world news

History of 5-Eyes – explainer

Partnership forged in wartime to monitor enemy radio transmissions now scoops up data about ordinary citizens

Monday 2 December 2013 16.30 EST

A field radio in the Pacific during the second world war. Communications technology has changed drastically – and intelligence gathering is far easier in the digital age. Photograph: Corbis

Paul Farrell

During the second world war intelligence officers from Britain and the US would crouch over bulky radio transmitters listening in on crackling enemy exchanges. In the years since then, communications technology has changed drastically - and intelligence gathering is far easier in the digital age.

But despite the changes it is the same agreement that still governs the sharing of signals intelligence between Britain, the US, Australia, New Zealand and Canada - known in shorthand as the "5-Eyes" countries.

The exchange of intelligence was an important part of US-UK efforts during the second world war. This co-operation continued after the war, resulting in the UKUSA agreement of 1946. As a British dominion at the time, Australia was not party to the agreement in its own right, but all British dominions occupied a special status that elevated them above other "third-party" countries.

By 1955 the role of the other 5-Eyes nations was formalised when the agreement was updated: "At this time only Canada, Australia and New Zealand will be regarded as UKUSA-collaborating Commonwealth countries," an annexure in the new agreement reads.

The Defence Signals Branch - now known as the Australian Signals Directorate - was to "collaborate directly", with tasks as determined by the US National Security Agency, and "will exchange raw material, technical material and end product of these tasks".

It is not clear how much the agreement has changed since then, and whether Australia is still being allocated "tasks" in such a way - but the

nature of those tasks would be very different.

"In the days when the agreement was put together, your main source of signals was high-frequency radio that could be transmitted for several thousand kilometres around the world, so you had a whole network of stations to monitor HF radio," says Australian National University professor Des Ball, an Australian intelligence expert. "Many of those stations are still here."

Throughout the 1960s these radio signals were left behind; in their place came satellite or microwave relay communications, and each of the parties began developing interception methods for these. With each leap in technology came new capabilities.

"As communications moved into much much higher of the frequency spectrum with mobile phones and then cell phones, they moved into facilities that could intercept those much shorter range signals, so there has been an evolution which has matched the change in means of communications," Ball says.

Intelligence gathering has developed even further with digital communication interceptions, and as leaked NSA documents have shown, Australia has been operating listening posts around the Asia-Pacific region, passing data back to the US.

But high-frequency radio transmissions are vastly different from the internet, in both form and purpose. The executive director of the Cyberspace Law and Policy Centre, David Vaile, says the internet should not be seen as a medium designed for this kind of mass data collection.

"With the vast amount of information that's exposed online there is a greater need for more protection," Vaile says.

The original agreement was created to share information about intelligence gathered on foreign countries, not domestic surveillance. But that purpose and the scope of the intelligence being gathered also appears to have changed.

The 1946 agreement specifically related to "foreign intelligence", which is defined as "all communications of the government or of any military, air, or naval force, faction, party, department, agency, or bureau of a foreign country, or of any person or persons acting or purporting to act therefor, and shall include communications of a foreign country which may contain information of military, political or economic value". It specifically excludes the US, the British Commonwealth and nations, and the British empire from the scope of this sort of information.

But we now know from documents provided by the whistleblower Edward Snowden that the NSA has been able to retain vast amounts of data from Britain and other 5-Eyes nations, allowing information about ordinary citizens to be caught up in the dragnet.

In a draft 2005 directive in the name of the NSA's director of signals intelligence, the agency prepared policies that would enable spying on 5-Eyes partners, even without permission of the other country: “[The March 1946 UKUSA agreement] has evolved to include a common understanding that both governments will not target each other's citizens/persons. However, when it is in the best interest of each

nation, each reserved the right to conduct unilateral Comint action against each other's citizens/persons.

"Under certain circumstances, it may be advisable and allowable to target second-party persons and second-party communications unilaterally when it is in the best interests of the US."

This shift in the agreement is what Vaile says is one of the most serious risks, because it helps facilitate spying on the citizens of other parties to the agreement.

"If you actually did want to spy more on the local people then it appears that with co-operation of the other partners this is easier, because they would have the legal right in their own domestic law to treat the citizens of the other countries as foreigners, and that appears to be where the rot has set in."

“There used to be a very clear distinction between intelligence gathering on non-nationals and domestic citizens, but that appears to have changed.”

The limitations placed on the activities of the 5-Eyes countries with respect to the what they can gather on the other partners appear to have changed over time. The question that remains is just how far the partners have gone in conducting surveillance on each other.

Tags: Surveillance, Espionage, Australia, NSA, The NSA files

Related stories

- 

  Australia needs to face up to the dangers of facial recognition technology

  David Paris
  State and federal governments must follow the lead of cities here and abroad to suspend its use and develop a regulatory framework
  7 Aug 2020
  7 Aug 2020
  Australia needs to face up to the dangers of facial recognition technology

- Encryption laws are hurting Australia's tech sector, Atlassian says

  Rushed bill makes overseas companies reluctant to engage with local players, MPs told
  27 Jul 2020
  Encryption laws are hurting Australia's tech sector, Atlassian says

- George Brandis's salvo in cryptowars could blow a hole in architecture of the internet

  Attorney general isn’t just proposing a backdoor into encrypted communications - it’s a giant sinkhole your backdoor fell into
  12 Jun 2017
  George Brandis's salvo in cryptowars could blow a hole in architecture of the internet

The snooper's charter is back - video explainer

The UK government’s bid to increase surveillance powers in the investigatory powers bill, the so-called ‘snooper’s charter’, has survived several attempts to kill it

1:23

2 Mar 2016

The snooper's charter is back - video explainer

- Australian police to adopt technology capable of collecting emails

  10 Dec 2013

  Australian police to adopt technology capable of collecting emails

- Australia's surveillance has 'achieved too much' to stop, says David Johnston

  3 Dec 2013

  Australia's surveillance has 'achieved too much' to stop, says David Johnston

- Data seizures a 'gross intrusion' into privacy, civil liberties groups say

  3 Dec 2013

  Data seizures a 'gross intrusion' into privacy, civil liberties groups say

- Revealed: Australian spy agency offered to share data about ordinary citizens

  2 Dec 2013

  Revealed: Australian spy agency offered to share data about ordinary citizens

+ − More Related stories

Popular

Popular in World news | Popular in The Guardian

1 **MH370: Indian Ocean crash may have been heard by underwater microphones**
Curtin University in Western Australia says analysis shows a possibility, albeit slim, that listening devices picked up impact

2 **Qataris defend country's right to host World Cup amid anger and denial**

3 **Bowe Bergdahl: Taliban release dramatic video of handover to US**

4 **Claim of 800 children's remains buried at Irish home for unwed mothers**

5 **Tiananmen square protests and crackdown: 25 years on**

6 **G7 presses Vladimir Putin to pursue peaceful end to Ukraine crisis**

7 **Tony Abbott's delayed departure for Indonesia blamed on Labor**

8 **Heathrow's new Terminal 2 opens to first passengers**

9 **Tony Abbott heads for Indonesia - the day in politics**

10 **Barnaby Joyce backtracks after cracking joke about Peta Credlin**

Back to top