

Then there is the question of oversight. The UK government claims that the interception in such a broad fashion is authorised by ministers under at least 100 certificates issued under section 8(4) of the Regulation of Investigatory Powers (Ripa) which allows sweeping an indiscriminate trawls of data. But Alex Bailin QC, an expert on surveillance at the Matrix Chambers, is sceptical. "We are told there is proper oversight but the question is whether ministers simply sign these certificates. But I wasn't even aware section 8(4) existed until Friday."

Like Chakrabarti, Bailin suspects that intelligence agencies are subcontracting out surveillance to foreign partners. "The reality is that Ripa is incredibly complex and full of legal loopholes that permit this kind of thing. The real question is whether the act is actually fit for purpose when you are dealing with interception like this."

The European parliament's thesis has been confirmed by the *Guardian's* revelations. Now the legal and ethical scrutiny can begin in earnest.